Ingeniería Social

Ciberseguridad (CIB)

©Ismael Ripoll

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

December 4, 2023

Índice

1. Principios de ataque
2. Motivaciones intrinsecas
3. Vectores de ataque
4. Sicología de los ataques
5. Herramientas
6. Protección

Definición

Definition

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

- La ingeniería social es otra herramienta más a disposición de los atacantes, donde el objetivo atacado es una persona en lugar de un programa.
- Puesto que las personas son el “weakest link” de los sistemas informáticos, los ataques a las personas suelen ser más fáciles.
- Se busca utilizar las “debilidades” de las personas, sin que estás sean conscientes.
- En caso de ser conscientes, ya pasaría a ser extorsión, chantaje, tortura, etc.

Principios generales de manipulación

Autoridad El atacante suplanta un cargo de autoridad (o se comporta como si la tuviera), para que se acaten sus ordenes.

Aprobación social Ser aceptado por el grupo es una de las fuerzas que más determinan el comportamiento de las personas. Esta técnica se usa mucho en la publicidad.

Escasez Fomentar el miedo a la fata de algún bien o servicio. La frase “hasta fin de existencias” es una forma de generar atención y deseo sobre algo.

Urgencia Las personas damos más importancia a las cosas urgentes que a las importantes. Se suelen combinar urgencia con escasez, para no dar tiempo a pensar.

Confianza Solemos valorar y aceptar mejor las opiniones de la gente que conocemos.

Principios sicologios de la ingeniería social (I)

Afecto fuerte: se aplica cuando el ciberdelincuente hace una declaración o proporciona información que desencadena emociones fuertes. Si la víctima siente una fuerte sensación de sorpresa, anticipación o enojo, entonces será menos probable que reflexione sobre los que se le dice y por tanto pueda razonar lógicamnete.

Sobrecarga: ocurre cuando se le da demasiada información demasiado decrisa. Las víctimas absorben la información en lugar de evaluarla, lo que hace que acepten los argumentos y revelen la información solicitada.

Reciprocidad: se basa en la premisa de que si alguien nos da algo o nos promete algo, debemos devolverle el favor.

Principios sicologios de la ingeniería social (II)

Relaciones engañosas: se puede aplicar cuando existe una relación de confianza. Cuando un ciberdelincuente y una víctima tienen características similares, se proporciona un fuerte incentivo para que la víctima ayude al ciberdelincuente. También se puede conseguir hablando sobre un enemigo común.

Difusión de responsabilidad: se produce cuando se hace sentir a las víctimas que no se les puede responsabilizar por sus acciones, y que están tomando decisiones que marcarán la diferencia entre el éxito o el fracaso de la empresa.

Autoridad: es muy común, porque las personas están condicionadas a responder con cumplimiento a la autoridad.

Principios sicologios de la ingeniería social (III)

Integridad y coherencia: se aplican cuando las personas tienden a creer que otros están expresando sus verdaderas actitudes cuando hacen una declaración. La tendencia a creer en los demás se basa principalmente en la propia honestidad al expresar sus sentimientos.

Jayanth Kancherla "Motivational and Psychological Triggers in Social Engineering" Georgia Institute of Technology

Motivaciones

Generales:

- Dinero.
- Sexo (diversión)
- Ideología.
- Amor (a la pareja o a la familia).

De los hackers:

- Dinero.
- Ego (reconocimiento técnico).
- Diversión (Sexo, juego, etc.)
- Ideología.
- Pertenencia a grupo.
- Estatus (atacar a grandes).

Vectores de ataque

La terminología es muy variada.

Phishing Enviar mail o sms con un mensaje “atractivo”. Es una envío masivo del mismo mensaje a un gran número de targets esperando que alguno “piquen”.

Spear phishing La diferencia está en la personalización del mensaje. En este caso se escribe con información específica para la victima.

Whaling (ballena) Igual que el spear phishing pero cuando el objetivo es un “pez gordo”. El trabajo del atacante pasa por localizar a los CEOs de las empresas y optimizar el lenguage utilizado.

Tail gate Colarse en un edificio detrás de otra persona.

Baiting (anzuelo) Dejar objetos o mails que no van dirigidos a la víctima de forma explicita pero que casualmente acaba en sus manos.

Sicología de los ataques

- Gánate su confianza. Compartir escalas de valores.
- Existe algún problema externo al atacante que requiere de una acción rápida.
- Al atacante puede tomar el rol de ser el débil. Esto es, no es una amenazada, sino el amenazado.
- Pedir (o hacer) un favor crea vínculos emocionales.
- Ser progresivo en las peticiones. Empezar por algo que sea fácil (y legal).
- Hay que intentar no desvelar los auténticos objetivos del ataque. No se pregunta directamente por lo que se busca.

Herramientas

Estás herramientas están incluidas en Kali Linux.

- SET (Social Engineering Tookit): Construir exploits contra personas (generar mails de phishing, man in de middle, ...).
- Maltego: Busca y organiza información en base a OSINT de una persona o empresa. Necesario antes de iniciar un ataque de ingeniería social.

Por ejemplo, para hacerse pasar por un instalador de telefónica es necesario conocer la jerga, procedimientos, indumentaria, etc.

Protección

- Estar concienciado -> No abrir correos no solicitados Y menos ficheros desconocidos.
- Establecer separaciones físicas y lógicas entre los datos externos y los internos.
  - Puesto que el mail es el principal vector de ataque, leer el mail en una sandbox.
  - Utilizar diferentes ordenadores para manejar información con distinto grado de importancia. Yo uso varias máquinas virtuales (y físicas).
- Desconfiar de lo que parezca demasiado bueno. Es mejor dejar pasar una oportunidad a comerse 20 ataques.
- Las prisas sobrevenidas (las que no has generado tú) hay que tomárselas con calma.
- Cuidado con aquellos que dicen compartir tus mismas inquietudes. Por si se está utilizando el principio de la familiaridad.