METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #19 COMPROMISO DE TERCERO / PROVEEDOR

Pautas para manejar y responder a una vulneración de terceros.

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.

Objetivo de la IRM: El objetivo de esta Metodología de Respuesta a Incidentes (IRM19) es proporcionar orientación sobre la gestión y respuesta a incidentes que impliquen la afectación de un tercero con el que tu organización mantiene una relación operativa. Las afectaciones a terceros pueden exponer los datos, sistemas u operaciones de la organización a riesgos y amenazas; esta metodología tiene como objetivo minimizar el impacto potencial en los activos de información y la reputación de tu organización.

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.

- Mantener un inventario actualizado de todos los terceros, socios, proveedores y contratistas con acceso a los sistemas, datos, equipos o infraestructura de la organización.
- Preparar y tener disponible un directorio de contactos de personas a involucrar cuando se contraten servicios de terceros.
- Definir puntos de contacto específicos 24/7 y personas para intervenir durante horas no laborables.
- Establecer un proceso para evaluar la madurez del sistema de información de los proveedores de servicios incorporados mediante un cuestionario KYS.
- Establecer y mantener Acuerdos de Nivel de Servicio (SLA) con terceros, incluyendo requisitos de seguridad y respuesta a incidentes; y cláusulas específicas de alerta en caso de un compromiso de un tercero.
- Revisar y evaluar regularmente los controles de seguridad, políticas y procedimientos de terceros.
- Establecer un mapa formal de interconexiones y flujos de comunicación con los proveedores de servicios.
- Implementar un “Botón Rojo” para cortar todos los enlaces informáticos con el proveedor de servicios afectado si surge tal necesidad.
- Evaluar la viabilidad, capacidad y el tiempo requerido para bloquear enlaces de interconexión con un tercero o accesos de terceros; validar mediante pruebas y simulacros de corte. Asegurarse de tener en cuenta el impacto en el negocio y los requisitos regulatorios.
- Realizar ejercicios conjuntos de respuesta a incidentes con terceros críticos de manera regular.
- Preparar una estrategia de comunicación interna y externa en caso de incidente, incluyendo canales de comunicación alternativos para los contactos aplicables.
- Establecer un proceso de vigilancia de blogs y sitios de “shaming” de ransomware; elaborar una lista completa de palabras clave, categorías industriales o geografías para aplicar al proceso de seguimiento deseado. Tenga en cuenta que, dependiendo del país, las actividades de investigación que involucren datos filtrados pueden estar sujetas al cumplimiento de las normativas locales de protección de datos, incluido el GDPR y el código penal. Consulte con su oficial de protección de datos, oficial de cumplimiento o asesores legales antes de establecer el proceso de vigilancia. Realizar una vigilancia activa de actores de amenazas conocidos, particularmente operadores de ransomware.
- Mantener una supervisión regular de empresas que han sufrido un ciberataque, especialmente aquellas comprometidas por ransomware.
- Automatizar alertas internas para notificar la presencia de un socio en uno de los sitios de blogs de “shaming”.

- Preparar instalaciones dedicadas para el análisis o sandboxing de los datos y archivos aplicables para usar durante el incidente.

Se deben considerar requisitos legales adicionales al configurar el proceso de monitoreo, por ejemplo: https://www.cnil.fr/fr/la-recherche-sur-internet-de-fuites-dinformations-rifi

2.2 IDENTIFICACIÓN

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

Es posible que necesite notificar a los interesados, socios y reguladores al inicio de este paso si es necesario.

Detección.

- Utilice monitoreo proactivo derivado de la vigilancia de blogs de denuncias, fuentes abiertas o notificaciones privadas: verifique y analice regularmente todos los feeds de inteligencia de amenazas aplicables para la detección temprana de información sobre posibles compromisos de terceros.
- Monitoree continuamente los flujos de red de ingreso/egreso para detectar oportunamente anomalías en las interconexiones con terceros.
- Involucre a todas las partes interesadas previamente identificadas (Negocios, Compras, Legal, Infraestructura, Seguridad de la Información, etc.); evalúe el impacto potencial con base en la información disponible sobre el incidente y la retroalimentación de los departamentos de negocio y TI.
- Evalúe posibles escenarios de remediación: bloquear interconexiones, reforzar la supervisión basándose en la evaluación de riesgos frente a los impactos potenciales en la producción.
- Comunicar/escalar el incidente a niveles superiores en su organización (hasta la Junta Directiva) para tener la visión más completa y exhaustiva de la situación.
- Establezca canales de comunicación con el tercero afectado para compartir información sobre el incidente en curso. Si la naturaleza del incidente lo requiere, configure canales alternativos dedicados (no corporativos) para usar en la comunicación e intercambio de datos durante el incidente.
- Evalúe el nivel de confiabilidad del proveedor según el grado de transparencia que se pueda establecer con el tercero, la percepción de la calidad de su comunicación y la entrega efectiva de los informes aplicables de investigación y gestión del incidente, IOC, etc.

Recomendaciones adicionales de diligencia debida: en caso de signos de lateralización, consulte el IRM 18-LargeScaleCompromise.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Si el incidente implica acceso a recursos sensibles de la organización, puede convocarse una célula específica de gestión de crisis.

- Suspender temporalmente o restringir el acceso del tercero afectado a los sistemas, datos, equipos o infraestructura de la organización, según sea necesario.
- Limitar la comunicación por correo electrónico de manera total o selectiva (es decir, redirigiendo los correos proporcionados a un entorno o bandeja de entrada aislado, eliminando adjuntos, enlaces u otro contenido).
- Establecer reuniones periódicas con el proveedor afectado, incorporando a los interesados correspondientes.
- Coordinar con el tercero afectado la implementación de medidas de contención, como aislar sistemas comprometidos, bloquear IOCs maliciosos o cambiar credenciales.

Si aplica a los IOCs obtenidos:

- Bloquear el tráfico hacia los C2.
- Bloquear cualquier IP detectada como usada por los atacantes.
- Desactivar cuentas comprometidas/creadas por los atacantes.
- Enviar las muestras no detectadas a su proveedor de seguridad de endpoints y/o a sandbox privados.
- Enviar las URLs, nombres de dominio y IP maliciosas no categorizadas a su proveedor de seguridad perimetral.

Si el tráfico crítico para el negocio no puede ser desconectado, permitirlo tras implementar controles de seguridad adicionales para detectar oportunamente e inhibir la proliferación lateral.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR MEDIDAS PARA LIMITAR EL IMPACTO EN LA PRODUCCIÓN.

- Reevaluar la transparencia y aplicabilidad de los esfuerzos de remediación de terceros.
- Considerar solicitar un informe formal del incidente según corresponda al proceso en curso de manejo de incidentes o investigación forense, es decir, una carta de compromiso firmada por la junta del proveedor o un informe de investigación realizado por el encargado del incidente / servicio forense a cargo del incidente.
- Solicitar una lista actualizada de IOC aplicables revelados por el proceso de investigación.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Todos los pasos siguientes se deben realizar de manera paso a paso y con monitoreo técnico.

- Obtener un informe formal de un tercero de confianza que asegure que la situación del reclamante ha vuelto realmente a la normalidad.
- Decidir con los actores identificados internamente si es factible reabrir los servicios y las interconexiones con el socio.
- Trabajar con el tercero afectado para restaurar los servicios o sistemas afectados, asegurando que sean seguros y estén libres de vulnerabilidades.
- Reevaluar y actualizar el perfil de riesgo del tercero a la luz del incidente.
- Restituir gradualmente el acceso del tercero a los sistemas, datos e infraestructura de su organización, asegurando que se implementen las medidas de seguridad apropiadas.

2.6 LECCIONES APRENDIDAS

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

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

Capitalizar

- Realizar una revisión post-incidente con la tercera parte afectada para identificar áreas de mejora.
- Actualizar los manuales de procedimientos aplicables o metodologías de gestión de incidentes y otros procesos pertinentes basados en las lecciones aprendidas del incidente.
- Compartir las lecciones aprendidas con los interesados y los actores de la comunidad de seguridad para mejorar la postura de seguridad general y las capacidades de respuesta a incidentes.
- Mantener informados a los interesados relevantes dentro de su organización durante todo el proceso de respuesta al incidente, incluyendo la alta dirección y el departamento legal.
- Asegurarse de que el incidente haya sido debidamente documentado, incluyendo cronograma, impacto y medidas de respuesta, para fines de cumplimiento y auditoría.
- En coordinación con los departamentos legales y de relaciones públicas, preparar y emitir comunicaciones apropiadas a las partes externas, si es necesario.

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
IDS	Sistema de Detección de Intrusiones
IPS	Sistema de Prevención de Intrusiones
KYS (Know Your Supplier)	Proceso de evaluación de madurez de seguridad de proveedores mediante cuestionarios técnicos.
Sandboxing	Instalaciones aisladas para el análisis dinámico de archivos o datos sospechosos sin riesgo para la red principal.
Botón Rojo (Red Button)	Mecanismo técnico diseñado para cortar de forma inmediata todos los enlaces informáticos con un proveedor afectado.
C2 (Command and Control)	Servidores externos utilizados por atacantes para controlar sistemas comprometidos; el IRM indica bloquear el tráfico hacia estos puntos.
Proliferación Lateral (Lateralización)	Movimiento de un atacante dentro de una red después de la intrusión inicial; se recomienda consultar el IRM #18 en estos casos.
Blogs de "Shaming	Sitios utilizados por operadores de ransomware para publicar datos filtrados de sus víctimas, usados aquí como fuente de monitoreo proactivo.