Social Engineering Testing

Un Social Engineering Testing es una técnica utilizada para evaluar la seguridad de los recursos y activos de la organización desde el punto de vista de la materia de seguridad de las personas dentro de nuestra organización.

Esta técnica identifica las vulnerabilidades existentes a nivel de concientización y conocimiento sobre diferentes vectores de ataques orientado a las personas dentro de nuestra organización. Específicamente, se busca además de la identificación, la explotación de las vulnerabilidades referidas al engaño de personas y de esa manera se observa el impacto real sobre la organización por medio de esta.

Este tipo de servicio se realiza de manera interna y externa, en donde de manera interna se busca identificar y explotar las vulnerabilidades que sean visibles desde un escenario con acceso a los recursos y activos de la organización, mientras que de manera externa se hace mediante diversos engaños como pueden ser campañas de phishing, llamados a la empresa, entrega de dispositivos maliciosos, etc.

Objetivos principales

- ✓ Obtener una fotografía del estado de la seguridad que la organización, en un momento determinado.
- ✓ Visualizar su compañía desde el punto de vista del atacante, localizando debilidades, vulnerabilidades y puntos de acceso no autorizados, antes que lo hagan los atacantes.
- ✓ Comprobar el verdadero impacto de las vulnerabilidades en su entorno particular.
- ✓ Comprobar si el nivel de protección existente se condice con la política de seguridad establecida por la organización.
- ✓ Comprobar la efectividad de sus medidas de protección, políticas y procesos de detección de intrusos y respuesta a incidentes.
- ✓ Descubrir vulnerabilidades a partir de cambios en las configuraciones de la infraestructura.
- ✓ Dar seguimiento a la aplicación de parches y corrección de vulnerabilidades en la organización.

¿Por qué realizar un Social Engineering Testing?

- ✓ Para conocer el estado de la seguridad de una organización (especialmente si nunca se realizó una auditoría de estas características), referido y dirigido particularmente a la concientización y capacitación de nuestros empleados.

- ✓ Para establecer un punto de partida y comenzar a gestionar la seguridad de la organización.
- ✓ Para constituir un ciclo de revisión y mejora para la seguridad de manera continua. A fin de lograr minimizar todo tipo de amenaza.

Las etapas asociadas a este servicio son:

- ✓ Reconocimiento de la organización u objetivo.
- ✓ Análisis y detección de posibles Vulnerabilidades de Social Engineering Testing.
- ✓ Explotación de vulnerabilidades asociadas.
- ✓ Armado y presentación de reportes.

Todas estas etapas son orientadas y basadas en los posibles vectores de explotación que se puedan lograr realizar dentro del servicio.

Reportes

En este servicio se generan 2 entregables o reportes que ayudan y guían al cliente en el proceso de remediación de vulnerabilidades.

El primero de ellos, el **Informe Ejecutivo**, describe el nivel de riesgo de la compañía sin entrar en detalles técnicos, evidenciando las problemáticas por medio de conceptos claros y gráficas.

El segundo reporte, el **Informe Técnico**, apunta al área técnica de la empresa, ayudando al personal de TI a solucionar los problemas detectados.

En este reporte se muestran todas las evidencias de los tests ejecutados de manera tal que todas las tareas sean repetibles y transparentes para el cliente.