FALENCIAS DE LA SEGURIDAD INFORMÁTICA.

Moreno, Ruby., Mahecha, Alexandra.
Rubalex24@hotmail.com
Universidad Piloto de Colombia

Resumen—Esta vez abordaremos el tema de la Ingeniería Social enfocada al área de contacto con los usuarios internos o externos de la compañía cuando se tienen problemas con los diferentes elementos que integran la tecnología de la información, el Help Desk y desafortunadamente la falta de capacitación en el tema, el desconocimiento del personal que realiza el primer nivel de soporte y la política en la agilidad en la atención de estos servicios hace que esta área sea la más vulnerable a los ataques informáticos.

Índice de Términos— Help Desk, Ataques Wiki y suplantación

I. INTRODUCCIÓN

Este tipo de ataque es el más usual; ya que el contacto es más rápido y fácil de realizar. Un atacante puede llamar haciéndose pasar por un funcionario de la empresa y obtener información o brindando ayuda prestando soporte técnico para obtener información privilegiada; la cual pueda ser explotada para encontrar nuevas vulnerabilidades y poner la empresa en riesgo.

II. ATAQUES A EXPERTOS

El SANS 2013 Help Desk Security and Privacy Survey publicado recientemente señalaba que las tareas principales de los agentes de Help Desk es atender las peticiones de los empleados y otras relacionadas con los incidentes en los pc y restablecimiento de password.

Los agentes de Help Desk están entrenados para ser amables, completar, resolver o transferir el mayor número de llamadas posible; destaca el informe. Pero un tercio de los profesionales de TI

(Tecnologías de la Información). Encuestados reconocieron que tenían una formación muy débil en gestión de riesgos y seguridad, ellos afirman que la capacitación de su personal de Help Desk no es la más apropiada, un 5% no tenía ninguna capacitación y un 6% no sabía sobre seguridad.

El 70% de los encuestados reconocieron que los ataques de "ingeniería social" en los que alguien trata de conseguir información sensible o password de los agentes del Help Desk, suponen un riesgo significativo.

Los agentes de Help Desk, que pueden tener acceso a fuentes de información corporativa sensible, suelen estar medidos por métricas de productividad y rapidez, lo que significa que los agentes están bajo presión para trabajar con rapidez. Y los Help Desk están a menudo faltos de personal. "Como resultado un agente puede ignorar requerimientos de calidad y conformidad para poder cumplir los objetivos de cantidad y puntualidad" destaca el informe SANS.

El informe también hace notar que las posiciones de entrada del Help Desk no están particularmente bien pagas, y existe una alta rotación de personal, con cifras cercanas al 30 o 40 por ciento.

La automatización de operaciones del Help Desk es en general bastante bajo. Menos de la mitad de los

encuestados dijeron tener algún tipo de herramientas de autenticación de usuarios o de autorización. El Help Desk está "lejos de ser uno de las áreas críticas en el presupuesto corporativo" indica el informe SANS. Alrededor de un cuarto de los profesionales de TI (Tecnologías de la Información). Encuestados afirmaron haber tomado en consideración el coste de tener un incidente de seguridad a la hora de establecer el presupuesto del Help Desk, pero la mayoría no.

Teniendo las anteriores observaciones se deben fortalecer las políticas de contratación, como son la capacitación, los salarios, la rotación del personal, los procedimientos, los escalamientos, las aplicaciones para el registros de los incidentes que indiquen la naturaleza y la solución del mismo para que se realicen los diferentes ajustes para que el número de incidentes reportados sean menores o que sean diferentes a los que se han reportado anteriormente; esto para que la seguridad de la información y las políticas, normas, estándares y procedimientos estén acordes a la estrategia de seguridad de la información.

A continuación se realizara una breve descripción de ataques de ingeniería social, comenzando por el método de "autoridad falsa" técnica que es usada muy a menudo y se basa en intentar convencer a la victima de que el atacante está en una posición en la que esa información le es necesaria haciéndose pasar por un superior.

Está técnica puede ser usada en empresas muy grandes, donde lo más normal es que un empleado no conozca a todos sus superiores, por lo que un atacante puede hacerse pasar por un superior y solicitar la información que necesite. Por tal razón no es necesario hacer muchos esfuerzos para que el atacante consiga dicha información.
Un ejemplo de este tipo de ataques podría ser el siguiente:

Supongamos que un atacante entra a una compañía de software y se hace pasar por un empleado del departamento de seguridad, y explica a los jefes que tiene que instalar un nuevo archivo para evitar que los pc de todos los empleados se infecten con un virus que acaba de salir y que para hacer esto es necesario que los empleados le faciliten las contraseñas de acceso a sus pc, con lo que el atacante ya podría hacer lo que quisiera con los pc de los empleados.(Es muy utilizada en empresas de más de 50 empleados).

