TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

Inacap

Ingeniería Social, Tipos de atacantes

Seguridad de la Información

Inacap

Ingeniería Social

La ingeniería social en seguridad de la información se refiere a un conjunto de técnicas manipulativas que los atacantes utilizan para engañar o influenciar a las personas con el fin de obtener acceso no autorizado a información, sistemas, recursos o servicios.

A diferencia de los ataques técnicos, que se enfocan en explotar vulnerabilidades de software o hardware, la ingeniería social se basa en explotar la psicología humana y las interacciones sociales para lograr los objetivos del atacante.

Dama, le habla Francisco Javier Pérez Cotapoh, ejecutivo de banca personas de Bancoestao.

Inacap

Casos comunes de ataques de ing. Social

Phishing	
Es uno de los métodos más comunes y consiste en el envío de correos electrónicos fraudulentos que parecen provenir de fuentes legítimas (como bancos, servicios en línea, o incluso compañeros de trabajo). El objetivo es engañar a la víctima para que revele información confidencial como contraseñas, números de tarjeta de crédito o información personal.	Spear Phishing: Es una forma más específica de phishing, donde el atacante personaliza el mensaje dirigido a una víctima específica, aumentando las probabilidades de que la víctima caiga en la trampa. Whaling: Es un tipo de phishing dirigido a altos ejecutivos o personas de gran importancia dentro de una organización (por ejemplo, directores generales o responsables financieros).

nacap

Casos comunes de ataques de ing. Social

Vishing (Poise Phishing)
Consiste en realizar llamadas telefónicas fraudulentas en las que el atacante se hace pasar por una entidad legítima (como un banco, una compañía de seguros o una autoridad) para obtener información sensible de la víctima, como números de tarjetas de crédito o datos bancarios.

Pretexting
El atacante crea una falsa narrativa o "pretexto" para obtener información de la víctima. Por ejemplo, el atacante puede hacerse pasar por un compañero de trabajo, un proveedor o incluso un miembro de la familia y pedir a la víctima que revele información confidencial.

nacap

Casos comunes de ataques de ing. Social

Baiting

Este tipo de ataque aprovecha la curiosidad de la víctima. El atacante ofrece algo atractivo (como un software gratuito, un archivo interesante o un dispositivo USB) para que la víctima lo descargue o lo use. Sin saberlo, la víctima puede estar introduciendo malware o divulgando información personal al hacerlo.

Quizzes o encuestas engañosas:

A menudo se difunden en redes sociales o a través de correos electrónicos que invitan a los usuarios a participar en encuestas o juegos. Estos cuestionarios pueden ser diseñados para obtener información personal de manera sutil y, en ocasiones, para descubrir las respuestas a preguntas de seguridad de cuentas (por ejemplo, "¿Cuál es tu mascota favorita?" o "¿En qué ciudad naciste?").

Casos comunes de ataques de ing. Social

Baiting

Este tipo de ataque aprovecha la curiosidad de la víctima. El atacante ofrece algo atractivo (como un software gratuito, un archivo interesante o un dispositivo USB) para que la víctima lo descargue o lo use. Sin saberlo, la víctima puede estar introduciendo malware o divulgando información personal al hacerlo.

Quizzes o encuestas engañosas:

A menudo se difunden en redes sociales o a través de correos electrónicos que invitan a los usuarios a participar en encuestas o juegos. Estos cuestionarios pueden ser diseñados para obtener información personal de manera sutil y, en ocasiones, para descubrir las respuestas a preguntas de seguridad de cuentas (por ejemplo, "¿Cuál es tu mascota favorita?" o "¿En qué ciudad naciste?").

Casos comunes de ataques de ing. Social

Tailgating

En el contexto físico, el tailgating es cuando un atacante sigue a una persona autorizada para acceder a un área restringida sin tener los permisos adecuados. Por ejemplo, el atacante puede aprovechar que alguien con una tarjeta de acceso válida entra en un edificio y luego "colarse" detrás de esa persona para no levantar sospechas.

nacap

Métodos utilizados por los atacantes de ingeniería social:

Manipulación psicológica

Los atacantes juegan con las emociones humanas, como la confianza, la urgencia o el miedo, para que la víctima actúe rápidamente sin pensar en las consecuencias.

Urgencia

Crean un sentido de urgencia, haciendo que la víctima sienta que necesita actuar de inmediato (por ejemplo, un correo que dice "su cuenta será bloqueada en 24 horas").

Confianza y autoridad

Se hacen pasar por figuras de autoridad o compañeros de confianza, lo que hace que las personas se sientan más inclinadas a confiar en ellos.

