Ingeniería social amenaza latente para la seguridad informática.

Espitia, Angélica María.
angelikaespitia@gmail.com
Universidad Piloto de Colombia

Resumen—En el marco de la seguridad informática es importante resaltar la ingeniería social teniendo en cuenta que omite el dominio de cuestiones técnicas y se basa en el aprovechamiento del eslabón más débil el usuario; sin importar lo fuerte que sea el sistema de seguridad implementado en las organizaciones. La ingeniería social puede ser utilizada por los atacantes como estrategia para obtener información de forma ilegal, pero también puede ser utilizada de forma defensiva por las organizaciones las cuales deberían generar planes de sensibilización y concientización a los usuarios sobre la importancia de la seguridad de la información.

Abstract- In the context of computer security is important to highlight the social engineering that omits considering the domain of technical issues and is based on exploiting the weakest link the user; no matter how strong the security system implemented in organizations. Social engineering can be used by attackers as a strategy to obtain information illegally, but can also be used defensively by organizations which should generate sensitization and awareness plans users about the importance of information security.

Índice de Términos—Ataques, Defensa, Ingeniería Social, Riesgo.

I. INTRODUCCIÓN

La ingeniería social no es una amenaza nueva, ha existido desde el origen de los tiempos es una mezcla de ciencia, psicología y arte. Por esta razón observaremos las dos caras de esta estrategia desde el punto de vista del atacante y del atacado (naciones, organizaciones, personas). Algunos conceptos básicos son:

- Ingeniería Social [1]: Cualquier acto que influye en una persona a tomar una acción que pueden o no ser de su interés. No siempre es negativo, pero abarca la forma en que nos comunicamos ejemplo: con nuestros padres, terapeutas, hijos, cónyuges y otros.

- Riesgo [2]: Es la posibilidad de incurrir en pérdidas por deficiencia, falla o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura, o por la ocurrencia de acontecimientos externos, que tengan capacidad de incidir en el desarrollo del negocio.

En la actualidad debido a las nuevas plataformas tecnológicas, los nuevos riesgos y retos de la industria (Redes sociales, comercio electrónico, transacciones bancarias, almacenamiento en la nube, entre otros) afectan tanto a personas como organizaciones que son susceptibles de sufrir ataques basados en ingeniería social; teniendo en cuenta que se aprovechan del eslabón más débil “las personas”. La mayoría de estos ataques en las organizaciones son controlados y/o contrarrestados en inversión de equipos, tecnología y aun creemos que es suficiente, pero realmente estamos descuidando la concientización de los usuarios con relaciona a la seguridad de su información.

Adicional a esto las nuevas tecnologías de comunicaciones han permitido que la brecha entre usuarios y máquinas sea cada vez menor, los complejos sistemas de comunicación también han desarrollado modelos que dan al usuario la capacidad de intercambiar información de una manera cada vez más rápida, fácil y sencilla. Ejemplos de esto es la evolución de los mensajes de correo electrónico, mensajeros instantáneos, redes sociales, mensajes de texto, entre otros, los cuales proporcionan una manera efectiva de intercambio de información. Por esta razón con el uso y aprovechamiento de tecnologías los usuarios tienden a confiar en todo lo que hay detrás, es decir, si el usuario ve una interfaz amigable o "conocida", normalmente supondría que el dueño de dicha información es precisamente quien la está publicando. Es decir, si ve un correo o la pagina web principal de la organización YZ, supondrá que es efectivamente la organización YZ es quien está emitiendo la información, o al menos es lo que la mayoría de los usuarios que no han sido informados de los riesgos y amenazas de seguridad informática tendrían en mente.

II. INGENIERÍA SOCIAL Y LAS COMUNICACIONES ELECTRÓNICAS

Lo primero que debemos recordar es que el usuario es el punto más débil en la infraestructura de seguridad, debido que con una sola acción permite la omisión todas las protecciones tecnológicas implementadas detrás de él. La finalidad de la ingeniería social es manipular a una persona en su entorno laboral o personal para que de forma directa o indirecta realice actividades que conlleven a la consecución de un fin específico para quien aplica esta técnica. En pocas palabras es la habilidad de engañar para conseguir información de forma ilegal de una persona o sistema. Como lo indica Christopher Hadnagy en su libro "Ingeniería Social el Arte del Hacking Personal" la Ingeniería Social es "El acto de manipular a una persona para que lleve a cabo 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 logar que se realice una determinada acción". Un Ejemplo son los médicos que a menudo utilizan elementos que se consideran de Ingeniería Social para "manipular" a sus pacientes para que realicen acciones que son buenas para ellos, en cambio un estafador utiliza estos mismos elementos de Ingeniería Social para convencer a su víctima para que realice acciones que le perjudican. Aunque el resultado es muy diferente, el proceso puede ser similar.

