Vectores de ataque

Los incidentes pueden ocurrir de innumerables maneras, por lo que no es factible desarrollar instrucciones paso a paso para manejar cada incidente. Las organizaciones deberían estar generalmente preparadas para manejar cualquier incidente, pero deberían centrarse en estar preparadas para manejar incidentes que usan vectores de ataque comunes. Los diferentes tipos de incidentes merecen diferentes estrategias de respuesta. Los vectores de ataque enumerados a continuación no están destinados a proporcionar una clasificación definitiva para los incidentes; más bien, simplemente enumeran métodos comunes de ataque, que pueden usarse como base para definir procedimientos de manejo más específicos.

- Medios externos / extraíbles: un ataque ejecutado desde medios extraíbles o un dispositivo periférico, por ejemplo, código malicioso que se propaga a un sistema desde una unidad flash USB infectada.
- Desgaste: un ataque que emplea métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios (por ejemplo, un DDoS destinado a perjudicar o negar el acceso a un servicio o aplicación; un ataque de fuerza bruta contra un mecanismo de autenticación, como como contraseñas, CAPTCHAS o firmas digitales).
- Web: un ataque ejecutado desde un sitio web o una aplicación basada en la web, por ejemplo, un ataque de secuencias de comandos entre sitios utilizado para robar credenciales o una redirección a un sitio que explota una vulnerabilidad del navegador e instala malware.
- Correo electrónico: un ataque ejecutado a través de un mensaje de correo electrónico o un archivo adjunto, por ejemplo, un código de explotación disfrazado de documento adjunto o un enlace a un sitio web malicioso en el cuerpo de un mensaje de correo electrónico.
- Suplantación de identidad: un ataque que implica el reemplazo de algo benigno con algo malicioso, por ejemplo, suplantación de identidad, ataques de intermediario, puntos de acceso inalámbrico no autorizados y ataques de inyección SQL, todo implica suplantación de identidad.
- Uso inapropiado: cualquier incidente que resulte de la violación de las políticas de uso aceptable de una organización por un usuario autorizado, excluyendo las categorías anteriores; por ejemplo, un usuario instala software para compartir archivos, lo que lleva a la pérdida de datos confidenciales; o un usuario realiza actividades ilegales en un sistema.
- Pérdida o robo de equipo: la pérdida o robo de un dispositivo informático o medio utilizado por la organización, como una computadora portátil, teléfono inteligente o token de autenticación.
- Otro: Un ataque que no encaja en ninguna de las otras categorías. Esta sección se centra en las prácticas recomendadas para manejar cualquier tipo de incidente. Está fuera del alcance de esta publicación dar consejos específicos basados en los vectores de ataque; tales pautas se proporcionarían en publicaciones separadas que aborden otros temas de manejo de incidentes, como NIST SP 800-83 sobre prevención y manejo de incidentes de malware.

Señales de un incidente

Para muchas organizaciones, la parte más desafiante del proceso de respuesta a incidentes es detectar y evaluar con precisión los posibles incidentes, determinando si ha ocurrido un incidente y, de ser así, el tipo, el alcance y la magnitud del problema. Lo que hace que esto sea tan desafiante es una combinación de tres factores:

