Preparación 1

Objetivo: Establecer contactos, definir procedimientos y recopilar información para ahorrar tiempo durante un incidente.

- Aumente la conciencia del usuario y las políticas de seguridad

  Nunca dé información personal o corporativa a una persona no identificada. Esto incluye IDs de usuario, contraseñas, información de cuentas, nombre, dirección de e-mail, números de teléfono (móvil o fijo), dirección, número de seguro social, cargos, información sobre los clientes, la organización o los sistemas de TI.

  El objetivo de la ingeniería social consiste en robar datos de recursos humanos, secretos corporativos o de clientes o usuarios.

  Reporte cualquier caso sospechoso a su superior, quien lo remitirá al Oficial de Seguridad, con el fin de tener información centralizada.

- Si es necesario, tenga definido un proceso para redirigir cualquier solicitud "extraña" a un "teléfono rojo".

  El número del "teléfono rojo" deben estar claramente etiquetado como "Ingeniería Social". **Este número de teléfono tiene que ser fácil de identificar en la guía telefónica global de su organización, pero no deberá mostrar las consultas inversas (numero->usuario).**
  Las llamadas al "teléfono rojo" siempre deben de grabarse para fines de recolección de pruebas.

- Prepárese a sostener la conversación con los ingenieros sociales para identificar qué información podría ayudar a rastrear el atacante y sus objetivos.
- Revise con su departamento legal para ver qué acciones están permitidas y qué reacciones pueden manejar.

Identificación - USUARIO 2

Objetivo: Detectar los hechos, determinar su alcance, e involucrar a las partes apropiadas.

- Llamada telefónica: alguien no conoce lo llama a usted o a su servicio, para solicitar información detallada.
  - Si el contacto trabaja fuera de la empresa y pide información que podría ser valiosa para un competidor, niéguese a contestar y vea la **parte 3.**
  - Si el contacto se hace pasar por un empleado de su empresa, pero el número de teléfono está oculto o no es interno, proponga que le devuelve la llamada al número registrado en el directorio. Si el atacante supuestamente está de acuerdo, devuelva la llamada para comprobarlo. Si se niega, vea la **parte 3**.

  El atacante puede utilizar varias técnicas para hacer que su víctima a hable (miedo, curiosidad, empatía ...). En ningún caso revele información.
  Escuche con atención a sus solicitudes y al final pida un número de teléfono para devolver la llamada o una dirección de correo electrónico para responder.
  Tome nota y mantenga la calma, incluso si el atacante está gritando o amenazando, recuerde que trata de utilizar las debilidades humanas.
  Si usted puede ir más lejos, le será de valor la siguiente información:
  - El nombre del corresponsal,
  - Información / persona solicitada
  - Acento, conocimiento del idioma,
  - Hablar del medio y conocimiento organizacional,
  - Los ruidos de fondo
  - Hora y la duración de la llamada
- E-mail / Alguien que no conoce solicita información detallada.
  - Si el contacto tiene un e-mail externo y pde información que podría ser valiosa para un competidor, vea la parte 3.
  - Si el contacto utiliza una dirección interna de correo electrónico pero está pidiendo información extraña, dele algunas explicaciones pero utilice el directorio de la organización para obtener el nombre de su jefe y contéstele con copia a él.
- Finalmente notifique a la gerencia superior para informarle que se ha encontrado un incidente de ataque de ingeniería social. Ellos podrían comprender el objetivo en función del contexto.

Contención - USUARIO 3

Objetivo: Mitigar los efectos del ataque sobre el entorno objeto.

En este paso, usted debe estar seguro de que está tratando con un ataque de ingeniería social.

