¡CUIDADO!: EXISTE INGENIERIA SOCIAL

Barbosa, Lourdes. Suarez, Catherine
lsbarbosac@hotmail.com, Catherine.suarezrodriguez@gmail.com
Universidad Piloto de Colombia

Resumen— El artículo desarrolla la lógica y fundamentos de la Ingeniería Social en la cual se emplean conductas para influenciar el pensamiento y acción de una persona o grupo de personas para obtener información. Es una disciplina que consiste básicamente en conseguir datos de otra persona sin que esta perciba que está revelando "información sensible" y que normalmente no lo haría. A nivel informático, generalmente se usa para conseguir nombres de acceso y contraseñas. Para usar esta disciplina no hay que ser un experto en sistemas, ni requiere muchos conocimientos, simplemente hay que saber a quién dirigir el "ataque" y bastante astucia. Es el arte de conseguir algo que nos interesa de otra persona por medio de habilidades sociales (manipulación). Estas conductas o técnicas que usan estas personas (también llamados Ingenieros Sociales) son tan estudiadas que para alguien que no conoce nada o no esta enrolado en temas de seguridad, son altamente efectivas y es por eso que la Ingeniería Social es tan preocupante. Aumenta todos los años el número de víctimas, es por eso que las personas necesitan protegerse para que no sean unas víctimas más.

Palabras Clave - Biométricos, Firewalls, Hacker, Parches**,** Robo de Identidad, Sniffer, Spam, Troyano.

Abstract - The article develops the logic and foundations of social engineering (Social Engineering) are those behaviors and techniques used to gather information from people. It is a discipline that is basically to get data to another person without the will realize that this revealing "sensitive information" and that normally would not do that. AT computer level, it is usually used to get names of access and passwords. To use this discipline is not to be an expert in systems, nor does it require much knowledge, simply know who lead the "attack" and quite cunning. It is an art, the art of getting something that we are interested in another person by means of social skills (manipulation). These behaviors or techniques that use these people (also called social engineers) are so studied that for someone who is not embedded in security issues, are highly effective, and that is why the Social engineering is so worrying. Increases every year the number of victims, that is why you need protected so that it is not a victim.

Keywords - Biometrics, Firewalls, Hacker, Identity Theft, Sniffer, Trojan, Spam, Patches.

I. INTRODUCCIÓN

Hoy en día sólo son necesarias las malas intenciones y una conexión a internet para sembrar el caos. Ya no es cuestión de conocimientos, sobre todo teniendo en cuenta que en los sistemas operativos más populares, se antepone la comodidad a la seguridad del sistema mismo.
La mayoría de los ataques a la seguridad se deben a errores humanos y no a fallas electrónicas. Los intrusos usan ingeniería social para acceder y siempre alguien los deja entrar sin ningún problema.
Las personas deben educarse, leer y entender a lo que están expuestas.

II. INGENIERÍA SOCIAL

Ingeniera Social se genera de muchas formas: El arte y ciencia de hacer que la gente haga lo que se desea", o "Ataque realizado por un hacker con trucos psicológicos en usuarios de una red para que entreguen información de acceso al sistema" y para terminar "Conseguir información importante (un *password por ejemplo) de una persona en lugar de intentar acceder a su PC*". En realidad la ingeniería social puede ser todo esto, dependiendo la óptica con que se mire. En lo único en que todas las personas coinciden es en que la ingeniería social es la manipulación de la tendencia humana de la confianza, y el objetivo de la persona que ejerce esta acción es obtener la información necesaria para acceder a la información sensible de una compañía ***[1]***.
La seguridad se fundamenta en la confianza: confianza en la protección y en la autenticación. Generalmente aceptado como el eslabón más débil en la cadena de la seguridad, las personas y la tendencia a confiar en las demás personas abren las puertas a muchísimas vulnerabilidades.

Los Ingenieros sociales utilizan métodos de engaños para obtener contraseñas o información útil. Pueden emplearse programas engañosos, páginas web falsas, concursos o cuestionarios falsos que piden a los usuarios que ingresen una contraseña. Si un usuario escribe la misma contraseña que usa en el trabajo, el hacker puede ingresar en las instalaciones sin tener que descifrar ni siquiera una línea de código, o incluso simplemente chatear con una persona ignorante del tema.

Increíblemente, la mayoría de las personas son manipuladas como para dar contraseñas a un extraño. El hecho que el atacante pueda persuadir a las personas para que le suministre el número de tarjeta de crédito, puede sonar como un algo

poco factible, sin embargo suministra datos confidenciales diariamente en distintos medios, en el mundo de las empresas de alta tecnología en las que se desarrollan proyectos reservados, donde la calificación técnica necesaria para entender la información que se quiere obtener es muy alta. Las operaciones de ingeniería social de este nivel pueden llevar meses de cuidada planificación y evaluación de muchos parámetros, van más allá de una actuación puntual basada en una llamada con más o menos gracia o picardía.

