-HABLEMOS DE Ingenieria Social-

Ingeniería social: definición

La ingeniería social es una técnica utilizada por atacantes informáticos para manipular a las personas y obtener información confidencial o acceso a sistemas informáticos. En lugar de explotar vulnerabilidades técnicas, se aprovecha de la psicología humana y la interacción social.

Los ingenieros sociales suelen emplear estrategias persuasivas, como la manipulación emocional, la suplantación de identidad o la creación de escenarios convincentes para

engañar a las víctimas y obtener información sensible, contraseñas o acceso a sistemas corporativos.

Esta forma de ataque se basa en la confianza, el engaño y la manipulación, y puede ocurrir a través de diferentes medios, como correos electrónicos, llamadas telefónicas, mensajes de texto o interacciones en redes sociales.

Cómo funciona la ingeniería social y cómo protegerte

Casi todos los tipos de ataques conllevan algún tipo de ingeniería social. Por ejemplo, están los clásicos correos electrónicos de "phishing" y estafas de virus, con un gran contenido social. Los correos electrónicos de phishing intentan convencer a los usuarios de que su origen es legítimo con la esperanza de obtener información personal o datos de la empresa, por insignificante que parezcan. Por otra parte, los correos que contienen archivos adjuntos con virus a menudo aparentan provenir de contactos confiables u ofrecen contenido multimedia que parece inofensivo, como videos "divertidos" o "tiernos".

En algunos casos, los atacantes utilizan métodos más simples de ingeniería social para acceder a una red o computadora. Por ejemplo, un hacker puede frecuentar el comedor público de un gran edificio de oficinas, buscar usuarios que estén trabajando en sus tablets o computadoras portátiles y mirar los dispositivos por encima de su hombro. Con esta táctica pueden conseguir una gran cantidad de contraseñas y nombres de usuario, todo sin necesidad de ni enviar un solo correo electrónico ni escribir una línea de código de virus.

Otros ataques requieren una comunicación real entre el atacante y la víctima; en estos casos, el atacante presiona al usuario para que le otorgue acceso a la red con el pretexto de un problema grave que es necesario resolver de inmediato. Los atacantes utilizan en igual medida la rabia, la culpa y la tristeza para convencer a los usuarios de que necesitan su ayuda y no pueden negársela.

Para terminar, es importante prestar atención a la ingeniería social como un medio para crear confusión. Numerosos trabajadores y consumidores no se dan cuenta de que, con solo un poco de información (como el nombre, la fecha de nacimiento o la dirección), los hackers pueden acceder a múltiples redes haciéndose pasar por usuarios legítimos o miembros del personal de TI. Después de lograrlo, les resulta fácil restablecer contraseñas y obtener acceso prácticamente ilimitado.

La protección contra la ingeniería social comienza con la educación; los usuarios necesitan aprender que no deben hacer nunca clic en enlaces sospechosos y siempre deben proteger sus credenciales de inicio de sesión, incluso en la oficina y en el hogar. Sin embargo, si las tácticas sociales logran su objetivo, el resultado probable es una infección por malware. Para combatir los rootkits, troyanos y otros bots, es fundamental implementar una solución de seguridad de Internet de alta calidad que sea capaz de eliminar infecciones y rastrear su origen.

Casi todos los tipos de ataques conllevan algún tipo de ingeniería social. Por ejemplo, están los clásicos correos electrónicos de "phishing" y estafas de virus, con un gran contenido social. Los correos electrónicos de phishing intentan convencer a los usuarios de que su origen es legítimo con la esperanza de obtener información personal o datos de la empresa, por insignificante que parezcan. Por otra parte, los correos que contienen archivos adjuntos con virus a menudo aparentan provenir de contactos confiables u ofrecen contenido multimedia que parece inofensivo, como videos "divertidos" o "tiernos".

¿Cómo podemos protegernos de la ingeniería social?

No entregues datos personales a personas extrañas por teléfono, correos electrónicos o redes sociales.

Configurá la privacidad en las redes sociales para que no queden expuestos tus datos personales.

Informate y aprendé sobre este tipo de amenazas.

Usá una contraseña segura.

Configurá la autenticación en dos pasos para estar alerta de accesos indebidos a tus cuentas.

Prestá atención a cualquier persona que te pida información personal.