Aunque es un ejemplo muy simple, podemos ver que el atacante haciéndose pasar por otra persona ha conseguido con relativa facilidad las contraseñas de todos los empleados de la empresa.

A continuación, un listado de los ataques más comunes y algunas estrategias para lograr prevenirlos:

1) Al teléfono: Suplantación de Identidad, para impedirla hay que entrenar a los empleados para que nunca entreguen información confidencial por teléfono y que se implemente una política como por ejemplo solicitar el número de identificación del funcionario que solicita el servicio.

2) Acceso a las instalaciones: Acceso no autorizado, para prevenirlo hay que disponer de un equipo de vigilantes con entrenamiento en seguridad para todos los empleados y establecer procedimientos para el acceso físico a las diferentes áreas de la compañía.

3) En la oficina: Se evita teniendo precaución al escribir usuarios y/o contraseñas cuando alguien este observando, o si hay que hacerlo, que sea muy rápido y no olvidar tomar la precauciones necesarias.

4) En los Help Desk: Suplantación de identidad, para minimizar este riesgo hay que asignarle a cada empleado un PIN o Token de seguridad el cual permita comprobar la identidad de la persona que llama.

5) En las instalaciones de la oficina: Visitantes sin acompañamiento de ningún funcionario, para evitar problemas se debe exigir acompañamiento en todo momento a los visitantes cuando estén en las instalaciones de la Organización.

6) Centros de cómputo: Intentos de acceso, de extraer equipos o de ingresar elementos que puedan capturar información confidencial. Se recomienda contar con un centro de cómputo bajo controles de

acceso biométricos actualizados al igual que los inventarios, todos los equipos que se encuentren allí almacenados, como también vigilancia por cámaras monitoreadas.

7) Canecas de basura: Se debe contar con trituradoras de papel, y de procedimientos de borrado de información adecuados.

8) Intranet/Internet: Inserción de keyloggers[1] para obtener nombres de usuario y contraseñas, para evitarlo hay que hacer rutinas de mantenimiento de las redes, así como dar entrenamientos a los empleados en la creación de contraseñas fuertes es decir contraseñas Alfanuméricas.

9) Correo electrónico: Se debe contar con procedimientos avalados por el área para que las solicitudes sean autorizadas por el jefe inmediato del funcionario que solicita el respectivo soporte.

10) Comunicaciones por Lync: Estas también se deben verificar y autenticar según los requerimientos que se soliciten por este medio.

11) Teléfonos móviles: El 50% de redes sociales revela información confidencial

A) Ingeniería social factor humano

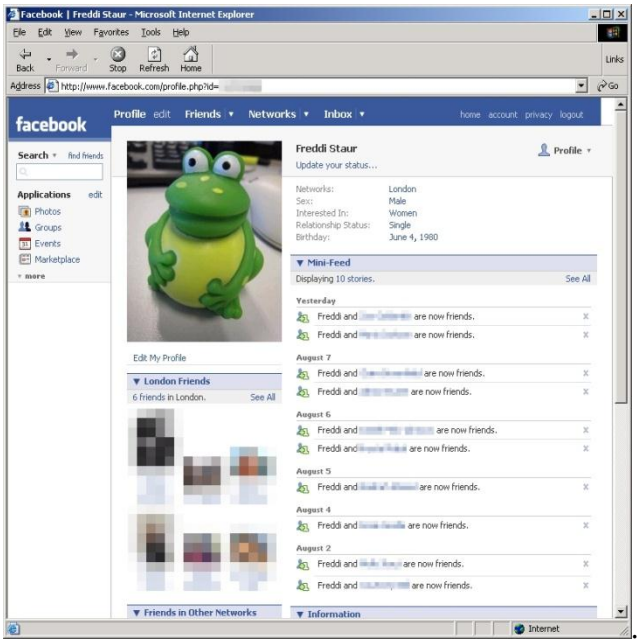

Figura 1. Ingeniería social factor humano – Imagen tomada de red social personal

[1] Keyloggers: Suele usarse como malware, permitiendo que Otros usuarios tengan acceso a contraseñas importantes como Tarjetas Crédito etc…

1) *Tenga en cuenta:* Cambie las opciones de privacidad. No Publique información sensible y la que publique, revise que sea visible solo a su círculo de amigos.

