Preparación 1

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

Contactos
■ Identifique los contactos internos (equipo de seguridad, equipo de respuesta a incidentes, departamento legal, etc)
■ Identifique los contactos externos que pudieran ser necesarios, principalmente para fines de investigación, como agentes del orden.
■ Asegúrese de que el proceso de escalamiento de incidentes de seguridad esté definido y que los actores estén también claramente definidos.
■ Asegúrese de tener las capacidades de recopilación de información (comunidades, contacto, etc) que podrían estar involucrados en dichos incidentes.

Conciencia
■ Asegúrese de que todos los empleados tengan conocimiento de las cuestiones de chantaje. Esto puede ser parte del programa de concienciación sobre la seguridad.

Verifique que los procesos de respaldo de respuesta a incidentes estén en su lugar y actualizados.

Identificación 2

Objetivo: Detectar el incidente, determinar su alcance, e involucrar a las partes apropiadas.

■ Alerte a las personas relevantes

■ Mantenga los rastros de cualquier comunicación relacionada con el incidente (no borre correos electrónicos; anote cualquier contacto telefónico con el número, fecha y hora si están disponibles, fax, etc) Trate de conseguir tantos detalles como sea posible sobre el autor (nombre, fax, dirección postal, etc)

■ Examinar los posibles cursos de acción con su equipo de respuesta a incidentes y el equipo legal.

■ Si se trata de datos internos, compruebe que dispone de una copia de seguridad de los mismos y trate de averiguar cómo fueron obtenidos.

■ Informe a la alta dirección que está sucediendo un chantaje es una realidad y que está siendo manejado de acuerdo a un proceso definido.

Contención 3

Objetivo: Mitigar los efectos del ataque sobre el medio ambiente dirigida.

Determine cómo se puede responder al chantaje y las consecuencias y costos de ignorar o responder sí o no.

Las amenazas más comunes vinculados con el chantaje son:

■ Denegación de servicio
■ Divulgación de información confidencial a través de Internet (Datos personales o tarjetas de crédito de clientes o trabajadores / directores, datos confidenciales internos de la empresa, etc)
■ Divulgación de información privada sensible sobre los empleados / VIP
■ Bloqueo del el acceso a los datos (borrado o cifrado por medio de ransomware por ejemplo [1])
■ Correo masivo con la marca (spam, pornografía infantil [2], rumores maliciosos, etc.)

Revise los antecedentes
Revise si han tenido lugar intentos similares de chantaje en el pasado. Averigüe si otras compañías han sido también amenazadas.

Todos los datos técnicos relacionados deben ser cuidadosamente revisados y recogidos con fines de investigación;

Busque si alguien tendría interés en amenazar su empresa/institución
- Competidores
- Grupos ideológicamente motivados
- Empleados actuales o ex-empleados

Trate de identificar al atacante con los trozos de información disponible.

Específicamente, trate de encontrar la manera en que el atacante entró en el sistema u obtuvo el objeto del chantaje.

Póngase en contacto con las autoridades locales para informarles.

Trate de ganar tiempo y los detalles del estafador. Solicítele:
■ La prueba de lo que dice: Muestra de los datos, prueba de su intrusión, etc.
■ Tiempo para conseguir lo que quiere delincuente (dinero, etc.)

Remedio 4

Objetivo: Adoptar medidas para eliminar la vulnerabilidad y evitar futuros incidentes.

Si se ha identificado un defecto en un activo

técnico o en un proceso que permite al atacante obtener acceso al objeto del chantaje, pide solución **inmediata** a fin de evitar otro caso.

■ Después de obtener la mayor información posible, ignore el chantaje y asegúrese de colocar observación apropiada para detectar y reaccionar ante cualquier nuevo surgimiento.

■ No tome ninguna decisión de remediación solo(a) si hay activos estratégicos o personas en juego. Involucre a los departamentos apropiados en la decisión.

Recuerde que una respuesta positiva a los autores del delito es una puerta abierta para más chantajes.

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 las acciones para mejorar los procesos de manipulación de chantaje y así sacar provecho de esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM # 8

Chantaje

Lineamientos para manejar un intento de chantaje

Autor IRM: CERT SG /Julien Touche
Versión IRM: 1.2
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