Debido a lo expuesto anteriormente y teniendo en cuenta que en la actualidad por la masificación de las comunicaciones (correo electrónico, mensajes de texto, chat y redes sociales como facebook, twitter, instagram, por nombrar algunas) y el uso de dispositivos móviles que permiten a las personas y empresas comunicarse en tiempo real se observa que los usuarios aun no son consientes de la importancia de la información que publican y por esta razón son susceptibles a procesos de ingeniería social.

Estos son algunos de los casos más representativos de uso de la ingeniería social en comunicaciones electrónicas:

- La Estafa Nigeriana o timo 419 se lleva a cabo utilizando el correo electrónico. Adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que muchas de estas estafas provienen de ese país. Es un tipo de correo basura, esta escrito en idioma inglés donde los estafadores explican que una persona tiene acceso a unos fondos acumulados pero que tiene problemas para efectuar movimientos con estos dineros, porque se trata de fondos secretos y requiere sacarlos de Nigeria lo más rápido posible, entonces ofrece una compensación exagerada por este "favor". Cuando tienen confianza con la victima ofrecen transferir millones de dólares a su cuenta bancaria a cambio de un pequeño cargo. Si la persona responde al

ofrecimiento inicial, le envía documentos que parecen ser oficiales, para terminar de ganar la confianza de la victima. En este punto es donde se le pide que provea los números de sus cuentas bancarias y una serie de información de carácter privado para hacer efectivo el traspaso. Y así consiguen la información personal de sus victimas.

- Phishing: Es un ataque simple pero efectivo busca engañar al usuario para que piense que el administrador del sistema solicita clave con fines legítimos. Por eso las personas que navegan en internet frecuentemente reciben mensajes que solicitan contraseñas o información de su tarjeta de crédito con el motivo de crear una cuenta, reactivar una configuración o realizar otra operación aparentemente inofensiva. Por esta razón la mayoría de entidades bancarias lanzan campañas para concientizar al usuario de verificar la veracidad de los sitios que solicitan información relacionada con sus cuentas bancarias.

- Spoofing: Busca suplantar la identidad en la red; en la mayoría de ocasiones con fines maliciosos. Uno de las situaciones más comunes es el envío de virus a través de correos electrónico aparentemente inofensivos, por esa razón muchas personas solo revisan correos que tengan un remitente conocido, pero existe la probabilidad que alguien se apropie de una cuenta de correo para utilizarla en envío de correos masivos basados en la libreta de direcciones de este correo.

III. TIPOS DE INGENIEROS SOCIALES

La Ingeniería Social puede verse desde diferentes ámbitos. Ser maliciosa o amigable dependiendo de su fin construir o destruir. Por esta razón existen diferentes tipos de ingenieros sociales de acuerdo a lo que buscan

- Hackers: a través de la ingeniería social buscan sustraer información para afectar sistemas informáticos.
- Probadores de seguridad: se apoyan en la ingeniería social para entender como actúan los usuarios y que actividades se pueden realizar para evitar que caigan en esta tipo de manipulación.
- Espías: Buscan obtener información privilegiada manipulando a las personas.
- Agentes de recursos humanos: se apoyan en la ingeniería social para entender y conocer a las personas a ser contratadas.
- Vendedores: se apoyan en la ingeniería social para entender las necesidades y gustos de los compradores.
- Gobiernos: No siempre son vistos como Ingenieros Sociales, pero los gobiernos utilizan la Ingeniería Social para controlar el mensaje que envían a las personas que gobiernan.

Parece que se puede encontrar la Ingeniería Social o algún aspecto de ella en cualquier campo. Por eso, se sostiene firmemente que la Ingeniería Social es una ciencia.

IV. INGENIERÍA SOCIAL COMO UTILIZARLA

Lo más importante para las organizaciones y las personas es la información, por esta razón se debe realizar un proceso de capacitación y concientización sobre este tema. Recordemos que esta es la mejor defensa contra la mayoría de los ataques de Ingeniería Social. Incluso en aquellos contra los que el conocimiento del tipo de ataque no puede proteger al 100% la información, pero cuando se conoce en detalle estos ataques las personas tendrán mayor control y se mantendrán alerta. La formación permite mejorar habilidades propias y permanecer actualizados. Se debe realizar pruebas recordemos que la practica es necesaria.