- Los incidentes pueden detectarse a través de muchos medios diferentes, con diferentes niveles de detalle y fidelidad. Las capacidades de detección automatizada incluyen IDPS basados en red y en host, software antivirus y analizadores de registros. Los incidentes también pueden detectarse a través de medios manuales, como problemas informados por los usuarios. Algunos incidentes tienen signos evidentes que pueden detectarse fácilmente, mientras que otros son casi imposibles de detectar.
- El volumen de posibles signos de incidentes suele ser alto; por ejemplo, no es raro que una organización reciba miles o incluso millones de alertas de sensores de detección de intrusos por día. (Consulte la Sección 3.2.4 para obtener información sobre el análisis de tales alertas).
- Se necesitan conocimientos técnicos especializados y profundos y una amplia experiencia para un análisis adecuado y eficiente de los datos relacionados con incidentes. Los signos de un incidente se dividen en una de dos categorías: precursores e indicadores. Un precursor es una señal de que puede ocurrir un incidente en el futuro. Un indicador es una señal de que un incidente puede haber ocurrido o puede estar ocurriendo ahora. La mayoría de los ataques no tienen precursores identificables o detectables desde la perspectiva del objetivo. Si se detectan precursores, la organización puede tener la oportunidad de prevenir el incidente alterando su postura de seguridad para salvar a un objetivo del ataque. Como mínimo, la organización podría monitorear la actividad que involucra al objetivo más de cerca. Ejemplos de precursores son:
    - Entries Entradas de registro del servidor web que muestran el uso de un escáner de vulnerabilidades
    - Un anuncio de un nuevo exploit que se dirige a una vulnerabilidad del servidor de correo de la organización
    - Una amenaza de un grupo que indica que el grupo atacará a la organización. Si bien los precursores son relativamente raros, los indicadores son demasiado comunes. Existen demasiados tipos de indicadores para enumerarlos exhaustivamente, pero a continuación se enumeran algunos ejemplos:
        - Sensor Un sensor de detección de intrusiones en la red alerta cuando se produce un intento de desbordamiento de búfer contra un servidor de base de datos.
        - El software antivirus alerta cuando detecta que un host está infectado con malware.
        - Administrator Un administrador del sistema ve un nombre de archivo con caracteres inusuales.

- Host Un host registra un cambio de configuración de auditoría en su registro.
- Una aplicación registra múltiples intentos fallidos de inicio de sesión desde un sistema remoto desconocido.
- Un administrador de correo electrónico ve una gran cantidad de correos electrónicos rechazados con contenido sospechoso.
- Un administrador de red nota una desviación inusual de los flujos de tráfico de red típicos

Fuentes comunes de precursores e indicadores

Alertas

IDPSs Los productos IDPS identifican eventos sospechosos y registran los datos pertinentes sobre ellos, incluida la fecha y la hora en que se detectó el ataque, el tipo de ataque, las direcciones IP de origen y destino y el nombre de usuario (si corresponde y se conoce). La mayoría de los productos IDPS usan firmas de ataque para identificar actividades maliciosas; las firmas deben mantenerse actualizadas para que se puedan detectar los ataques más recientes. El software IDPS a menudo produce falsos positivos: alertas que indican que se está produciendo actividad maliciosa, cuando en realidad no ha habido ninguna. Los analistas deben validar manualmente las alertas de IDPS ya sea revisando de cerca los datos de respaldo registrados o obteniendo datos relacionados de otras fuentes.

SIEMs Los productos de información de seguridad y gestión de eventos (SIEM) son similares a los productos IDPS, pero generan alertas basadas en el análisis de los datos de registro (ver más abajo).

Antivirus and antispam software El software antivirus detecta varias formas de malware, genera alertas y evita que el malware infecte a los hosts. Los productos antivirus actuales son efectivos para detener muchas instancias de malware si sus firmas se mantienen actualizadas. El software antispam se utiliza para detectar spam y evitar que llegue a los buzones de los usuarios. El spam puede contener malware, ataques de phishing y otro contenido malicioso, por lo que las alertas del software antispam pueden indicar intentos de ataque.

Software de comprobación de integridad de archivos El software de comprobación de integridad de archivos puede detectar cambios realizados en archivos importantes durante incidentes. Utiliza un algoritmo hash para obtener una suma de verificación criptográfica para cada archivo designado. Si se altera el archivo y se vuelve a calcular la suma de verificación, existe una probabilidad extremadamente alta de que la nueva suma de verificación no coincida con la suma de verificación anterior. Al recalcular regularmente las sumas de verificación y compararlas con valores anteriores, se pueden detectar cambios en los archivos.

