METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #21 PRIORIZACIÓN DE VULNERABILIDADES CRÍTICAS

Directrices para el proceso de priorización de vulnerabilidades críticas basado en inteligencia de amenazas Cibernéticas.

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 Gestión de Vulnerabilidades (VMM) es una guía concisa diseñada para profesionales que gestionan y abordan vulnerabilidades de seguridad específicas dentro de una organización.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

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

Recordatorios clave.

Siga el IRM: Adhiera a la metodología establecida para asegurar un enfoque estructurado y eficaz en la gestión de vulnerabilidades.

Documente a fondo: Mantenga notas detalladas de todos los hallazgos, acciones tomadas y decisiones realizadas durante los procesos de evaluación y remediación de vulnerabilidades.

Mantenga la calma: Mantenga procedimientos calmados y sistemáticos al identificar y abordar vulnerabilidades.

Involúcrese de manera apropiada: Contacte de inmediato al equipo de Gestión de Vulnerabilidades de su organización o al CERT si se necesita apoyo adicional o escalamiento.

Al utilizar las hojas de la Metodología de Gestión de Vulnerabilidades, las organizaciones pueden asegurar un enfoque consistente y eficiente para identificar, priorizar y mitigar vulnerabilidades. Esta metodología estructurada respalda la protección de los activos críticos y mejora la postura general de seguridad.

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.

OBJETIVOS:

Mejorar la Gestión de Vulnerabilidades.

Mejorar la identificación y priorización de vulnerabilidades a través de la Inteligencia de Amenazas Cibernéticas.

Optimizar la Asignación de Recursos.

Asegurar que los recursos limitados se centren en abordar las vulnerabilidades más críticas.

Fortalecer la Respuesta a Incidentes.

Integrar la Inteligencia de Amenazas Cibernéticas en la Respuesta a Incidentes para proporcionar contexto y capacidades de toma de decisiones accionables durante la gestión de incidentes.

Reducir la Exposición al Riesgo.

Minimizar la ventana de oportunidades para los atacantes abordando proactivamente las vulnerabilidades de alto riesgo.

2.1 PREPARACIÓN

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

- Desarrollar o adquirir fuentes de CTI relacionadas con vulnerabilidades y exploits, como feeds de amenazas, informes de inteligencia, acceso a repositorios y bases de datos dedicadas.
- Configurar herramientas y plataformas internas de monitoreo de vulnerabilidades y CTI para la agregación y análisis de datos.
- Asignar responsabilidades para la recolección, análisis e integración de CTI en la gestión de vulnerabilidades.
- Crear directrices para la evaluación y priorización de vulnerabilidades utilizando CTI.
- Desarrollar un inventario completo de todos los sistemas y versiones de software dentro de la organización para comprender la superficie de ataque potencial.
- Establecer un programa de inteligencia de amenazas para recopilar y analizar continuamente datos sobre amenazas y vulnerabilidades emergentes.
- Preparar canales de comunicación y plantillas para la rápida difusión de información necesaria para fines de Gestión de Vulnerabilidades durante un incidente relacionado con vulnerabilidades.
- Capacitar al equipo de respuesta a incidentes y a otros equipos involucrados en el uso de herramientas, servicios y metodologías de inteligencia de amenazas y monitoreo de vulnerabilidades.
- Establecer canales operativos para compartir información de manera eficiente entre los equipos involucrados.

Conciencia Empresarial para la Gestión Proactiva de Vulnerabilidades.

Gestionar proactivamente las vulnerabilidades es crucial para proteger los sistemas de información de su empresa. En lugar de esperar a que ocurra un exploit, **comunique la importancia de la gestión de vulnerabilidades a su organización**. Destaque casos de uso relevantes para ilustrar los posibles impactos en las operaciones comerciales y la producción, llamando así la atención sobre la importancia de una gestión oportuna de vulnerabilidades. **Eduque a sus partes interesadas sobre lo que implica la gestión de vulnerabilidades y asegúrese de que comprendan los riesgos y beneficios asociados.** Deje claro que las partes interesadas pueden pedir ayuda y asistencia siempre que sea necesario. A través de una conciencia eficiente y una comunicación abierta, empodera a sus equipos para proteger mejor los activos y sistemas de información de su organización.

2.2 IDENTIFICACIÓN

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

Escaneo de Vulnerabilidades

- Utilizar herramientas automatizadas para identificar vulnerabilidades en sistemas y aplicaciones.

Recolección de CTI

- Recopilar inteligencia de diversas fuentes de CTI, incluyendo inteligencia de fuentes abiertas, feeds comerciales y centros de intercambio y análisis de información, como los ISACs.

Perfilado de Actores de Amenaza

- Identificar posibles actores de amenaza relevantes para la industria y la infraestructura tecnológica de la organización.