Recopilar Información: Ninguna información es irrelevante desde la perspectiva de la Ingeniería Social, por eso hasta el detalle mas mínimo puede permitir la obtención de datos valiosos para las personas y/o las organizaciones.

Ejemplo: Estamos interesados en la información de una nueva compañía ABC, nuestro primer paso es verificar en internet y existe muy poca información, pero se realiza un rastreo y se encuentra que un alto directivo de la compañía utiliza el correo corporativo en una de las redes sociales verificamos sus gustos y sabemos que colecciona monedas antiguas, se crea una pagina web atractiva con información relacionada con monedas antiguas (pero con un marco malicioso que recopila información del equipo del directivo), se procede a enviar un correo al alto directivo el cual tiene un link a la pagina que se creo previamente. Por medio de la red social se obtiene el número de celular del directivo. Con este simple caso se refleja que un simple dato "correo electrónico corporativo" puede llegar a afectar la seguridad de la organización

De acuerdo a lo anterior es importante realizarnos estas preguntas:

¿Cómo se puede recopilar información?
¿Qué fuentes de recopilación de información existen y son utilizados por los Ingenieros Sociales?
¿Qué puede deducir del objetivo de acuerdo a los datos recopilados?
¿Cómo puede ubicar, almacenar y catalogar toda esta información para facilitar su utilización?

Existen muchas herramientas que ayudan a recopilar y utilizar la información. Para realizar pruebas de seguridad y auditorías de Ingeniería Social es recomendable la utilización de una distribución de Linux BackTrack y especialmente Dradis y BasKet útiles para la recopilación y almacenamiento de información. La prioridad de un Ingeniero Social, es reunir información, pero si no se puede recuperarla y utilizarla de manera ágil entonces resulta inútil.

Fuentes de Recopilación de Información: Existen diferentes y variadas fuentes de recopilación de información. A continuación desplegare algunas de las posibilidades existentes:

- Recopilar Información de los sitios web: Los sitios web personales (Perfil de Facebook, twitter, instagram, entre otros) o corporativos (Paginas web corporativas, periódicos online, revisas online, entre otros), pueden proporcionar una gran cantidad de información. Lo primero que se debería realizar es reunir los datos básicos que se encuentren el sitio web de la persona u organización esto te permitirá contestar las siguientes preguntas

¿Qué hace la persona u organización?
¿Qué productos o servicios presta la persona u organización?
¿Dónde se encuentra localizado (Cuidad, Barrio)?
¿Cuáles son los números de contacto?
¿Cuáles son las palabras y frases importantes?
¿Cuál es la nomenclatura de los correos Electrónicos?

- Recopilar Información en las Redes Sociales: Tanto personas como organizaciones se encuentran altamente interesadas por la redes sociales, pero para las organizaciones tiene un factor interesante por que se visualiza como una opción de publicidad barata que llega a un gran número de clientes potenciales. Por esta razón es importante tener en cuenta que conforme los empleados brindan más información online sobre su vida, ejemplo actualizaciones sobre su situación personal y laboral, publicaciones con actualizaciones de su ubicación y cambios en el currículum, las organizaciones corren más riesgos de que los competidores observen todos sus movimientos debido a la exposición de información.

V. DEFENSAS, CONSIDERACIONES Y BUENAS PRÁCTICAS

Es importante que tanto las personas como las organizaciones se pregunten ¿existe defensas efectivas en contra de la ingeniería social? La respuesta a esta cuestión es si, pero todos los mecanismos se basan en la cultura informática y no en cuestiones cien por ciento técnicas, cabe aclarar que una parte significativa de la seguridad recae en los usuarios, tanto en las comunicaciones personales como en la vida real. Por esta razón es importante que las personas entiendan que existen situaciones de las que debemos desconfiar o ser manejadas con cuidado para evitar riesgos.

Como punto de partida algunas amenazas específicas, a continuación se describen recomendaciones que permitir disminuir de forma significativa la posibilidad de ser víctimas de alguna técnica de ingeniería social aplicada:

- Si se recibe cualquier correo de remitentes desconocidos, debe tratarse con extremo cuidado, ya que no solamente puede tratarse de un correo con información falsa, sino que puede contener archivos maliciosos adjuntos.