Acciones para todos los empleados:

- **Llamada telefónica**
  - Si el atacante le insta a dar un número de teléfono, siga estos pasos:
    - Si existe, utilice la opción "línea de teléfono rojo" de su CERT/ CSIRT.
    - Dele el número con un nombre ficticio.
    - Llame de inmediato al equipo del CERT / CSIRT explicando lo sucedido y el nombre ficticio elegido.
  - Si el atacante presiona demasiado y no le da tiempo para hallar el número de teléfono rojo, pídale que le llame más tarde, aduciendo una reunión.
  - Si el atacante desea contactar con alguien, siga los siguientes puntos:
  - Ponga en espera al atacante y llame al equipo del CERT / CSIRT y explíqueles lo sucedido.
  - Transfiera la llamada del atacante al equipo del CERT / CSIRT (no le de el número)

- **E-mail**
  - Para fines de investigación, reenvíe el correo electrónico completo , incluídas las cabeceras (envíe como documento adjunto) a su equipo de seguridad . Puede ayudar a realizar el seguimiento del atacante.

Contención - CERT/CSIRT 3

Acciones para el CERT o el equipo de respuesta a incidentes (CSIRT):

- Llamada telefónica
  - Continúe la conversación con el atacante y utilice una de estas técnicas:
    - Suplante la identidad de las personas con las que el atacante está esperando a hablar.
    - Hable despacio para hacer durar la conversación y trate que el atacante cometa un error.
    - Explíquele que el ataque de ingeniería social está prohibido por la ley, que es castigado con sanciones y que el equipo de abogados se encargará de la cuestión si persiste.
  - Si se ha utilizado el número telefónico "trampa", bórrelo y cree otro, luego incluya el nuevo en el directorio.
-
- E-mail
  - Recoja la mayor cantidad de información posible sobre la dirección de correo electrónico:
    - Analice los encabezados de correo electrónico y trate de localizar la fuente
    - Busque la dirección de correo electrónico con las herramientas de Internet
    - Geolocalize al usuario tras la dirección de correo electrónico
- Agregue todos los ataques de ingeniería social para visualizar un patrón.

Remedio 4

Objetivo: Tomar acciones para remover la amenaza y evitar incidentes futuros.

Algunas acciones de remediación posibles pueden ser probados:

- Alerte a la policía y/o presente una denuncia,
- Discuta el problema en círculos de confianza para saber si la empresa se enfrenta sola a este problema,
- Se se le puede identificar, amenace al atacante con acciones legales.

Recuperación 5

Objetivo: Restaurar el sistema a las operaciones normales.

Notifique a la alta dirección de las acciones y las decisiones adoptadas en el caso de la ingeniería social.

.

Repercusiones 6

Informe

Deberá de escribirse un informe de incidente y ponerlo a disposición de todos los interesados. Deberán de describirse los siguientes temas:

- La detección inicial.
- Las acciones y línea de tiempo.
- Lo que sí funcionó.
- ¿Qué salió mal?
- Costo del incidente

Capitalice

Deberán de definirse acciones para mejorar los procesos de detección de malware de Windows para sacar provecho de esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

PeCERT

IRM #10

Ingeniería Social

Cómo manejar un incidente de ingeniería social (por correo electrónico o teléfono)

Autor IRM: CERT SG
Versión IRM: 1.0
email: cert.sg@socgen.com
web: http://cert.societegenerale.com
Traducción: Francisco Neira
email: neira.francisco@gmail.com
Twitter: @neirafrancisco

Extracto

Esta "Metodología de Respuesta a Incidentes" (IRM, por sus siglas en inglés) es una hoja resumen dedicada a los manejadores de incidentes que investigan un asunto de seguridad específico. Quién debe de usar estas hojas IRM?

- Administradores
- Centro de Operaciones de Seguridad (SOC)
- CISOs y sus delegados
- CSIRT (equipos de respuesta a incidentes informáticos)

Recuerde: Si usted afronta un incidente, siga el IRM, tome notas y no pierda el control. Contacte su CSIRT inmediamente si es necesario.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación: Alistarse para manejar el incidente
- Identificación: Detectar el incidente
- Contención: Limitar el impacto del incidente
- Remedio: Remover la amenaza
- Recuperación: Recobrar a una etapa normal
- Repercusiones: Delinear y mejorar el proceso