Muchas veces, el Ingeniero Social simplemente observa el entorno y aprovecha datos que están a la vista cuando el sentido común indica que deberían guardarse en un lugar seguro, como el papel que arroja a la basura o el sticker adhesivo con password (contraseña) debajo del teclado. También el factor humano es una parte esencial del juego de seguridad. No existe un sistema informático que no dependa de algún dato ingresado por un operador humano. En la Ingeniería Social se emplea grandes dosis de ingenio, sutileza y persuasión para así lograr obtener información a través de otra persona sin que se dé cuenta de que está revelando información importante con la que además, el atacante puede dañar la computadora. Esto significa que esta debilidad de seguridad es universal, independiente de plataforma, el software, red o edad de equipo.

Las víctimas típicas incluyen las empresas telefónicas, servicios de Helpdesk y CRM, corporaciones renombradas, agencias e instituciones gubernamentales y militares, instituciones financieras, hospitales y las personas con acceso dispositivos informáticos y como lo hacen usan el teléfono, en el sitio de trabajo, buscan en la basura, revisan el internet e intranet y fuera del sitio de trabajo.

III. Técnicas de la Ingeniería Social

Se establecen una clasificación de compromiso que divide estas prácticas en tres tipos según el nivel de interacción del Ingeniero social:

Técnicas Pasivas: Observación [2]

La observación de un acontecimiento concreto, de un lugar, de una persona o grupos de personas va más allá del concepto de "ver lo que pasa". Observar con detenimiento pero a la vez sin despertar sospechas. Fomentar capacidades como la "memoria visual" es muy importante para obtener de una situación la mayor cantidad de datos en el menor tiempo posible.

Si el objetivo es un lugar al cual se quiere acceder, es necesario conocer las medidas de seguridad, los accesos, el personal que lo vigila, la situación de los sistemas de alarma, si los despachos usan o no llave, si hay salidas sencillas o complicadas, si hay sistemas de grabación y si realmente se usan o no.

Técnicas no presenciales [2]

Muchas de las actuaciones de los ingenieros sociales se realizan a distancia, utilizando ya sea el teléfono, el fax, las redes de datos o incluso cartas tradicionales. A lo largo de los años se han ido perfeccionando las formas de operar y abriendo el abanico de las mismas a otros medios, he aquí algunas de ellas.

La contraseña perdida [2]

Todos hemos leído muchas veces que no es bueno utilizar en las contraseñas palabras que tengan significado, fechas que se relacionen con nosotros, números de DNI, nombres de familiares, etc. Esta recomendación no siempre se sigue, además de ello, existe una tendencia generalizada a utilizar la misma contraseña en múltiples servicios y esto facilita mucho el trabajo a aquellos que pretenden obtenerla de forma ilícita. No olvidar tampoco a aquellos que guardan en las agendas los números secretos de los cajeros, contraseñas de los PC de casa u oficina, mail, etc.

Ingeniería Social y Mail [2]

El mail es una forma de acercamiento a terceros que permite una cierta protección de la intimidad y el anonimato del Ingeniero Social si este toma unas mínimas precauciones. A través de él y mediante mensajes más o menos "simpáticos" llegan muchos virus.

Ingeniería Social y WEB [2]

Con una conexión a Internet se lleva acabo los ataques a los datos privados se instalan programas que capturan las pulsaciones del teclado o virus que secuestran el computador y envían información, realizan un contacto con la victima por cualquier medio como por ejemplo un mensaje en el cual al abrir cualquier vínculo automáticamente se da acceso al ordenador.

IRC y otros chats [2]

Los chats son los lugares de la red donde más información se puede obtener utilizando técnicas de ingeniería social. Los chats en los que grupos de usuarios conversan de forma más o menos anónima, favorecen el acercamiento y la charla intima y sobre todo, es en ellos donde las personas bajan más la guardia. A veces los ratos de charla son largos y es difícil estar siempre alerta. Además de todo ello es verdaderamente sencillo crearse una o varias personalidades falsas que pueden utilizarse según la persona o personas a las que se quiere investigar.

IS y Videoconferencia [2]

Entendemos ya todo el hecho de que la razón de la IS es la obtención de la información. En muchos casos, esta se consigue sin conocimiento de la persona cuya información se está aprovechando. Sin embargo, no siempre es así. Hay una forma de actuación asociada a este tipo de aplicaciones que permiten no solo escribirnos sino también ver y oír a nuestro interlocutor, esta forma de actuación es el chantaje.

Una de las aficiones de muchos de los usuarios de estas aplicaciones es el practicar cibersexo. Así 2 personas se ven mientras "hacen sus cosas". En esta situación es muy sencillo grabar imágenes fijas o incluso la sesión completa. Una vez

guardadas en el disco se utilizan como forma de extorsión a personas casadas o con responsabilidades para las personas que realizan estas prácticas puede ser un verdadero problema.

Ingeniería Social y teléfono [2]

El teléfono es el medio predilecto de los ingenieros sociales. Seguramente donde se originó el término y donde más ataques de este tipo hay documentados. El uso ofrece ventajas con respecto a otros:

La ocultación de número permite, en un primer momento, mantener el anonimato de una manera simple.

Permite además actuar a distancia, incluso desde otro país, lo que hace difícil la captura del Ingeniero Social.