Puntuación de Vulnerabilidades

- Evaluar la severidad de las vulnerabilidades identificadas utilizando estándares como CVSS, EPSS, etc.

Integración de CTI

- Correlacionar las vulnerabilidades con CTI para comprender si están siendo explotadas activamente o si son objetivo de actores de amenaza.

Análisis Ambiental

- Evaluar la relevancia de cada vulnerabilidad en el contexto de la realidad ambiental de la organización y del panorama de amenazas realista.

Priorización

- Determinar el impacto potencial y la probabilidad de explotación de cada vulnerabilidad.
- Aplicar puntuaciones derivadas de CTI a las vulnerabilidades basándose en factores como la disponibilidad de exploits, la actividad de los actores de amenazas y la focalización de la industria.

- Crear flujos de trabajo basados en lógica o puntuación para categorizar las vulnerabilidades en niveles de prioridad (por ejemplo, muy alta, alta, media, baja) basándose en la combinación de riesgo y puntuaciones de CTI.
- Incluir el factor de criticidad del negocio y el impacto potencial en operaciones y producción al priorizar vulnerabilidades para su organización.

Estándares y Herramientas de Priorización

CVSS se centra en la gravedad de las vulnerabilidades según sus características técnicas, pero carece de datos sobre la explotabilidad en el mundo real.

EPSS predice la **probabilidad de explotación**, proporcionando un enfoque más dinámico y accionable para la **priorización**.

Las herramientas de Gestión de Riesgos de Vulnerabilidad a menudo combinan las puntuaciones de CVSS y EPSS con contexto organizacional o ambiental adicional, como la criticidad de los activos o el impacto en el negocio.

Los proveedores y organizaciones a menudo desarrollan sus propios Modelos y Sistemas de Puntuación Propietarios adaptados a su tolerancia al riesgo y necesidades operativas específicas.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

- Desarrollar planes de acción para abordar primero las vulnerabilidades de alta prioridad, aprovechando la gestión de parches, cambios de configuración u otras estrategias de mitigación.
- Asignar plazos sensibles al tiempo y acuerdos de nivel de servicio correspondientes a los diferentes niveles de gravedad de las vulnerabilidades.
- Asignar recursos de manera efectiva para asegurar la remediación oportuna de las vulnerabilidades críticas.
- Informar a las partes interesadas relevantes sobre las vulnerabilidades priorizadas y los planes de remediación.

Un **Acuerdo de Nivel de Servicio** o **SLA** en la Gestión de Vulnerabilidades es un acuerdo **formal que define las expectativas, los plazos y las responsabilidades para abordar las vulnerabilidades de seguridad**. **Es esencial para garantizar que las vulnerabilidades se remedien de manera oportuna y eficiente**, reduciendo el riesgo de explotación y alineándose con los objetivos de seguridad de la organización.

Los SLA establecen plazos específicos para solucionar vulnerabilidades según su gravedad. Por ejemplo, las vulnerabilidades críticas podrían necesitar ser abordadas en un plazo de 24 a 72 horas, mientras que los problemas de menor riesgo podrían tener plazos más largos. Estos plazos aseguran que los riesgos más graves se prioricen y mitiguen rápidamente.

Los SLA se adaptan al apetito de riesgo de la organización y al impacto potencial de las vulnerabilidades. Por ejemplo, las vulnerabilidades críticas que podrían provocar incidentes de seguridad significativos, fugas de datos o interrupciones se abordan más rápidamente que los problemas menores.

2.4 REMEDIACIÓN

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

Planificación de la Remediación

- Desarrollar planes de acción para abordar primero las vulnerabilidades de alta prioridad, aprovechando la gestión de parches, cambios de configuración u otras estrategias de mitigación.

Asignación de Recursos.

- Asignar recursos de manera efectiva para garantizar la remediación oportuna de las vulnerabilidades críticas.

Comunicación.

- Informar a los interesados pertinentes sobre las vulnerabilidades priorizadas y los planes de remediación.

Establecer Mecanismos de Respaldo y Reversión.

- Crear copias de seguridad del sistema antes de aplicar parches o realizar cambios; asegurar que los sistemas o aplicaciones estén respaldados para permitir la recuperación en caso de problemas inesperados.
- Desarrollar planes y procedimientos de reversión para revertir rápidamente los cambios si las acciones de remediación provocan interrupciones o no abordan de manera efectiva las vulnerabilidades.

Realizar Pruebas Previas a la Remediación.

- Aplicar parches o cambios de configuración en un entorno de pruebas o sandbox para evaluar su impacto antes de implementarlos en producción.
- Evaluar de manera proactiva la compatibilidad para asegurarse de que las acciones de remediación no afecten negativamente el rendimiento del sistema, la funcionalidad o la compatibilidad con otras aplicaciones.