- No publique su árbol familiar para que no sea ubicado su entorno.

- Tenga cuidado con la información que revela en las "redes sociales" de Internet.

- Supervise el acceso y los contactos de sus hijos, recuerde ellos pueden ser su punto más débil.

- No publique información relativa a su empresa o a las funciones que desempeña.

- El 41% de los usuarios de Facebook revela información personal a cualquiera (Fuente SOPHOS)

2) *Recomendaciones*

Es muy importante capacitar al usuario (empleado y superiores) en reconocer a este tipo de personas, siempre se le debe solicitar la identificación, y preferentemente tener un protocolo de trabajo (por ejemplo si se realizará una actualización de software, enviar 24hs antes un email a todos los empleados avisando que pasará el técnico a realizar el trabajo.)

B) "Suplantación"

Aunque se parece mucho a una autoridad falsa, no es lo mismo, es decir, la suplantación se parece a la autoridad falsa en el hecho de que se intenta engañar a una persona haciéndose pasar por alguien que tiene más privilegios en el sistema.

La diferencia radica que la suplantación se basa en hacerse pasar por una persona que realmente existe. En esta técnica el atacante se hace pasar por otra persona de distintos modos, por ejemplo podría imitar la voz de la persona a suplantar, usar un chat

o incluso imitar su estilo de escritura leyendo sus correos, es decir, que un atacante podría recopilar información confidencial de una persona y hacerse pasar por ella.
Una vez que el atacante ha conseguido convencernos que es quien dice ser, sólo le quedará pedirnos la información que desea obtener para acceder a nuestros sistemas.

1) Recomendaciones

Es muy importante capacitar al usuario (empleado y superiores) en reconocer a este tipo de personas, nunca se debe dar información confidencial por chat ni por teléfono, se debe seguir un protocolo de seguridad de trabajo .El peor error de las empresas es confiar en que nunca les sucederá.

Por ejemplo si se debe entregar información confidencial esta debe ser personalmente, si debe ser enviada por email se debe encriptar, y si es un archivo por chat, debe estar comprimido y encriptado con claves de acceso que las dos personas conocen o compartan.
Hay muchas técnicas más de ingeniería social que un cracker o timador pueden utilizar para obtener información confidencial.

C) "Ataque telefónico"

Las empresas grandes generalmente tercerizan el servicio de Help Desk, es normal que haya cambios de personal sin que la empresa lo sepa y allí es donde se presenta la vulnerabilidad.

1) Recomendación

Solicitar siempre a la empresa una lista actualizada de empleados activos y recordarles a los empleados quien es su Help Desk semanalmente.

D) Ingeniería social" On-Line

De todas las formas anteriormente expuestas, la "Ingeniería social On-Line" es quizás la que se practica con mayor frecuencia. Los medios por excelencia donde se dan este tipo de ataques, suelen ser los canales de IRC[2] dedicados a los principiantes del chat. La información recopilada no es demasiado importante, pero seguramente a quien la obtuvo, le proporcionara un tiempo valioso de conexión para seguir con sus Crackers, así como una cuenta "limpia" desde la cual actuar.

No debemos descartar que ataques de este tipo pudieran ser perpetrados incluso en pequeñas corporaciones con un esquema de seguridad absolutamente deficiente, los cuales dejen libradas las conexiones de Internet de sus dos o tres empleados.

1) Recomendación

Trata de no hablar de más con personas que no conoces, nunca sabes quién está del otro lado.

III. CONCLUSIONES

Las Estadísticas indican que en la mayoría de los ataques, el punto de partida inicia con la Ingeniería Social.

Ley 1273: Tipifica la integridad, confidencialidad, disponibilidad de la protección de Datos, pero no se toma en cuenta la más alta vulnerabilidad de los datos "La Ingeniería Social". [A]

REFERENCIAS

[A] ley 1273, Secretaria de Senado de la Republica, Delitos Informáticos, 2009, www.secretariasenado.gov.co

[B] Revista SANS, España, www.sans.org

Autor

Ruby Alexandra Moreno Mahecha, aspirante al título de Especialista en Seguridad Informática – Universidad Piloto de Colombia.

"Este documento fue redactado en base a mi experiencia Profesional, la cual espero sirva para transmitir las falencias de la Seguridad Informática en nuestro país. "

[2] IRC: Canal de Comunicaciones en tiempo real en la cual pueden hablar usuarios al mismo tiempo (Chat interno.)