La voz ofrece muchísima información a quienes practican ingeniería social. Datos acerca del estado de ánimo del interlocutor, o si es un profesional del medio (teleoperadores, etc.).

Esto lo convierte en el elemento más utilizado para obtener información de forma no presencial.

Técnicas presenciales no agresivas [2]

Se llama así cuando lo que se desea es llegar de cualquier manera a la información, sin el control de visitas a edificios, o acceso a datos sin permiso alguno, es permitir el ingreso de cualquier persona.

Buscando en la basura, siguiendo personas y vehículos, Vigilando Edificios, Ingeniería social en situaciones de crisis

Métodos agresivos [2]

Esta técnica permite realizar la búsqueda de información que se la consigue sin conocimiento de la persona, usando tácticas y métodos que ya involucre a la persona de manera directa.

Suplantación de personalidad, Chantaje o extorsión y Presión psicológica.

IV. Como Protegerse

El personal de una empresa debería de seguir las siguientes recomendaciones para evitar caer víctima en las trampas de la Ingeniería Social [3]:

1. - Antes de abrir los correos analizarlos con un antivirus eficaz y debidamente actualizado, ya que cualquier mensaje de correo electrónico puede contener códigos maliciosos aunque no le acompañe el símbolo de datos adjuntos.

2. -Nunca ejecutar un programa de procedencia desconocida, aun cuando previamente sea verificado que no contiene virus. Dicho programa puede contener un troyano o un Sniffer que reenvíe nuestra clave de acceso.

3. - Los usuarios no necesitan tener acceso a todo tipo de ficheros ya que no todos son necesarios para el trabajo habitual, por ello puede ser conveniente por parte del administrador bloquear la entrada de ficheros con extensiones ".exe", .vbs", etc.

4. - Nunca informe telefónicamente de las características técnicas de la red, la localización espacial o personas a cargo de la misma. Debe remitirlos directamente al responsable del sistema.

5.- Controlar los accesos físicos al lugar donde se hallan los servidores o terminales desde los que se puede conectar con los servicios centralizados de control.

6.- Nunca tirar documentación técnica a la basura, sino destruirla.

7.- Verificar previamente la veracidad de la fuente que solicite cualquier información sobre la red, la localización en tiempo y espacio y las personas que se encuentran al frente de la misma.

8.- En caso de existir, instalar los parches de actualización de software que publican las compañías para solucionar vulnerabilidades. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.

9.- Controlar que las anteriores instrucciones se cumplen sistemáticamente.

V. Conclusiones

La principal defensa contra la Ingeniería Social es sensibilizar, educar y entrenar a las personas en el uso de políticas de seguridad. Dude siempre de las redes sociales, correos electrónicos y otros canales de comunicación ya que son fuentes de información para un Ingeniero Social. Lo que no se debe hacer es ponerle al Ingeniero Social nuestra información en bandeja de plata.

Asegure sus dispositivos, protéjalos con herramientas de antivirus, configuración de firewall, estar alerta con las noticias de ataques informáticos y desconfíe cuando le soliciten, valide o envié los datos personales.

Como dijo Kevin Mitnick "*Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresan sin más. Tienen todo en sus manos."* [4]

Allan Vance *"La gente quiere ser agradable y no pretende armar un escándalo, pero es importante enseñarles a decir no. No debe haber sutilezas cuando lo que está en juego son nuestros ingresos."* [5]

Sus conocimientos en seguridad informática y medidas preventivas son su mayor defensa, ninguna institución bancaria, agencia de crédito o gubernamental lo va a proteger a usted mejor que usted mismo.

REFERENCIAS

[1] Familiarizándonos con la Ingeniería Social. (2010, Jun 16). [Online]. Available: http://seguridadinformacioncolombia.blogspot.com/2010/06/fundamentos-de-ingenieria-social.html

[2] INGENIERIA SOCIAL 1.0. [Online]. Available: http://www.scribd.com/doc/7215979/Texto-Ingenieria-Social

*[3]*Ingeniería Social (Parte 1). (2006, Sept 25). [Online]. Available: http://zameexweb.blogcindario.com/2006/09/00065-ingenieria-social-parte-1.html

[4] Referencias de libros:
Libro **El arte de la intrusión:** la verdadera historia de las hazañas de hackers, intrusos e impostores -Kevin Mitnick (2002)
http://www.angelux.net/2008/04/12/el-arte-de-la-intrusion-como-ser-un-hacker-o-evitarlos-kevin-d-mitnic.html

[5] Documental "Piratas Informáticos", Discovery Channel. (2010 Mar 10). [Online]. Available: http://ucctelecom.blogspot.com/2009/12/documental-piratas-informaticos.html

Autores
Breve referencias sobre la formación académica del autor y su experiencia.

Elaborado por:

Catherine Suárez Rodríguez
Ingeniero Electrónico
Ingeniero de Planeación y sistemas del INC
Universidad Los Libertadores 2002

Elaborado por:
Lourdes S. Barbosa Castillo
Ingeniero de Sistemas
Ingeniero VASS Consultoría de Sistemas
Universidad Piloto de Colombia 2010