Servicios de monitoreo de terceros. Los terceros ofrecen una variedad de servicios de monitoreo gratuitos y basados en suscripción. Un ejemplo son los servicios de detección de fraude que notificarán a una organización si sus direcciones IP, nombres de dominio, etc. están asociados con actividades de incidentes actuales que involucran a otras organizaciones. También hay listas negras gratuitas en tiempo real con información similar. Otro ejemplo de un servicio de monitoreo de terceros es una lista de notificaciones CSIRC; Estas listas a menudo están disponibles solo para otros equipos de respuesta a incidentes.

Logs

Sistema operativo, servicio y registros de aplicaciones Los registros de los sistemas operativos, los servicios y las aplicaciones (en particular, los datos relacionados con la auditoría) suelen ser de gran valor cuando se produce un incidente, como el registro de las cuentas a las que se accedió y las acciones realizadas. Las organizaciones deben requerir un nivel de inicio de sesión en todos los sistemas y un nivel de referencia más alto en los sistemas críticos.

Los registros se pueden usar para el análisis correlacionando información de eventos. Dependiendo de la información del evento, se puede generar una alerta para indicar un incidente. La Sección 3.2.4 discute el valor del registro centralizado.

Registros de dispositivos de red Los registros de dispositivos de red como firewalls y enrutadores no suelen ser una fuente primaria de precursores o indicadores. Aunque estos dispositivos generalmente están configurados para registrar intentos de conexión bloqueados, proporcionan poca información sobre la naturaleza de la actividad. Aún así, pueden ser valiosos para identificar tendencias de red y para correlacionar eventos detectados por otros dispositivos.

Flujos de red Un flujo de red es una sesión de comunicación particular que ocurre entre hosts. Los enrutadores y otros dispositivos de red pueden proporcionar información de flujo de red, que se puede utilizar para encontrar actividad de red anómala causada por malware, exfiltración de datos y otros actos maliciosos. Existen muchos estándares para los formatos de datos de flujo, incluidos NetFlow, sFlow e IPFIX.

Información disponible públicamente

Información sobre nuevas vulnerabilidades y exploits. Mantenerse al día con las nuevas vulnerabilidades y exploits puede evitar que ocurran algunos incidentes y ayudar a detectar y analizar nuevos ataques. La Base Nacional de Datos de Vulnerabilidad (NVD) contiene información sobre vulnerabilidades.32 Organizaciones como US-CERT33 y CERT® / CC proporcionan periódicamente información de actualización de amenazas a través de resúmenes, publicaciones en la web y listas de correo.

Personas de la organización. Los usuarios, los administradores del sistema, los administradores de la red, el personal de seguridad y otros miembros de la organización pueden informar signos de incidentes. Es importante validar todos estos informes. Un enfoque es preguntar a las personas que proporcionan dicha información qué tan seguros están de la exactitud de la información. Registrar esta estimación junto con la información proporcionada puede ayudar considerablemente durante el análisis de incidentes, particularmente cuando se descubren datos conflictivos.

Personas de otras organizaciones Los informes de incidentes que se originan externamente deben tomarse en serio. Por ejemplo, una organización puede contactar a la organización alegando que un sistema en la organización está atacando sus sistemas. Los usuarios externos también pueden informar otros indicadores, como una página web desfigurada o un servicio no disponible. Otros equipos de respuesta a incidentes también pueden informar incidentes. Es importante contar con mecanismos para que las partes externas informen los indicadores y para que el personal capacitado monitoree esos mecanismos cuidadosamente; Esto puede ser tan simple como configurar un número de teléfono y una dirección de correo electrónico, configurados para reenviar mensajes a la mesa de ayuda.

3.2.4 Análisis de incidents

La detección y análisis de incidentes sería fácil si se garantizara que cada precursor o indicador sea exacto; Por desgracia, este no es el caso. Por ejemplo, los indicadores proporcionados por el usuario, como una queja de que un servidor no está disponible, a menudo son incorrectos. Los sistemas de detección de intrusos pueden producir falsos positivos, indicadores incorrectos.

