METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #11 FUGA DE INFORMACIÓN

Tratar la información interna, divulgada intencionalmente.

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 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.

- Identifica contactos técnicos internos (equipo de seguridad, equipo de respuesta a incidentes...).
- Asegúrate de tener puntos de contacto en tu equipo de relaciones públicas (instituciones reguladoras), equipo de recursos humanos y departamento legal.
- Identifica contactos externos que puedan ser necesarios, principalmente para fines de investigación (como las Fuerzas del Orden (Law Enforcement), por ejemplo).
- Prepara una estrategia de comunicación interna y externa.
- Contactos de DPO (Data Protection Officer), CDO (Chief Data Officer), GDPR.

Política de Seguridad.

- Asegúrate de que el valor de la información corporativa se explique en las reglas de procedimiento, el organigrama de TI, la concienciación y las sesiones de capacitación.
- Asegúrate de que todos los activos valiosos estén identificados como deberían.
- Asegúrate de que el proceso de escalada de incidentes de seguridad esté definido, y que los actores estén claramente definidos e identificados.

2.2 IDENTIFICACIÓN

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

La fuga de datos puede ocurrir desde cualquier lugar. Recuerda que la causa de la fuga puede ser un empleado individual que elude los problemas de seguridad de forma voluntaria o involuntaria, o un equipo comprometido (es decir, a gran escala/ransomware).

1. **Detectar el Problema.**

Proceso de notificación de incidentes:

- La información interna puede ser una buena fuente de detección: confianza de los empleados, equipo de seguridad que identifica un problema, etc.

Herramienta de monitoreo público:

- Una vigilancia en los motores de búsqueda de Internet y bases de datos públicas puede ser muy valiosa para detectar fugas de información.

- Supervise los sitios web de listas de vergüenza de ransomware para detectar posibles fugas de datos, incluidos terceros.

Herramienta DLP (Data Loss Prevention - Prevención de Pérdida de Datos):

- Si hay una herramienta DLP en la empresa, puede proporcionar información valiosa a los gestores de incidentes que trabajan en fugas de información.

2. **Confirmar el problema**.

No haga nada sin una solicitud por escrito del CISO/persona a cargo en cuestión. Según el consejo de su equipo legal, un permiso por escrito del usuario en cuestión también podría ser útil.

3. **Correo Electrónico:**

- La fuente de la divulgación podría haber enviado datos utilizando su dirección de correo electrónico corporativa.
- En el sistema de mensajería, busque correos electrónicos enviados o recibidos desde una cuenta sospechosa o con un asunto especial.
- En el cliente de correo electrónico en el escritorio del sospechoso (si está disponible), use una herramienta que le permita buscar filtrando los correos electrónicos marcados como "PRIVADOS". Si realmente necesita hacerlo, pida al usuario un acuerdo por escrito, o pídale que esté con usted.
- Cuando sea aplicable, revise los archivos de registro relacionados.

4. Navegación.

- Los datos podrían haber sido enviados a correo web/foros/sitios web dedicados.
- En el servidor proxy o SIEM, verifique los registros relacionados con las conexiones de la cuenta sospechosa a la URL sospechosa utilizada para divulgar datos.
- En el escritorio (si está disponible), verifique el historial de los navegadores instalados. Recuerde que algunas personas pueden tener diferentes navegadores en el mismo ordenador de escritorio; asegúrese de verificar el historial de cada navegador. Si se puede marcar el momento de la fuga de datos con una marca de tiempo, algunos archivos de registro pueden proporcionar información útil.

5. Dispositivos de almacenamiento externo.

- Se puede utilizar una variedad de dispositivos para almacenar datos: llaves USB, CD-ROM, DVD, discos duros externos, teléfonos inteligentes, tarjetas de memoria.
- Se encontrará poca información sobre la transferencia de datos mediante estos dispositivos. La llave USB utilizada para transferir datos puede ser referenciada por el sistema operativo. Un análisis forense puede confirmar el uso del hardware, pero no los datos transmitidos.

6. Archivos Locales.

- Si aún no se ha encontrado nada, todavía hay posibilidades de encontrar rastros en el sistema de archivos local del sospechoso. Al igual que para las búsquedas de correo electrónico, use una herramienta de análisis que prohíba cualquier acceso a la zona PRIVADA del usuario. Si realmente necesita hacerlo, actúe de acuerdo con la legislación laboral local.

7. Transferencia de red.

- Se pueden usar múltiples formas para transferir datos fuera de la empresa: FTP, mensajería instantánea, etc. Intente buscar en los archivos de registro que muestren dicha actividad.
- Los datos también podrían haber sido enviados a través de un túnel VPN o a un servidor SSH. En este caso, se puede probar la conexión observando los archivos de registro, pero no se puede ver el contenido transmitido.

8. **Impresora**.

- Los datos pueden ser enviados a impresoras conectadas a la red. En este caso, busque rastros en la cola de impresión o directamente en la impresora, ya que algunos fabricantes almacenan directamente los documentos impresos en un disco duro local.

9. **Malware/Ransomware.**

- Un compromiso por malware/ransomware puede ser la fuente de una fuga de información y debe tratarse de acuerdo con la IRM 7 de "Detección de Malware" o la IRM 17 de "Ransomware".

Incluso cuando se haya encontrado suficiente evidencia, siempre busque más.
No es porque haya probado que los datos pasaron fraudulentamente de A a B con un método, que no se hayan enviado también a C con otro método. Tampoco olvide que alguien más podría haber accedido al ordenador. ¿Estaba el empleado sospechoso realmente frente a su ordenador cuando ocurrió la fuga?

10. **Analizar los datos afectados si están disponibles.**

- A veces, los datos filtrados pueden ser descargados y analizados por el equipo de seguridad. Los sitios web de listas de vergüenza de ransomware a menudo publican información filtrada.
- El uso de herramientas de análisis de datos como Aleph puede ayudar a los equipos legales a decidir qué acciones deben tomarse.

Al final de esta fase, puede considerar involucrar a los servicios de las fuerzas del orden y reguladores si es necesario.

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