Administración de Sistemas de Información

Unidad IV: Ingeniería Social

Grupo 6

2024

Integrantes:

- **Calcagno, Matías**
- **de los Ríos, Carolina**
- **Haudet, Felipe**
- **Ortiz, Lucas**

Introducción

La ingeniería social es una técnica utilizada para manipular a las personas con el fin de obtener información confidencial, acceso no autorizado a sistemas o provocar la ejecución de ciertas acciones. A diferencia de los ataques puramente técnicos, la ingeniería social se basa en la explotación de la confianza, la empatía o la curiosidad de las personas. Este método es altamente efectivo debido a la vulnerabilidad inherente del ser humano, ya que incluso los sistemas más seguros pueden ser comprometidos si los usuarios son engañados para entregar información o realizar acciones inapropiadas.

Desarrollo

Los atacantes de ingeniería social manipulan las emociones, la confianza y la falta de conocimiento de sus víctimas, generalmente a través de engaños que parecen inofensivos o rutinarios. Estos engaños pueden tomar muchas formas, pero todos ellos aprovechan la psicología humana en lugar de las vulnerabilidades tecnológicas.

Tipos de ataque en la Ingeniería Social

Los ataques pueden presentarse de varias formas. A continuación, se describen los tipos más comunes:

1. **Phishing:** El phishing es una de las formas más comunes de ingeniería social. En este ataque, el atacante envía correos electrónicos falsos o mensajes que parecen provenir de fuentes confiables, como bancos, redes sociales o colegas de trabajo. El objetivo es que la víctima haga clic en un enlace malicioso o proporcione información confidencial, como contraseñas o números de tarjetas de crédito.

2. **Spear Phishing:** Similar al phishing, pero más dirigido y personalizado. En lugar de enviar mensajes a una amplia audiencia, el atacante investiga a una persona o empresa en particular y adapta el mensaje para que parezca legítimo. Esto puede involucrar información específica que solo un individuo objetivo podría reconocer, aumentando la efectividad del ataque.

3. **Pretexting:** En este tipo de ataque, el atacante crea un escenario falso para engañar a la víctima y lograr que revele información o realice una acción. Esto puede incluir hacerse pasar por un empleado de soporte técnico, un funcionario gubernamental, o un colega de trabajo para obtener acceso a datos sensibles.

4. **Baiting:** El baiting implica atraer a la víctima a través de la promesa de algo atractivo. Por ejemplo, un atacante podría dejar una memoria USB maliciosa en un área pública esperando que alguien la recoja e inserte en su computadora, desencadenando la instalación de malware.

5. **Tailgating:** También conocido como “piggybacking”, el tailgating implica seguir físicamente a alguien para entrar en un área restringida sin el acceso adecuado. El atacante puede aprovechar la cortesía natural de las personas para colarse detrás de un empleado en un edificio asegurado.

6. **Vishing (Phishing por voz):** Esta variante de phishing utiliza llamadas telefónicas para engañar a las víctimas. Los atacantes se hacen pasar por figuras de autoridad o soporte técnico para obtener información personal o financiera. Las estafas por voz han aumentado con el uso de tecnologías de VoIP que permiten ocultar el origen real de las llamadas.

Fases de un Ataque de Ingeniería Social

Un ataque de ingeniería social suele pasar por varias fases. Comprender estas etapas ayuda a las organizaciones a identificar y prevenir ataques:

1. **Investigación:** El atacante recopila información sobre la víctima. Esto puede incluir datos personales, patrones de comportamiento, correos electrónicos, jerarquía dentro de una empresa, entre otros. A menudo, esta información se obtiene de redes sociales, sitios web de empresas o filtraciones previas de datos.

2. **Desarrollo de la relación:** En esta fase, el atacante establece contacto con la víctima, ganando su confianza. Este contacto puede ser a través de correos electrónicos, llamadas telefónicas o encuentros personales.

3. **Explotación:** Una vez que el atacante ha ganado la confianza de la víctima, explota esa relación para extraer la información deseada o realizar alguna acción, como proporcionar acceso a un sistema o descargar un archivo malicioso.