Estos ejemplos demuestran lo que hace que la detección y el análisis de incidentes sean tan difíciles: idealmente, cada indicador debe evaluarse para determinar si es legítimo. Para empeorar las cosas, el número total de indicadores puede ser de miles o millones por día. Encontrar los incidentes de seguridad reales que ocurrieron en todos los indicadores puede ser una tarea desalentadora.

Incluso si un indicador es exacto, no necesariamente significa que ha ocurrido un incidente. Algunos indicadores, como un bloqueo del servidor o la modificación de archivos críticos, pueden ocurrir por varias razones además de un incidente de seguridad, incluido un error humano. Sin embargo, dada la aparición de indicadores, es razonable sospechar que podría estar ocurriendo un incidente y actuar en consecuencia. Determinar si un evento en particular es realmente un incidente es a veces una cuestión de juicio.

Puede ser necesario colaborar con otro personal técnico y de seguridad de la información para tomar una decisión. En muchos casos, una situación debe manejarse de la misma manera, independientemente de si está relacionada con la seguridad. Por ejemplo, si una organización está perdiendo conectividad a Internet cada 12 horas y nadie conoce la causa, el personal querría resolver el problema con la misma rapidez y utilizaría los mismos recursos para diagnosticar el problema, independientemente de su causa. Algunos incidentes son fáciles de detectar, como una página web obviamente desfigurada. Sin embargo, muchos incidentes no están asociados con síntomas tan claros. Pequeños signos como un cambio en un archivo de configuración del sistema pueden ser los únicos indicadores de que ha ocurrido un incidente. En el manejo de incidentes, la detección puede ser la tarea más difícil.

Los manejadores de incidentes son responsables de analizar los síntomas ambiguos, contradictorios e incompletos para determinar qué ha sucedido. Aunque existen soluciones técnicas que pueden facilitar la detección, el mejor remedio es crear un equipo de miembros del personal altamente experimentados y competentes que puedan analizar los precursores e indicadores de manera efectiva y eficiente y tomar las medidas apropiadas. Sin un personal bien capacitado y capaz, la detección y el análisis de incidentes se realizarán de manera ineficiente y se cometerán errores costosos. El equipo de respuesta a incidentes debe trabajar rápidamente para analizar y validar cada incidente, siguiendo un proceso predefinido y documentando cada paso dado.

Cuando el equipo cree que ha ocurrido un incidente, el equipo debe realizar rápidamente un análisis inicial para determinar el alcance del incidente, como qué redes, sistemas o aplicaciones están afectados; quién o qué originó el incidente; y cómo está ocurriendo el incidente (por ejemplo, qué herramientas o métodos de ataque se están utilizando, qué vulnerabilidades se están explotando). El análisis inicial debe proporcionar suficiente información para que el equipo priorice las actividades posteriores, como la contención del incidente y un análisis más profundo de los efectos del incidente.

Realizar el análisis inicial y la validación es un desafío. Las siguientes son recomendaciones para hacer que el análisis de incidentes sea más fácil y más efectivo:

- Perfil de redes y sistemas. La elaboración de perfiles mide las características de la actividad esperada para que los cambios en ella se puedan identificar más fácilmente. Ejemplos de creación de perfiles son la ejecución de software de comprobación de integridad de archivos en hosts para obtener sumas de comprobación para archivos críticos y la supervisión del uso del ancho de banda de la red para determinar cuáles son los niveles de uso promedio y máximo en varios días y horas. En la práctica, es difícil detectar incidentes con precisión utilizando la mayoría de las técnicas de creación de perfiles; Las organizaciones deben utilizar la creación de perfiles como una de varias técnicas de detección y análisis.
- Comprender los comportamientos normales. Los miembros del equipo de respuesta a incidentes deben estudiar redes, sistemas y aplicaciones para comprender cuál es su comportamiento normal para que el comportamiento anormal pueda reconocerse más fácilmente. Ningún controlador de incidentes tendrá un conocimiento exhaustivo de todos los comportamientos en todo el entorno, pero los controladores deben saber qué expertos podrían llenar los vacíos. Una forma de obtener este conocimiento es mediante la revisión de entradas de registro y alertas de seguridad. Esto puede ser tedioso si el filtrado no se utiliza para condensar los

