METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #12 ABUSO POR PARTE DE UN EMPLEADO INTERNO

Guías para gestionar y responder a la divulgación intencional de información interna

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 3
2. PASOS PARA LA GESTIÓN DE INCIDENTES 4
2.1 PREPARACIÓN 5
2.2 IDENTIFICACIÓN 6
2.3 CONTENCIÓN 7
2.4 REMEDIACIÓN 8
2.5 RECUPERACIÓN 9
2.6 LECCIONES APRENDIDAS 10
3. DEFINICIONES 11

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de consulta dedicada a los encargados 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 y procesos.

- Asegurarse de tener puntos de contacto en el equipo de relaciones públicas, el equipo de recursos humanos y el departamento legal.
- Centralizar el registro (logging) para los controles de acceso.
- Asegurarse de tener un proceso global de autorización y habilitación. Este proceso debe ocuparse especialmente de la eliminación de privilegios en trabajos anteriores.
- Proporcionar una autenticación fuerte acorde con el riesgo de la aplicación de negocio.
- Preparar la estrategia de comunicación interna y externa.
- Preparar un proceso de Prevención de Pérdida de Datos (DLP) con el equipo de GDPR y riesgo.

Estar preparado para notificar a los proveedores implicados y a los servicios de la policía y reguladores si es necesario durante un incidente (gestión de células de crisis).

2.2 IDENTIFICACIÓN

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

Identificación Técnica:

- Alertas de un SIEM o herramientas de correlación:
  - El comportamiento malicioso puede haberse detectado con la correlación de varios eventos anormales.
- Alertas de un IDS/IPS que detecta una intrusión:
  - En caso de que el interno haya intentado hackear el sistema, un Sistema de Detección de Intrusiones (IDS) o Sistema de Prevención de Intrusiones (IPS) puede ser capaz de disparar una alerta.
- Alertas de controles y servicios DLP:
  - Herramientas y procesos para detectar y prevenir fugas de datos y exfiltración de datos.
- Alertas de controles de acceso físico.

Identificación Humana

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

- Notifique a la gerencia, al equipo legal y al equipo de relaciones públicas/comunicación para asegurarse de que estén preparados para lidiar con una divulgación masiva o dirigida.

- Dependiendo del vector de fuga, bloquee el acceso a la URI de divulgación, al servidor de divulgación, a la fuente de divulgación o a los destinatarios de la divulgación. Esta acción debe realizarse en todos los puntos de la infraestructura.

- Suspenda las credenciales lógicas y físicas de la persona interna si se ha confirmado la fuga. Involucre a RR.HH. y al equipo legal antes de cualquier acción.

- Aísle el sistema informático (escritorio, impresora) utilizado para divulgar datos con el fin de realizar un análisis forense posterior. Esta manipulación debe hacerse de la manera más difícil: retire el enchufe eléctrico (y la batería en caso de un ordenador portátil).

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR INCIDENTES FUTUROS.

- Si los datos han sido enviados a servidores públicos, solicite al propietario (o webmaster) que elimine los datos divulgados. Asegúrese de ajustar su solicitud a los destinatarios (un webmaster de hacktivismo no se comportará como un webmaster de prensa).

- Si no es posible eliminar los datos divulgados, proporcione un análisis completo al equipo de RR.PP. y a la gerencia. Supervise la difusión de documentos filtrados en sitios web y redes sociales (FB, Twitter, etc.) y los comentarios o reacciones de los usuarios de Internet.

Proporcione los elementos al equipo de RR.HH. para que eventualmente presente una queja contra la persona interna.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

- Si un sistema ha sido comprometido, restáurelo completamente.
- Finalmente, advierta a sus empleados o a algunos equipos locales sobre el problema para crear conciencia y aumentar las reglas de seguridad.
- Cuando la situación vuelva a la normalidad, retire finalmente la comunicación oficial.

Para obtener más detalles sobre la recuperación de la autenticación y la infraestructura, consulte la IRMXXX de compromiso de malware a gran escala.

2.6 LECCIONES APRENDIDAS

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

Informe a su jerarquía, subsidiarias y socios para compartir las mejores prácticas aplicadas en este incidente y hacer cumplir reglas similares en otras ubicaciones.

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores del incidente.

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

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 Emergencias Informáticas.
CSIRT	Equipo de respuesta a Incidentes de Seguridad, implícito como sinónimo/similar a CERT en la accesión de red phone.
NIST	Instituto Nacional de Estándares y Tecnología
TLP	Indica que la información puede ser distribuida sin restricciones
DLP	Una herramienta que, si está presente en la empresa, puede proporcionar información valiosa a los gestores de incidentes que trabajan en la fuga de información.
Ransomware Shaming List Websites	Sitios web que se deben monitorizar para detectar posibles fugas de datos (filtraciones) que a menudo publican información robada
Malware/Ransomware	Un compromiso por este tipo de software malicioso puede ser la fuente de una fuga de información.
Forensic Analysis (Análisis Forense)	Una manipulación que debe realizarse después de aislar el sistema informático utilizado para divulgar datos. También puede confirmar el uso de hardware externo, pero no los datos transmitidos.
Indicadores de Compromiso (IoCs)	Elementos que deben incluirse en el informe de lecciones aprendidas.
Spooler (de impresora)	Un lugar donde se deben buscar rastros de datos enviados a impresoras conectadas a la red