Curiosidad

Aprovechan la curiosidad de la víctima, ofreciendo algo que parece atractivo o interesante, pero que en realidad es una trampa.

nacap

Consecuencias de los ataques de ing. Social

Robo de información confidencial

La principal consecuencia es la obtención no autorizada de información personal o corporativa sensible, como contraseñas, datos bancarios o información de clientes.

Acceso no autorizado a sistemas

Los atacantes pueden obtener acceso a redes, sistemas y dispositivos, lo que podría resultar en el robo de datos, instalación de malware, o incluso el control completo de los sistemas.

Daño a la reputación

Un ataque exitoso de ingeniería social puede dañar la reputación de una organización, especialmente si los datos sensibles de clientes o empleados son comprometidos.

Pérdidas financieras

Los atacantes pueden usar la información obtenida para realizar transacciones fraudulentas, lo que puede resultar en pérdidas económicas para la organización o las personas afectadas.

Formas de prevención a los ataques de ing. Social

Educación y toma de conciencia

Entrenar a los empleados y usuarios sobre los riesgos de ingeniería social y cómo identificar correos electrónicos, llamadas o mensajes sospechosos es una de las mejores defensas.

Políticas claras en seguridad

Establecer procedimientos claros sobre cómo manejar la información sensible y garantizar que los empleados sigan buenas prácticas de seguridad, como la verificación de solicitudes antes de compartir datos.

Verificación de identidad

Siempre verificar las identidades de las personas que solicitan información o acceso, especialmente cuando se hacen por teléfono o correo electrónico. Usar múltiples métodos de autenticación (como la autenticación de dos factores) puede reducir el riesgo.

Formas de prevención a los ataques de ing. Social

Uso de tecnología de seguridad
Implementar herramientas como filtros de correo electrónico para bloquear mensajes de phishing, software antivirus para detectar malware y sistemas de detección de intrusiones para monitorear accesos no autorizados.
Simulacros de phishing:
Realizar simulacros internos de phishing y otros tipos de ingeniería social para educar a los empleados sobre cómo reconocer y manejar posibles ataques.
Seguridad Física
Limitar el acceso físico a las instalaciones y controlar el acceso a áreas restringidas para evitar el tailgating y otros tipos de intrusiones físicas.

Atacantes, caracterización

Cibercriminales (Cybercriminals)
Motivación: Económica. Buscan obtener beneficios financieros mediante actividades ilegales en línea.
Métodos: Usan técnicas como ransomware, fraude en línea, phishing, robo de datos y venta de información personal.
Objetivo: Obtener dinero directamente (a través de extorsión, fraude, etc.) o vender información robada en mercados ilegales.

Ejemplo: Un grupo de cibercriminales que lanza un ataque de ransomware a una empresa y exige un pago para liberar los datos secuestrados.

Atacantes, caracterización

Hackers (Piratas informáticos)
Motivación: Generalmente intelectual o de desafío personal. Buscan demostrar su habilidad técnica, acceso no autorizado o simplemente disfrutar del desafío de vulnerar sistemas.
Métodos: Utilizan una variedad de técnicas para obtener acceso a sistemas, como exploits, debilidades en software, ingeniería social, y acceso a redes.
Objetivo: Acceder a sistemas por el placer de demostrar su destreza técnica, muchas veces sin un propósito de lucro directo.

Un hacker que se infiltra en una red para robar información confidencial sin una intención de obtener ganancias económicas inmediatas.

Atacantes, caracterización

Tipos de hackers		
Black Hat	White hat	Grey Hat
Suelen estar motivados por beneficios financieros, venganza o incluso por el desafío personal. Buscan obtener acceso no autorizado a sistemas, robar datos sensibles, implementar ransomware, exfiltrar información confidencial o incluso realizar fraudes.	Los hackers "White Hat" (sombrero blanco) son profesionales de ciberseguridad que usan sus habilidades para proteger sistemas y ayudar a las organizaciones a identificar vulnerabilidades antes de que los Black Hats las exploten. Los White Hats trabajan dentro de los límites de la ley y a menudo realizan auditorías de seguridad y pruebas de penetración.	Los hackers "Gray Hat" (sombrero gris) están en una zona intermedia. Aunque no tienen malas intenciones, pueden realizar actividades que violan la ley (como entrar en un sistema sin permiso), pero no con el fin de causar daño directo o obtener ganancias. A menudo, informan sobre las vulnerabilidades que encuentran a las organizaciones afectadas.

Atacantes, caracterización

Hacktivistas
Motivación: Política o social. Los hacktivistas atacan para promover una causa política o social. Pueden estar motivados por cuestiones como los derechos humanos, la libertad de expresión, o la justicia social.
Métodos: Usan DDoS (ataques de denegación de servicio), defacement de sitios web (cambiar el contenido de una página web), o filtración de datos.
Objetivo: Llamar la atención sobre una causa, interrumpir servicios o exponer información confidencial que apoye sus ideales.