registros a un tamaño razonable. A medida que los manejadores se familiaricen con los registros y alertas, deberían poder concentrarse en las entradas inexplicables, que generalmente son más importantes para investigar. La realización de revisiones frecuentes de registros debe mantener el conocimiento actualizado, y el analista debe ser capaz de notar tendencias y cambios a lo largo del tiempo. Las revisiones también le dan al analista una indicación de la confiabilidad de cada fuente.

- Crear una política de retención de registros. La información sobre un incidente puede registrarse en varios lugares, como firewall, IDPS y registros de aplicaciones. Crear e implementar una política de retención de registros que especifique cuánto tiempo se deben mantener los datos de registro puede ser extremadamente útil en el análisis porque las entradas de registro anteriores pueden mostrar actividad de reconocimiento o instancias anteriores de ataques similares. Otra razón para retener los registros es que los incidentes pueden no ser descubiertos hasta días, semanas o incluso meses después. El período de tiempo para mantener los datos de registro depende de varios factores, incluidas las políticas de retención de datos de la organización y el volumen de datos. Consulte NIST SP 800-92, Guía para la administración de registros de seguridad informática para obtener recomendaciones adicionales relacionadas con el registro.
- Realizar correlación de eventos. La evidencia de un incidente puede capturarse en varios registros que contienen diferentes tipos de datos: un registro de firewall puede tener la dirección IP de origen que se utilizó, mientras que un registro de aplicación puede contener un nombre de usuario. Un IDPS de red puede detectar que se lanzó un ataque contra un host en particular, pero puede no saber si el ataque fue exitoso.

Es posible que el analista deba examinar los registros del host para determinar esa información. La correlación de eventos entre múltiples fuentes de indicadores puede ser invaluable para validar si ocurrió un incidente en particular.