Sistemas Integrados de Seguimiento de Remediación y Herramientas de Seguimiento.

Al implementar herramientas de seguimiento de remediación y seguimiento, las organizaciones pueden transformar la gestión de vulnerabilidades de un proceso cíclico a un programa de mejora continua, mejorando significativamente la postura de seguridad mientras se mantiene la integridad operativa en entornos complejos.

Las herramientas de seguimiento de remediación son soluciones especializadas que **rastrean, validan e informan sobre la efectividad de los esfuerzos de remediación de vulnerabilidades en toda la organización**. Estas herramientas cierran la brecha entre la gestión de vulnerabilidades y la gestión de parches al proporcionar visibilidad continua del progreso de la remediación y validar que las brechas de seguridad se han cerrado realmente. Cuando se implementan correctamente, estos sistemas crean responsabilidad, visibilidad tangible a través de KPI dinámicos y aseguran que no queden vulnerabilidades sin abordar después de los intentos iniciales de remediación.

De manera similar, los tableros de remediación a nivel empresarial proporcionan a los equipos de seguridad y a la dirección visibilidad en tiempo real sobre el estado de la remediación, los plazos y la efectividad. Estas plataformas consolidan datos de diversas herramientas de seguridad para presentar una vista unificada del progreso de la remediación en relación con los SLA establecidos y los umbrales de riesgo.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Implementar acciones de remediación.

- Para entornos más grandes, considere implementar las acciones de remediación por etapas para monitorear posibles problemas y minimizar riesgos, si aplica a la estructura y arquitectura de su organización.
- Utilice herramientas de automatización para tareas como implementación de parches, cambios de configuración o actualizaciones de código para agilizar el proceso de remediación y reducir errores siempre que sea posible.

Validar la efectividad de la remediación

- Realice pruebas posteriores a la remediación para confirmar que la vulnerabilidad ha sido totalmente solucionada sin introducir nuevos problemas de seguridad o de funcionamiento.
- Utilice herramientas de escaneo de vulnerabilidades después de la remediación para asegurarse de que los problemas previamente identificados ya no existan.

Documentación y métricas.

- Registre todas las actividades de remediación, incluyendo acciones realizadas y sus respectivos resultados.
- Monitoree indicadores clave de desempeño para evaluar la efectividad del proceso.

Procesos y Servicios Posteriores a la Remediación.

Los procesos efectivos posteriores a la remediación incorporan pruebas de verificación que confirman que las vulnerabilidades se han resuelto realmente y no solo se han tratado de manera superficial**. La caza de amenazas (Threat Hunting) puede utilizarse en el contexto posterior a la remediación** como un enfoque de seguridad proactivo que va más allá del escaneo tradicional de vulnerabilidades, buscando activamente signos de actividad de adversarios que puedan haber ocurrido durante la ventana de exposición de la vulnerabilidad. La caza de amenazas puede considerarse una capa crítica de verificación que garantiza que los entornos permanezcan seguros después de las acciones de remediación**. TH emplea técnicas avanzadas de detección, incluyendo análisis de comportamiento, detección de anomalías y reconocimiento de patrones para identificar posibles indicadores de compromiso** que los escáneres de vulnerabilidades estándar podrían pasar por alto. Por ejemplo, aunque una vulnerabilidad crítica de ejecución remota de código (RCE) pueda haberse parchado, la caza de amenazas puede revelar si fue explotada antes de la

remediación examinando registros del sistema, patrones de tráfico de red y cambios en la integridad de archivos.

El proceso de Gestión de la Superficie de Ataque o ASM proporciona visibilidad continua de las superficies de ataque externas e internas de una organización, ayudando a los equipos de seguridad a comprender el contexto y el impacto potencial de las vulnerabilidades en toda la empresa. **ASM complementa la gestión tradicional de vulnerabilidades al ofrecer información en tiempo real sobre los niveles de exposición incluso después de los esfuerzos de remediación. Los servicios de ASM descubren e inventarían activos de manera continua, monitorean cambios en la superficie de ataque y proporcionan capacidades de priorización basadas en el contexto empresarial y la inteligencia de amenazas**. Por ejemplo, después de remediar una vulnerabilidad crítica en una aplicación de cara al público, ASM puede verificar que la solución se haya implementado correctamente en todas las instancias y alertar sobre cualquier nuevo despliegue que pueda reintroducir la vulnerabilidad.

2.6 LECCIONES APRENDIDAS

OBJETIVO: MEJORAR LOS PROCESOS FUTUROS DE RESPUESTA A INCIDENTES Y GESTIÓN DE VULNERABILIDADES.