El grupo Anonymous realizando un ataque de DDoS a gobiernos o corporaciones para protestar por políticas que consideran injustas.

Atacantes, caracterización

Actores Estatales (Ataques patrocinados por gobiernos)
Motivación: Política y estratégica. Estos atacantes son patrocinados por gobiernos y suelen estar involucrados en actividades de ciberespionaje, desinformación, y guerra cibernética.
Métodos: Utilizan técnicas avanzadas y personal altamente cualificado para realizar ataques sofisticados, como phishing dirigido, malware personalizado, exploits de día cero, y manipulación de información.
Objetivo: Obtener información confidencial de otros gobiernos o empresas, interferir en elecciones, o realizar espionaje corporativo.

Ejemplo: El ataque cibernético Stuxnet, que se cree fue desarrollado por los gobiernos de EE.UU. e Israel para sabotear las instalaciones nucleares de Irán.

Atacantes, caracterización

Insiders (Atacantes internos)
Motivación: Personal o organizacional. Estos atacantes son personas dentro de la organización (empleados, contratistas o colaboradores) que tienen acceso legítimo a los sistemas y utilizan ese acceso para causar daño o robar información.
Métodos: Acceso no autorizado a datos, abuso de privilegios de administrador, filtración de información confidencial.
Objetivo: Pueden estar motivados por razones personales (como venganza), lucrativas (robo de propiedad intelectual), o de otro tipo (competencia desleal).

Ejemplo: Un empleado descontento que filtra datos sensibles de la empresa a un competidor o que utiliza su acceso para robar información financiera.

Atacantes, caracterización

Terroristas cibernéticos
Motivación: Ideológica. Los atacantes en esta categoría utilizan ataques cibernéticos para promover sus causas extremistas, o incluso para causar miedo y caos en la sociedad.
Métodos: Pueden utilizar ciberataques para interrumpir infraestructuras críticas, extorsionar gobiernos o difundir propaganda.
Objetivo: Causar daño en infraestructuras clave, alterar el orden social o político, o incluso causar daño físico indirecto (por ejemplo, atacando sistemas de control industrial).

Ejemplo: Un grupo terrorista que lanza ataques cibernéticos contra infraestructuras críticas, como plantas de energía o sistemas de control de tráfico aéreo.

Atacantes, caracterización

Ciberespías (Espionaje cibernético)
Motivación: **Gubernamental** o **industrial**. Los ciberespías están interesados en obtener acceso no autorizado a sistemas o bases de datos para robar secretos de estado o información confidencial de empresas.
Métodos: Explotación de vulnerabilidades en el software, phishing avanzado, malware dirigido, o espionaje de comunicaciones.
Objetivo: Obtener acceso a información valiosa, como secretos comerciales, tecnologías de vanguardia, o información confidencial de gobiernos.

Ejemplo: Un gobierno que espía las comunicaciones de una empresa extranjera para obtener secretos comerciales o tecnología avanzada.

Atacantes, caracterización

Lone Wolves (lobos solitarios)
Motivación: **Diversa**. Este tipo de atacante actúa solo y, a menudo, tiene motivaciones personales, como desquitarse de una organización o probar su propia habilidad.
Métodos: Utilizan métodos comunes como phishing, exploits de vulnerabilidades, o ataques DDoS.
Objetivo: A menudo buscan notoriedad o satisfacción personal. También pueden estar motivados por causas ideológicas o políticas.

Ejemplo: Un individuo que lanza un ataque cibernético a una empresa para demostrar sus habilidades o por resentimiento hacia una organización.

Atacantes, caracterización

Newbie (Novato)		
Características	Métodos de ataque básicos	Motivaciones
es alguien que es nuevo en el mundo de la ciberseguridad o en el ámbito de los ataques informáticos. A menudo, los newbies no tienen experiencia o habilidades avanzadas en hacking, y su enfoque en los ataques suele ser más básico y menos sofisticado en comparación con los atacantes más experimentados. Ven tutoriales en youtube, foros o comunidades on line	- Phishing básico: Enviar correos electrónicos falsos para intentar obtener credenciales o datos personales. - Escaneo de puertos: Usan herramientas simples para identificar puertos abiertos en sistemas vulnerables. - Contraseñas débiles: Intentan hackear cuentas usando fuerza bruta o ataques de diccionario contra contraseñas débiles. - Uso de herramientas automatizadas: Los newbies a menudo dependen de herramientas preexistentes (como Metasploit, Nmap, o Hydra) para realizar ataques sin comprender completamente cómo funcionan las vulnerabilidades que están explotando.	Muchos newbies se sienten atraídos por la curiosidad o el deseo de aprender. Otros pueden estar motivados por el desafío o el deseo de demostrar su habilidad en un campo que consideran emocionante.