- Mantenga todos los relojes de host sincronizados. Los protocolos como el Protocolo de tiempo de red (NTP) sincronizan los relojes entre los hosts.35 La correlación de eventos será más complicada si los dispositivos que informan eventos tienen configuraciones de reloj inconsistentes. Desde un punto de vista probatorio, es preferible tener marcas de tiempo constantes en los registros; por ejemplo, tener tres registros que muestren que se produjo un ataque a las 12:07:01 am, en lugar de registros que indiquen que el ataque ocurrió a las 12:07:01 , 12:10:35 y 11:07:06.
- Mantener y utilizar una base de información de conocimiento. La base de conocimiento debe incluir información que los manejadores necesitan para hacer referencia rápidamente durante el análisis de incidentes. Aunque es posible construir una base de conocimiento con una estructura compleja, un enfoque simple puede ser efectivo. Los documentos de texto, las hojas de cálculo y las bases de datos relativamente simples proporcionan mecanismos efectivos, flexibles y de búsqueda para compartir datos entre los miembros del equipo. La base de conocimientos también debe contener una variedad de información, incluidas explicaciones sobre la importancia y la validez de los precursores e indicadores, como las alertas IDPS, las entradas del registro del sistema operativo y los códigos de error de la aplicación.
- Utilice los motores de búsqueda de Internet para la investigación. Los motores de búsqueda en Internet pueden ayudar a los analistas a encontrar información sobre actividades inusuales. Por ejemplo, un analista puede ver algunos intentos de conexión inusuales dirigidos al puerto TCP 22912. Realizar una búsqueda en los términos "TCP", "puerto" y "22912" puede devolver algunos resultados que contienen registros de actividad similar o incluso una explicación del importancia del número de puerto. Tenga en cuenta que se deben utilizar estaciones de trabajo separadas para la investigación a fin de minimizar el riesgo para la organización de realizar estas búsquedas.
- Ejecute Sniffers de paquetes para recopilar datos adicionales. A veces, los indicadores no registran suficientes detalles para permitir que el controlador entienda lo que está ocurriendo. Si se produce un incidente en una red, la forma más rápida de recopilar los datos necesarios puede ser que un sniffer de paquetes capture el tráfico de la red. La configuración del rastreador para registrar el tráfico que coincide con los criterios especificados debería mantener el volumen de datos manejable y minimizar la captura accidental de otra información. Debido a problemas de privacidad, algunas organizaciones pueden requerir que los manejadores de incidentes soliciten y reciban permiso antes de usar rastreadores de paquetes.
- Filtrar los datos. Simplemente no hay tiempo suficiente para revisar y analizar todos los indicadores; como mínimo, se debe investigar la actividad más sospechosa. Una estrategia efectiva es filtrar categorías de indicadores que tienden a ser insignificantes. Otra estrategia de filtrado es mostrar solo las categorías de indicadores que son de la mayor importancia; sin embargo, este enfoque conlleva un riesgo considerable porque la nueva actividad maliciosa puede no caer en una de las categorías de indicadores elegidos.
- Busque ayuda de otros. Ocasionalmente, el equipo no podrá determinar la causa completa y la naturaleza de un incidente. Si el equipo carece de información suficiente para contener y erradicar el incidente, entonces debe consultar con recursos internos (por ejemplo, personal de seguridad de la información) y recursos externos (por ejemplo, US-CERT, otros CSIRT, contratistas con experiencia en respuesta a incidentes). Es importante determinar con precisión la causa de cada incidente para que pueda estar completamente contenido y las vulnerabilidades explotadas puedan mitigarse para evitar que ocurran incidentes similares.

3.2.5 Documentación de incidentes

Un equipo de respuesta a incidentes que sospeche que ha ocurrido un incidente debe comenzar inmediatamente a registrar todos los hechos relacionados con el incidente.36 Un libro de registro es un medio eficaz y simple para esto, 37 pero las computadoras portátiles, grabadoras de audio y cámaras digitales también pueden servir para este propósito.38 Documentar los eventos del sistema, las conversaciones y los cambios observados en los archivos puede conducir a un manejo del problema más eficiente, más sistemático y menos propenso a errores. Cada paso dado desde el momento en que se detectó el incidente hasta su resolución final debe documentarse y marcarse con el tiempo. Todos los documentos relacionados con el incidente deben estar fechados y firmados por el responsable del incidente. La información de

esta naturaleza también se puede usar como evidencia en un tribunal de justicia si se persigue el enjuiciamiento legal. Siempre que sea posible, los manejadores deben trabajar en equipos de al menos dos: una persona puede registrar y registrar eventos mientras que la otra persona realiza las tareas técnicas. La Sección 3.3.2 presenta más información acerca de la evidencia.39 El equipo de respuesta a incidentes debe mantener registros sobre el estado de los incidentes, junto con otra información pertinente.40 El uso de una aplicación o una base de datos, como un sistema de seguimiento de problemas, ayuda a asegurar que los incidentes sean manejado y resuelto de manera oportuna. El sistema de seguimiento de problemas debe contener información sobre lo siguiente:

- El estado actual del incidente (nuevo, en progreso, enviado para investigación, resuelto, etc.)
- Un resumen del incidente ・Indicadores relacionados con el incidente
- Otros incidentes relacionados con este incidente
- Acciones tomadas por todos los manejadores de incidentes en este incidente
- Cadena de custodia, si corresponde
- Evaluaciones de impacto relacionadas con el incidente
- Información de contacto para otras partes involucradas (por ejemplo, propietarios del sistema, administradores del sistema)
- Una lista de evidencia reunida durante la investigación del incidente
- Comentarios de los manejadores de incidentes
- Próximos pasos a seguir (por ejemplo, reconstruir el host, actualizar una aplicación).