- Analizar la efectividad de los procesos de priorización y remediación de vulnerabilidades.
- Incorporar los conocimientos obtenidos de la revisión en los procesos de CTI (ciberinteligencia de amenazas) y IRM (gestión de incidentes de respuesta) para mejorar la gestión futura de vulnerabilidades.
- Actualizar políticas, procedimientos y herramientas basándose en las lecciones aprendidas para mejorar el ciclo de vida general de la gestión de vulnerabilidades.
- Realizar una revisión post-incidente para evaluar la efectividad de la respuesta e identificar áreas de mejora.
- Actualizar los procesos de inteligencia de amenazas y gestión de vulnerabilidades basándose en las lecciones aprendidas.
- Compartir conocimientos y hallazgos con los interesados pertinentes para aumentar la conciencia organizacional y la preparación.
- Compilar un informe detallado del incidente, incluyendo las vulnerabilidades identificadas, las acciones tomadas y los resultados alcanzados.
- Utilizar la inteligencia de amenazas para proporcionar contexto y análisis del incidente, destacando tendencias y patrones.
- Distribuir el informe a los principales interesados y usarlo para informar las futuras estrategias de inteligencia de amenazas y respuesta a incidentes.

Retención de Conocimiento y Mejora Continua

La gestión del conocimiento en la respuesta a vulnerabilidades representa un componente crítico para construir la resiliencia organizacional y prevenir la recurrencia de explotaciones efectivas. El conocimiento valioso a menudo queda atrapado en entornos aislados, lo que impide un verdadero aprendizaje organizacional y conduce a errores de seguridad repetidos. La gestión efectiva del conocimiento transforma las experiencias individuales en sabiduría institucional al capturar sistemáticamente los enfoques de remediación, las estrategias de mitigación y los procesos de toma de decisiones que funcionaron —o no funcionaron— durante los incidentes de seguridad.

La recopilación y análisis sistemático de las lecciones aprendidas durante la remediación de vulnerabilidades crea un ciclo de retroalimentación que fortalece continuamente la postura de seguridad de una organización. Al documentar casi incidentes, mitigaciones exitosas y desafíos de remediación, los equipos de seguridad construyen una memoria institucional que se vuelve cada vez más valiosa con el tiempo. Este repositorio de conocimiento permite a las organizaciones destacar los incidentes de seguridad evitados, cuantificando así los "no eventos" que representan intervenciones de seguridad exitosas, lo que ayuda a demostrar el

valor de las inversiones en seguridad y los esfuerzos de remediación proactivos a la dirección.

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
Red Team	Entidades de seguridad ofensiva que simulan ataques reales contra los sistemas de la organización para probar las defensas.
Blue Team	Personal de defensa (SOC, CERT) encargado de detectar, investigar y mitigar las amenazas.
White Team	Miembros que actúan como árbitros o coordinadores del ejercicio, con quienes se debe validar si un incidente es una simulación o un atacante real.
Purple Team	Un enfoque de mejora continua donde se integran conocimientos de ataque y defensa; pueden encargarse de dar seguimiento al plan de acción post-ejercicio.
TTPs (Tactics, Techniques, and Procedures)	Patrones de ataque, métodos y técnicas comúnmente empleados por actores de amenazas avanzados.
Rules of Engagement (Reglas de Compromiso):	Documentación formal que define los límites, objetivos y alcances del ejercicio de Red Team.
Getting-out-of-Jail Card	Documento de autorización que certifica que las actividades sospechosas detectadas son parte de un ejercicio autorizado.
Reconocimiento de Red	Intentos de los atacantes por mapear la infraestructura y sistemas activos.
Mecanismos de Persistencia	Métodos (como backdoors o webshells) que el Red Team deja en los sistemas para mantener el acceso a largo plazo.
Red Button (Botón Rojo)	Control procedimental para detener inmediatamente todas las actividades del Red Team en caso de necesidad operativa o impacto real en producción.
Infraestructura Roja	Elementos técnicos (servidores, dominios) utilizados por el equipo ofensivo para ejecutar el ataque.

C2 (Command and Control)	Centros de comando identificados desde los cuales se controla la intrusión; el IRM sugiere bloquear el tráfico hacia ellos una vez detectados.
Endurecimiento (Harden system configurations)	Refuerzo de las configuraciones de seguridad, como limitar privilegios de usuario y desactivar servicios innecesarios, para prevenir futuras explotaciones.
Triaje	Proceso de evaluación inicial para determinar si una alerta de seguridad es un ejercicio de Red Team o una amenaza real.
Lateralización (Lateral Movement)	Movimientos del atacante a través de la red después del compromiso inicial; el documento refiere al IRM 18 para este escenario.
Remasterización de Sistemas	Acción de reconstruir sistemas desde cero o desde copias de seguridad seguras durante la fase de recuperación.