METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #8: EXTORSIÓN / CHANTAJE (BLACKMAIL)

Directrices para manejar intentos de Extorsión/Chantaje.

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

Contenido

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de referencia dedicada a los analistas que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. Mantenga la calma y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. Preparación: prepárese para manejar el incidente
2. Identificación: detectar el incidente
3. Contención: limitar el impacto del incidente
4. Remediación: eliminar la amenaza
5. Recuperación: recuperarse a una etapa normal
6. Lecciones aprendidas: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1 PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

Contactos.

- Identifique contactos internos (equipo de seguridad, equipo de respuesta a incidentes, departamento legal, etc.).
- Identifique contactos externos que puedan ser necesarios, principalmente para fines de investigación, como las Fuerzas del Orden (Law Enforcement).
- Asegúrese de que el proceso de escalamiento de incidentes de seguridad esté definido y de que los actores estén claramente definidos.
- Asegúrese de contar con capacidades de recopilación de inteligencia (comunidades, contactos, etc.) que puedan estar involucradas en tales incidentes.

Concientización (Awareness).

- Asegúrese de que todos los empleados relevantes estén al tanto de los problemas de chantaje. Esto puede ser parte del programa de concientización sobre seguridad.

Verifique que el proceso de copia de seguridad (backup) y respuesta a incidentes esté implementado y actualizado.

2.2 IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

- Alerte a las personas relevantes.
- Guarde rastros de cualquier comunicación relacionada con el incidente (no envíe correos electrónicos a la papelera; anote cualquier contacto telefónico con número de teléfono y marca de tiempo si está disponible, fax, etc.). Trate de obtener la mayor cantidad de detalles posible sobre el autor (nombre, fax, dirección postal, etc.).
- Examine posibles cursos de acción con su equipo de respuesta a incidentes y el equipo legal.
- Investigue el correo electrónico para obtener toda la información sobre el incidente (nombre de usuario, servidores MX, etc.).
- Si se trata de datos internos, verifique que tiene una copia de seguridad segura de los mismos y trate de averiguar cómo se recopilaron.
- Incluya a la alta gerencia para informarles que se está produciendo un chantaje y que se está manejando de acuerdo con un proceso definido.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

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

Las amenazas más comunes ligadas al chantaje son:

- Denegación de servicio (Denial of service).
- Revelar datos sensibles en Internet (tarjetas de crédito u otros datos personales de clientes o trabajadores/directores internos, datos confidenciales de la empresa, etc.).
- Revelar información privada sensible sobre empleados/VIPs.
- Bloquear su acceso a datos (borrados o cifrados a través de ransomware, por ejemplo,).
- Envío masivo de correos utilizando la marca (spam, sextorsión, pornografía infantil, rumores maliciosos, etc.).

Verifique los antecedentes.

- Verifique si intentos de chantaje similares han tenido lugar en el pasado. Verifique si otras compañías también han sido amenazadas.
- Todos los datos técnicos relacionados deben ser revisados cuidadosamente y recopilados para fines de investigación.
- Busque si alguien tendría algún interés en amenazar a su compañía:
    - Competidores.
    - Grupos con motivaciones ideológicas.
    - Empleados antiguos o actuales.
- Trate de identificar al atacante con la información disponible.
- Más generalmente, trate de **encontrar cómo el atacante ingresó al sistema u obtuvo el objeto del chantaje.**

Contacte a las fuerzas del orden locales para informarles.

Intente ganar tiempo y obtener detalles del estafador. Pregunte por:

- Prueba de lo que dijo: datos de ejemplo, prueba de intrusión, etc.
- Tiempo para conseguir lo que el estafador quiere (dinero, etc.).

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR FUTURAS DESFIGURACIONES.

Si se ha identificado una falla en un activo técnico o un proceso que permite al atacante obtener acceso al objeto del chantaje, solicite una corrección INMEDIATA para prevenir otro caso.

- Después de obtener la mayor cantidad de información posible, ignore el chantaje y asegúrese de que haya una vigilancia apropiada para detectar y reaccionar de acuerdo con cualquier nuevo seguimiento.
- No tome ninguna decisión de remediación solo si los activos estratégicos o las personas están siendo objeto de ataque. Involucre a los departamentos apropiados.

Recuerde que una respuesta positiva al estafador es una puerta abierta para futuros chantajes.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Notifique a la alta gerencia las acciones y la decisión tomada sobre el problema del chantaje.

2.6 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Si no desea presentar una denuncia, al menos notifique a las Fuerzas del Orden, ya que otras organizaciones podrían verse afectadas. Al mismo tiempo, informe a la jerarquía y a las subsidiarias para tener una posición única en caso de que el estafador intente chantajear a otro departamento interno

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores de la célula de gestión de crisis.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Si se identifica una vulnerabilidad, informe cualquier falla no documentada que afecte al editor de la aplicación, para que el código pueda ser revisado y reciba una corrección oficial.

Capitalizar

Se deben definir acciones para mejorar los procesos de gestión de infecciones por gusanos, para aprovechar esta experiencia.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Incidentes Informáticos
NIST	Instituto Nacional de Estándares y Tecnología
EDR	Detección y Respuesta de Puntos de Acceso
Ransomware	Tipo de malware que bloquea el acceso a los datos, ya sea borrándolos o cifrándolos para extorsionar a la víctima.
Sextorsión	Modalidad de chantaje que puede involucrar el uso de la marca para envíos masivos de correos con contenido sensible o rumores.
Denegación de Servicio (DoS)	Amenaza técnica que busca interrumpir la disponibilidad de los servicios como medida de presión.