El equipo de respuesta a incidentes debe proteger los datos de incidentes y restringir el acceso a ellos porque a menudo contiene información confidencial, por ejemplo, datos sobre vulnerabilidades explotadas, brechas de seguridad recientes y usuarios que pueden haber realizado acciones inapropiadas. Por ejemplo, solo el personal autorizado debe tener acceso a la base de datos de incidentes. Las comunicaciones de incidentes (por ejemplo, correos electrónicos) y los documentos deben estar encriptados o protegidos de otra manera para que solo el personal autorizado pueda leerlos.

3.2.6 Priorización de incidentes

Dar prioridad al manejo del incidente es quizás el punto de decisión más crítico en el proceso de manejo del incidente. Los incidentes no deben manejarse por orden de llegada como resultado de las limitaciones de recursos. En cambio, el manejo debe priorizarse en función de los factores relevantes, como los siguientes:

- Impacto funcional del incidente. Los incidentes que se dirigen a los sistemas de TI generalmente afectan la funcionalidad comercial que proporcionan esos sistemas, lo que resulta en algún tipo de impacto negativo para los usuarios de esos sistemas. Los manejadores de incidentes deben considerar cómo el incidente afectará la funcionalidad existente de los sistemas afectados. Los manejadores de incidentes deben considerar no solo el impacto funcional actual del incidente, sino también el posible impacto funcional futuro del incidente si no se contiene de inmediato.
- Impact Información del impacto del incidente. Los incidentes pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización. Por ejemplo, un agente malintencionado puede filtrar información confidencial. Los manejadores de incidentes deben considerar cómo esta filtración de información afectará la misión general de la organización. Un incidente que resulta en la exfiltración de información sensible también puede afectar a otras organizaciones si alguno de los datos pertenece a una organización asociada.
- Recuperación del incidente. El tamaño del incidente y el tipo de recursos que afecta determinarán la cantidad de tiempo y recursos que deben gastarse en recuperarse de ese incidente. En algunos casos, no es posible recuperarse de un incidente (por ejemplo, si se ha comprometido la confidencialidad de la información confidencial) y no tendría sentido gastar recursos limitados en un ciclo de manejo de incidentes alargado, a menos que ese esfuerzo se haya dirigido a garantizar que un incidente similar no ocurrió en el futuro. En otros casos, un incidente puede requerir muchos más recursos para manejar que lo que una organización tiene disponible.

Los manejadores de incidentes deben considerar el esfuerzo necesario para recuperarse realmente de un incidente y compararlo cuidadosamente con el valor que creará el esfuerzo de recuperación y cualquier requisito relacionado con el manejo de incidentes.

La combinación del impacto funcional en los sistemas de la organización y el impacto en la información de la organización determina el impacto comercial del incidente; por ejemplo, un ataque distribuido de denegación de servicio contra un servidor web público puede reducir temporalmente la funcionalidad para los usuarios que intentan acceder al servidor, mientras que el acceso no autorizado de nivel raíz a un servidor web público puede dar lugar a la filtración de información de identificación personal (PII), lo que podría tener un impacto duradero en la reputación de la organización.

La capacidad de recuperación del incidente determina las posibles respuestas que el equipo puede tomar al manejar el incidente. Un incidente con un alto impacto funcional y bajo esfuerzo para recuperarse es un candidato ideal para la acción inmediata del equipo. Sin embargo, algunos incidentes pueden no tener rutas de recuperación sin problemas y es posible que deba ponerse en cola para obtener una respuesta de nivel más estratégico; por ejemplo, un incidente que resulta en un atacante exfiltrando y publicando gigabytes de datos confidenciales no tiene una ruta de recuperación fácil ya que los datos ya está expuesto; en este caso, el equipo puede transferir parte de la responsabilidad del manejo del incidente de exfiltración de datos a un equipo de nivel más estratégico que desarrolle una estrategia para prevenir futuras infracciones y cree un plan de divulgación para alertar a aquellas personas u organizaciones cuyos datos se extrajeron. El equipo debe