4. **Cierre:** Después de haber obtenido lo que necesitaba, el atacante corta el contacto para evitar levantar sospechas. Sin embargo, en algunos casos, el atacante puede continuar manipulando a la víctima para obtener más información.

Técnicas y Psicología Detrás de la Ingeniería Social

La ingeniería social se basa en ciertos principios psicológicos para ser efectiva. Algunas de las técnicas psicológicas más utilizadas incluyen:

1. **Autoridad:** Los atacantes se hacen pasar por figuras de autoridad, como ejecutivos, agentes del gobierno o personal de TI, para convencer a las víctimas de que sigan sus instrucciones sin cuestionarlas.

2. **Urgencia:** La creación de un sentido de urgencia puede llevar a las víctimas a tomar decisiones precipitadas sin pensar en las consecuencias. Un atacante podría alegar que si la víctima no actúa de inmediato, habrá consecuencias graves, como la pérdida de datos o la suspensión de servicios.

3. **Simpatía:** El atacante puede crear un escenario donde la víctima sienta lástima o empatía hacia ellos, lo que facilita la manipulación. Por ejemplo, pueden pedir ayuda haciéndose pasar por alguien que está en apuros.

4. **Reciprocidad:** Las personas tienen una tendencia a devolver favores. Un atacante podría ofrecer un pequeño regalo o asistencia con la esperanza de que la víctima se sienta obligada a devolver el favor entregando información.

5. **Conformidad social:** Este principio explota el deseo de las personas de encajar o seguir la norma social. Un atacante podría convencer a la víctima de que todos en su organización están siguiendo ciertas políticas o procedimientos falsos para obtener acceso.

Prevención de la Ingeniería Social

Dado que los ataques de ingeniería social dependen principalmente de explotar el comportamiento humano, la prevención se enfoca en educar y concienciar a las personas y organizaciones. Algunas medidas clave incluyen:

1. **Educación y Concienciación:** La capacitación regular de los empleados sobre las tácticas de ingeniería social es crucial. Las simulaciones de phishing y los seminarios sobre ciberseguridad pueden ayudar a los usuarios a identificar y evitar caer en estos tipos de ataques.

2. **Verificación de Identidades:** Las políticas de seguridad deben requerir la verificación de identidades antes de compartir información confidencial o

proporcionar acceso a sistemas. Esto incluye la verificación en múltiples etapas y el uso de autenticación de dos factores (2FA).

3. **Políticas de Acceso y Contraseñas:** Limitar el acceso a la información y recursos basados en roles y la implementación de políticas de contraseñas seguras puede reducir el impacto de los ataques de ingeniería social. También es útil asegurarse de que los empleados no compartan contraseñas o credenciales de forma abierta.

4. **Seguridad Física:** Implementar medidas de seguridad física, como el uso de tarjetas de acceso y sistemas de vigilancia, puede evitar que los atacantes utilicen técnicas como el tailgating para obtener acceso no autorizado a instalaciones.

5. **Pruebas Regulares de Seguridad:** Las organizaciones deben realizar auditorías y pruebas de penetración para evaluar la efectividad de sus medidas de seguridad contra la ingeniería social.

Conclusión

La ingeniería social es una amenaza constante en el panorama de la ciberseguridad. Al aprovecharse de la psicología humana, los atacantes pueden eludir incluso las barreras técnicas más avanzadas. Para mitigar este riesgo, las organizaciones deben enfocarse en la concienciación, la formación y la implementación de medidas preventivas tanto a nivel humano como técnico. Aunque no se puede eliminar por completo el riesgo de ingeniería social, una estrategia integral puede reducir significativamente su impacto.

Bibliografía

- IBM. (s.f.). **Social engineering**. IBM. Recuperado el 8 de octubre de 2024, de: https://www.ibm.com/es-es/topics/social-engineering
- Argentina.gob.ar. (s.f.). **Qué es la ingeniería social y cómo protegerte**. Ministerio de Justicia y Derechos Humanos de la Nación. Recuperado el 8 de octubre de 2024, de: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte
- Cloudflare. (s.f.). **What is a social engineering attack?**. Cloudflare. Recuperado el 8 de octubre de 2024, de: https://www.cloudflare.com/es-es/learning/security/threats/social-engineering-attack/