Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

La Ingeniería Social

Presentación del tema

La ingeniería social (Social Engineering) constituye una de las amenazas más sofisticadas y efectivas en el ámbito de la seguridad de los Sistemas de Información (SI). A diferencia de los ataques puramente técnicos, la ingeniería social explota el factor humano como vector principal de vulnerabilidad. En lugar de vulnerar directamente sistemas tecnológicos, el atacante manipula psicológicamente a las personas para que revelen información, otorguen accesos o realicen acciones que comprometen la seguridad organizacional.

En la era digital, la exposición de datos personales en redes sociales, bases públicas, filtraciones masivas y plataformas profesionales incrementa significativamente la superficie de ataque. La información que circula sobre personas —hábitos, cargos laborales, relaciones personales, rutinas, preferencias— se convierte en insumo para ataques dirigidos y altamente personalizados. Desde la perspectiva de la administración y la gobernanza tecnológica, la ingeniería social es una cuestión estratégica vinculada a la cultura organizacional, la gestión del riesgo y la protección de activos informacionales.

Concepto y mecanismos psicológicos

La ingeniería social puede definirse como el conjunto de técnicas de manipulación psicológica utilizadas para inducir a una persona a revelar información confidencial, ejecutar acciones indebidas o vulnerar controles de seguridad. Se basa en la explotación de sesgos cognitivos y dinámicas sociales como la confianza, la autoridad, la urgencia, la empatía, el miedo y la curiosidad.

Principales técnicas

Phishing. Consiste en el envío de mensajes fraudulentos que simulan provenir de entidades legítimas para obtener credenciales o información sensible. La variante Spear

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Phishing es un ataque dirigido y personalizado basado en información previamente recopilada sobre la víctima.

Vishing (Voice Phishing). Ataque de ingeniería social mediante llamadas telefónicas fraudulentas, simulando ser soporte técnico, entidades bancarias o autoridades internas.

Smishing (SMS Phishing). Mensajes de texto fraudulentos que inducen al usuario a hacer clic en enlaces maliciosos o revelar información.

Baiting. Consiste en dejar dispositivos USB u otros objetos en lugares visibles con la esperanza de que alguien los conecte a un equipo corporativo, introduciendo malware.

Pretexting. El atacante crea una situación ficticia elaborada (pretexto) para obtener información. Por ejemplo, simula ser auditor externo para solicitar credenciales de acceso.

Quid pro quo. El atacante ofrece algo a cambio de información: soporte técnico gratuito a cambio de credenciales.

El entorno digital como amplificador de la superficie de ataque

Las redes sociales, los perfiles profesionales públicos y las filtraciones masivas de datos proporcionan a los atacantes información valiosa para personalizar sus ataques. El OSINT (Open Source Intelligence) es la práctica de recopilar información de fuentes abiertas para preparar ataques dirigidos. La información aparentemente inocua —cargo, empresa, nombre del jefe, estructura organizacional— puede ser suficiente para construir un pretexto convincente.

Medidas de mitigación

Los controles contra la ingeniería social son principalmente administrativos y culturales. Los programas de concientización en seguridad (Security Awareness) deben incluir simulacros de phishing, formación en verificación de identidad, protocolos claros para la divulgación de información y canales de reporte de incidentes. La verificación de

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

identidad por canales independientes antes de otorgar accesos o realizar transferencias es un control preventivo crítico.

Desde la gobernanza de TI, la ingeniería social debe considerarse en el análisis de riesgos como un vector de amenaza de alta probabilidad y alto impacto, especialmente en organizaciones con procesos financieros digitalizados.

Conceptos clave

- Ingeniería social como explotación del factor humano como vector de ataque.
- Técnicas: phishing, vishing, smishing, baiting, pretexting y quid pro quo.
- OSINT como herramienta de recopilación de información para ataques personalizados.
- La concientización en seguridad como principal control preventivo.
- Verificación de identidad por canales independientes como mecanismo crítico.

Preguntas de repaso del tema

1. ¿Por qué la ingeniería social se considera una amenaza diferente a los ataques técnicos?
2. ¿Qué mecanismos psicológicos explotan las técnicas de ingeniería social?
3. ¿Cuál es la diferencia entre phishing y spear phishing?
4. ¿Qué es el pretexting y cómo puede prevenirse?
5. ¿Cómo puede el entorno digital ampliar la superficie de ataque de ingeniería social?
6. ¿Qué es el OSINT y cómo lo utilizan los atacantes?

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

7. ¿Por qué los programas de Security Awareness son el principal control preventivo?
8. ¿Qué protocolos organizacionales reducen el riesgo de ingeniería social?
9. ¿Cómo debe incluirse la ingeniería social en el análisis de riesgos tecnológicos?
10. ¿Por qué los controles técnicos solos son insuficientes para mitigar la ingeniería social?