priorizar la respuesta a cada incidente en función de su estimación del impacto comercial causado por el incidente y los esfuerzos estimados necesarios para recuperarse del incidente. Una organización puede cuantificar mejor el efecto de sus propios incidentes debido a su conciencia situacional. La Tabla 3-2 proporciona ejemplos de categorías de impacto funcional que una organización podría usar para calificar sus propios incidentes. Los incidentes de calificación pueden ser útiles para priorizar recursos limitados.

Tabla 3-2. Categorías de impacto funcional

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Table 3-3 provides examples of possible information impact categories that describe the extent of information compromise that occurred during the incident. In this table, with the exception of the 'None' value, the categories are not mutually exclusive and the organization could choose more than one.

Table 3-3. Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table 3-4 shows examples of recoverability effort categories that reflect the level of and type of resources required to recover from the incident.

Table 3-4. Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Las organizaciones también deben establecer un proceso de escalamiento para aquellas instancias en las que el equipo no responde a un incidente dentro del tiempo designado. Esto puede suceder por muchas razones: por ejemplo, los teléfonos celulares pueden fallar o las personas pueden tener emergencias personales. El proceso de escalamiento debe indicar cuánto tiempo una persona debe esperar una respuesta y qué hacer si no se produce una respuesta. Generalmente, el primer paso es duplicar el contacto inicial. Después de esperar un breve tiempo, quizás 15 minutos, la persona que llama debe escalar el incidente a un nivel superior, como el gerente del equipo de respuesta a incidentes. Si esa persona no responde dentro de un cierto tiempo, entonces el incidente debe escalarse nuevamente a un nivel superior de gestión. Este proceso debe repetirse hasta que alguien responda.

3.2.7 Notificación de incidentes Cuando se analiza y prioriza un incidente, el equipo de respuesta a incidentes debe notificar a las personas apropiadas para que todos los que necesiten participar desempeñen sus funciones. Las políticas de respuesta a incidentes deben incluir disposiciones relativas a la notificación de incidentes, como mínimo, qué se debe informar a quién y en qué momentos (por ejemplo, notificación inicial, actualizaciones periódicas del estado). Los requisitos de informes exactos varían entre las organizaciones, pero las partes que generalmente se notifican incluyen:

- CIO
- Jefe de seguridad de la información
- Oficial de seguridad de información local
- Otros equipos de respuesta a incidentes dentro de la organización
- Equipos externos de respuesta a incidentes (si corresponde)
- Propietario del sistema
- Recursos humanos (para casos que involucran a empleados, como acoso por correo electrónico)
- Asuntos públicos (para incidentes que pueden generar publicidad)
- Departamento legal (para incidentes con posibles ramificaciones legales)
- US-CERT (requerido para agencias y sistemas federales operados en nombre del gobierno federal; consulte la Sección 2.3.4.3)
- Aplicación de la ley (si corresponde)

Durante el manejo de incidentes, el equipo puede necesitar proporcionar actualizaciones de estado a ciertas partes, incluso en algunos casos a toda la organización. El equipo debe planificar y preparar varios métodos de comunicación, incluidos los métodos fuera de banda (por ejemplo, en persona, en papel), y seleccionar los métodos que sean apropiados para un incidente en particular.

Los posibles métodos de comunicación incluyen:

- Correo electrónico
- Sitio web (interno, externo o portal)
- Llamadas telefónicas
- En persona (por ejemplo, sesiones informativas diarias)
- Greeting Saludo del buzón de voz (por ejemplo, configure un buzón de voz separado para actualizaciones de incidentes y actualice el mensaje de saludo para reflejar el estado actual del incidente; use el saludo del buzón de voz de la mesa de ayuda)
- Papel (por ejemplo, publicar avisos en tableros de anuncios y puertas, entregar avisos en todos los puntos de entrada).