- Como una medida de protección general, se debe saber que las entidades bancarias nunca solicitarán información confidencial por correo electrónico, o incluso cualquier tipo de información del usuario.

- Al utilizar servicios bancarios en línea, se deben digitar siempre la url y verificar que cuente con la característica de pagina segura la cual inicia con https, así como que la dirección del portal realmente pertenezca a la url de la entidad, por ejemplo, si el banco ABC ofrece servicios en línea, y con total seguridad se sabe que su dirección web es www.ABC.com, entonces se debe verificar que no sea una dirección similar ejemplo www.ABCc.com. Una característica del phishing es que paginas auténticas pueden suplantarse con una simple similitud de las palabras, para el caso anterior podría ser que la página falsa fuera www.ABCc.com. El simple hecho de que se parezca, hace que muchos usuarios desprevenidos no se den cuenta y accedan. En este tipo de engaños que por muy sutiles y sencillos que parezcan, siguen siendo muy efectivos.

- No enviar información de acceso personal por correo electrónico. El no aplicar este tipo de medidas a pesar de su sencillez, es causa de innumerables inconvenientes en términos de seguridad informática, recordemos que la ingeniería social permite obtener información sensible y representa un problema económico para las víctimas.

En concreto, la ingeniería social realmente representa un problema serio de seguridad. No se necesita que el usuario sea un experto conocedor de seguridad, pero más allá de las consideraciones básicas se debe tener presente por lo menos cómo o en dónde están las amenazas, que muchas veces no serán virus, programas o equipos infectados, sino simplemente técnicas de engaño.

VI. REFLEXIÓN PERSONAL

Desde mi punto de vista las organizaciones deben capacitar y concientizar a sus empleados con relación a la importancia de la información. En la actualidad las personas no controlan lo que publica por medios electrónicos, no son consientes que el dato más simple puede conducir a información sensible de carácter personal o de la organización.

Además en la mayoría de organizaciones no existen políticas claras que les indiquen a los empleados la importancia de la información y los peligros a los que se ve expuesta la organización si son revelados. Un ejemplo sencillo es que sucedería si por un error de un empleado es pública a través de redes sociales la formula de la coca –

cola, es posible que surjan preguntas como ¿Cuál sería su impacto en el negocio? ¿Cómo actuaria la competencia? ¿Cuál es el grado de afectación de la imagen corporativa?, son preguntas simples que nos permiten visualizar que tan vital es la información para una organización.

Aunque la ingeniería social ha existido desde siempre en la actualidad somos más susceptibles a ataques basados en ella debido a la masificación de las comunicaciones y la poca o casi nula capacitación con relación a esta técnica.

VII. CONCLUSIONES

- Es importante entender que la seguridad informática no es simplemente un grupo de elementos tecnológicos y locativos engranados, se requiere de concientización y cultura por parte de las personas y la organización. Recordemos que el eslabón más débil en el entorno de la seguridad informática es el usuario. Por esta razón deben existir medidas que informen a los usuarios de la importancia de la información y su protección.

- Muchas organizaciones consideran que invertir en tecnología y servicios les asegura el cien por ciento de la seguridad de su infraestructura de TI y tienden a ignorar la importancia de los usuarios.

- Aunque algunas organizaciones tienen clara su postura con respecto a la importancia de la información, en el transcurso de esta investigación es evidencio que las personas no son consientes del valor de la información y consideran que las campañas de cultura informática no sirven y simplemente son una pérdida de tiempo y recursos .

REFERENCIA

[1] INGENIERO SOCIAL, INC. (2014) ¿Qué es la Ingeniería Social? http://www.social-engineer.org/about/

[2] DALTABUITZ; HERNÁNDEZ; MALLÉN, VASQUEZ. La Seguridad de la información. Limusa, Noriega Editores. 2007

[3] HADNAGY. Ingenieria Social: El Arte Del Hacking Personal. Anaya Multimedia. 2011

[4] SANTILLÁN, (2009). Ingeniería Social, Técnica de Ataque Eficaz en Contra de la Seguridad Informática http://revista.seguridad.unam.mx/numero-03/ingenier%C3%AD-social-t%C3%A9cnica-de-ataque-eficaz-en-contra-de-la-seguridad-inform%C3%A1tica

[5] SANDOVAL, (2011). Ingeniería Social: Corrompiendo la mente humana http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana