METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #5: COMPORTAMIENTO MALICIOSO EN LA RED

Guía para manejar una actividad de red sospechosa

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.

Sistemas de Detección de Intrusiones (EDR, NIPS, IPS).

- Asegúrese de que las herramientas de monitoreo estén actualizadas.
- Establezca contactos con sus equipos de red y de operaciones de seguridad.
- Asegúrese de que se defina un proceso de notificación de alertas y que sea bien conocido por todos.
- Verifique el acceso al dispositivo y su capacidad para observar los perímetros afectados.
- Asegúrese de que puede aislar los puntos finales y el área (con EDR o Firewall, por ejemplo).

Red (Network)

- Asegúrese de que haya un inventario de los puntos de acceso de la red disponible, accesible y actualizado, si es posible, con control de versiones.
- Asegúrese de que los equipos de red tengan mapas de red y configuraciones actualizadas con las zonas afectadas y los equipos operativos.
- Busque regularmente posibles puntos de acceso de red no deseados y ciérrelos.
- Busque acceso VPN y acceso a la Nube desde ubicaciones poco comunes.
- Implemente y supervise herramientas de gestión de tráfico.

Tráfico base (Baseline traffic).

- Identifique el tráfico y los flujos base.
- Identifique los flujos críticos para el negocio.

Asegúrese de que las personas se sientan cómodas con las herramientas y sepan cómo usarlas. Mantenga los registros operativos incluso cuando hayan sido archivados.

Tener una buena política de retención de registros es esencial (más de 6 meses).

2.2 IDENTIFICACIÓN

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

Fuentes de detección:

- Notificación por parte del usuario/mesa de ayuda (helpdesk).
- Registros, alertas e informes de IDS/IPS/NIDS/EDR.
- Detección por parte del personal de red.
- Registros de Firewall y proxy.
- Queja de una fuente externa.
- Honeypots o cualquier otra solución engañosa.

Registrar la actividad de red sospechosa

Las tramas de red se pueden almacenar en un archivo y transmitirse a su equipo de respuesta a incidentes para su posterior análisis.
Utilice herramientas de captura de red (tshark, windump, tcpdump...) para volcar el tráfico malicioso.
Utilice un hub o port mirroring en una LAN afectada para recopilar datos valiosos.
El análisis forense de red requiere habilidades y conocimientos. Pida asistencia o consejo a su equipo de respuesta a incidentes.
Sepa cómo restaurar y consultar registros incluso cuando hayan sido archivados.

Analizar el ataque

- Analice las alertas generadas por su IDS.
- Revise las estadísticas y registros de los dispositivos de red.
- Intente comprender el objetivo del tráfico malicioso e identifique los componentes de la infraestructura afectados por él.
- Haga un mapa con los riesgos del negocio para priorizar adecuadamente el análisis o la contención.
- Identificar las características técnicas del tráfico:
  - Dirección(es) IP de origen
  - Puertos utilizados, TTL, ID de Paquete
  - Protocolos utilizados
  - Máquinas/servicios objetivo
  - Exploit(s)
  - Cuentas remotas con sesión iniciada

Al final de este paso, se deben haber identificado las máquinas afectadas y el modus operandi del ataque. Idealmente, la fuente del ataque también debería haber sido identificada. Aquí es donde debe realizar sus investigaciones forenses, si es necesario. Si se ha identificado una computadora comprometida, consulte las hojas de referencia IRM dedicadas a la intrusión.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Si el problema se considera estratégico (acceso a recursos sensibles), se debe activar una célula de gestión de crisis específica.

Dependiendo de la criticidad de los recursos afectados, se pueden realizar y monitorear los siguientes pasos:

- Desconecte el área comprometida de la red.
- Aísle la fuente del ataque. Desconecte la(s) computadora(s) afectada(s) para realizar una investigación posterior.
- Adopte controles de mitigación aceptables (MFA, geo-filtrado) para el flujo crítico para el negocio de acuerdo con los gerentes de la línea de negocio.
- Finalice las conexiones o procesos no deseados en las máquinas afectadas.
- Utilice reglas de firewall/IPS/EDR para bloquear el ataque.
- Utilice reglas de IDS para que coincidan con este comportamiento malicioso e informen al personal técnico sobre nuevos eventos
- Aplicar acciones ad hoc en caso de problema estratégico:
  - Deniegue destinos de egreso en EDR, proxies y/o firewalls.
  - Configure la gestión de políticas de controles de seguridad para contener o rechazar conexiones de máquinas comprometidas.
  - Limite el acceso a datos críticos/confidenciales.
  - Cree documentos con trampas (booby-trapped documents) con marcas de agua que puedan usarse como prueba de robo.
  - Notifique a los usuarios de negocio objetivo sobre lo que se debe hacer y lo que está prohibido.
  - Configure las capacidades de registro en modo detallado (verbose) en el entorno objetivo y almacénelos en un servidor remoto seguro.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA DETENER EL COMPORTAMIENTO MALICIOSO.

Bloquear la fuente

- Utilizando el análisis de los pasos previos de identificación y contención, descubra todos los canales de comunicación utilizados por el atacante y bloquéelos en todos los límites de su red.
- Si la fuente ha sido identificada como un insider (empleado o persona interna), tome las medidas adecuadas e involucre a su equipo de gestión y/o RR.HH. y/o al equipo legal.
- Si la fuente ha sido identificada como un delincuente externo, considere involucrar a los equipos de abuso y a los servicios de aplicación de la ley si es necesario.

Remediación técnica

- Defina un proceso de remediación. Si es necesario, este proceso puede ser validado por otra estructura, como su equipo de respuesta a incidentes, por ejemplo.
- Los pasos de remediación de los IRMs de Intrusión (2-Windows y 3-Linux) también pueden ser útiles.

Probar y Ejecutar

- Pruebe el proceso de remediación y asegúrese de que funcione correctamente sin dañar ningún servicio.
- Imponga el proceso de remediación una vez que las pruebas hayan sido aprobadas tanto por TI como por el negocio.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

1. Asegúrese de que el tráfico de red vuelva a la normalidad.
2. Vuelva a permitir las conexiones a los segmentos de red previamente contenidos.

Todos estos pasos se realizarán de forma gradual y con una supervisión técnica.

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

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
IDS	Sistema de Detección de Intrusiones
IPS	Sistema de Prevención de Intrusiones
IOC	Un IoC (Indicador de Compromiso) es cualquier evidencia forense que indica que un sistema o red ha sido atacado por una amenaza de seguridad.
tshark	Es un analizador de tráfico de red de línea de comandos que es la versión para terminal de Wireshark.
windump	Es la versión de Windows de la herramienta de línea de comandos tcpdump, utilizada en ciberseguridad para capturar y analizar el tráfico de red en tiempo real.
tcpdump	Es una herramienta de línea de comandos esencial para la captura y análisis de tráfico de red.
firewall	Es un dispositivo o software que actúa como una barrera de seguridad entre una red interna confiable y redes externas no confiables, como Internet.
helpdesk	Un helpdesk es un sistema o equipo centralizado que proporciona atención al cliente y soporte técnico.
proxy	Es un servidor o dispositivo que actúa como intermediario entre un cliente (tu dispositivo) y un servidor (la página web o servicio al que deseas acceder).
Honeypots	Es un sistema informático diseñado para atraer ciberataques y registrar las acciones de los atacantes.
TTL	(Time to Live) es un parámetro clave en la ciberseguridad que actúa como una especie de fecha de caducidad para los paquetes de datos que se transmiten a través de la red.
ID de Paquete	Se refiere a un identificador de red, que es una dirección única asignada a un componente de red, como una computadora o un router.

Exploit	Es un programa, técnica o fragmento de código diseñado para aprovechar una vulnerabilidad en un sistema informático.
MFA	La autenticación multifactor (MFA) es una medida de seguridad que requiere la verificación de la identidad del usuario mediante la presentación de al menos dos formas diferentes de credenciales antes de permitir el acceso a un sistema, aplicación o servicio.
geo-filtrado	Se refiere a la práctica de controlar el acceso a contenido digital o servicios basado en la ubicación geográfica del usuario.