SOPHOS

Guía de planificación de la respuesta a incidentes de Sophos

Contenido

Introducción

Este documento se ha diseñado para ofrecer una presentación completa de las prácticas recomendadas en respuesta a incidentes y orientar en el análisis de las ciberamenazas tanto en el aspecto técnico como en el organizativo. El objetivo de esta guía es ayudar a las empresas a desarrollar procesos de respuesta a incidentes efectivos.

Dirigida a profesionales de la seguridad de la información en cargos técnicos u organizativos, así como a principiantes sin experiencia previa en ciberseguridad, esta guía sirve de introducción a la respuesta a incidentes. Tenga en cuenta que no hace referencia exhaustiva a los marcos legales y normativos para la gestión de la seguridad de la información. Debe utilizarse como material complementario junto con las directrices de respuesta y divulgación de filtraciones aplicables específicas de su organización. Asimismo, el rol de los ciberseguros debe valorarse aparte, ya que las pólizas pueden contener pautas que difieren de las recomendaciones incluidas en esta guía de respuesta a incidentes.

Una estrategia eficaz de preparación ante ciberincidentes proporciona a las organizaciones protocolos y procedimientos establecidos que les permiten reaccionar ante los riesgos, asignarlos y contenerlos con mayor rapidez. El propósito de este documento es ayudar a establecer los procesos de respuesta a incidentes en la fase de preparación de un ciclo de vida de gestión de incidentes y, en última instancia, minimizar el impacto financiero y operativo para las organizaciones al permitir una contención más rápida de los ciberincidentes.

Recomendamos a los profesionales de la seguridad que incorporen estos conceptos y métodos de investigación en sus propios planes y procesos de respuesta a incidentes según sea necesario. Esta guía puede leerse de principio a fin o por secciones, centrándose en las más relevantes para el lector. Aunque no ofrece un plan detallado y definitivo para gestionar los ciberincidentes, está pensada para ayudar a los equipos de seguridad a preparar y establecer sus propios procesos.

Las fases de gestión de incidentes descritas en esta guía están en la línea del marco de respuesta a incidentes recomendado por la SANS, que consiste en seis fases diferenciadas. Este marco hace hincapié en cada una de las fases del ciclo de vida de la gestión de incidentes y se ha diseñado para ayudar a los profesionales de la seguridad a prepararse para responder de forma efectiva a los incidentes. No obstante, no pretende ser un manual de estrategias. Los ciberincidentes son dinámicos y, aunque los marcos proporcionan una estructura necesaria para una estrategia general, el criterio profesional de los expertos en seguridad y la concienciación en materia de seguridad de los empleados son fundamentales para lidiar con estos incidentes.

Preparación

La primera fase del ciclo de respuesta a incidentes es la fase de preparación. Las actividades y los esfuerzos realizados durante esta fase influyen significativamente en la eficiencia y eficacia de las subsiguientes fases. En consecuencia, la fase de preparación no es solo crucial, sino que también debe revisarse y actualizarse regularmente. Los elementos de la fase de preparación comprenden aspectos tanto no técnicos, por ejemplo procesos y procedimientos, como componentes técnicos, tales como el endurecimiento del sistema, la recopilación de telemetría y la formación. Al dedicar el tiempo y los recursos necesarios a la preparación, las organizaciones pueden poner los cimientos para una estrategia de respuesta a incidentes robusta y resiliente.

Procesos y procedimientos

Unos procesos y procedimientos bien documentados son esenciales para el correcto funcionamiento del equipo de respuesta a incidentes. Al diseñar y distribuir estas directrices entre el personal seleccionado para participar en el proceso de gestión de incidentes, podrá garantizar la integridad de la información y la armonización de objetivos entre todas las partes interesadas. Contar con procesos y procedimientos claramente definidos ayuda a mantener la coherencia en la estrategia del equipo, facilita la comunicación y contribuye a una respuesta ágil y coordinada a los ciberincidentes.

Plan de gestión de incidentes

Un plan de gestión de incidentes efectivo debe establecer unos procedimientos claros para gestionar los incidentes de ciberseguridad y proporcionar las pautas necesarias a todas las partes implicadas. A fin de garantizar un enfoque integral a la respuesta a incidentes, debe incorporar los siguientes elementos en su plan de gestión de incidentes:

- **Definición de las partes interesadas:** identifique a las partes interesadas más importantes y asigne roles en el proceso de gestión de incidentes, como responsables de incidentes, equipo de TI complementario, organización y liderazgo, y partes externas como proveedores de servicios de TI, fuerzas del orden y proveedores de respuesta a incidentes.
- **Clasificación de incidentes y niveles de gravedad:** establezca criterios para clasificar los incidentes en función de factores como el posible impacto, los sistemas afectados y el tipo de amenaza. Defina los niveles de gravedad para priorizar y dirigir las acciones de respuesta a incidentes.
- **Procedimientos de traslado de incidencias:** desarrolle unos procedimientos de derivación claros para los incidentes que excedan las capacidades o la autoridad de los encargados de la respuesta inicial, como implicar a altos directivos o expertos externos según sea necesario.
- **Comunicaciones:** garantice una comunicación efectiva durante una crisis usando plantillas predefinidas de respuesta a incidentes para el personal, los clientes y los Partners. Plantéese la incorporación de prácticas de planes de recuperación de desastres y de continuidad empresarial para evaluar canales de comunicación de respaldo para el correo electrónico, la mensajería y las videoconferencias.
- **Inventario de recursos:** mantenga un inventario de recursos actualizado para hacer un seguimiento de todo el hardware y el software de la organización y gestionarlo. Esta información es crucial para determinar la propagación, el impacto y la respuesta a una amenaza.
- **Cronología de respuesta a incidentes:** cree una cronología para cada fase del proceso de respuesta a incidentes detallando los plazos para las distintas fases, a fin de garantizar una respuesta puntual y organizada.
- **Documentación y notificación de incidentes:** estandarice el proceso para documentar todos los aspectos de un incidente, incluidas las acciones realizadas, las decisiones tomadas y los resultados conseguidos. Esta documentación será crucial para el análisis posterior al incidente y las posibles investigaciones legales y normativas.
- **Evaluaciones tras la intervención y mejora continuada:** implemente un proceso para realizar evaluaciones posteriores a las acciones después de un incidente para determinar la efectividad de la respuesta e identificar áreas de mejora. Utilice esta información para actualizar y mejorar el plan de gestión de incidentes según sea necesario.

Al incorporar estos elementos a su plan de gestión de incidentes, su organización estará mejor preparada para gestionar y responder a los incidentes de ciberseguridad de manera efectiva y eficiente.

Documentación legal

Durante la fase de preparación, las empresas deben asumir sus responsabilidades legales relativas a la divulgación, la normativa para la gestión de incidentes y otros aspectos relevantes de la ciberseguridad. En las siguientes secciones se detallan algunas cuestiones legales comunes, pero cada organización debe llevar a cabo un análisis exhaustivo de los requisitos normativos específicos de su sector y ubicación. Identifique a las personas responsables de la notificación y el cumplimiento legal dentro de la organización e inclúyalos como partes interesadas en el plan de respuesta a incidentes, asignándoles roles bien definidos.

- **Responsabilidades de divulgación normativa y legal:** algunas organizaciones pueden estar sujetas a la obligación o recomendación legal de divulgar los incidentes en función de su sector o estado.
  - Organizaciones de sectores de infraestructuras críticas
  - Agencias gubernamentales
  - Empresas que cotizan en bolsa
- **Privacidad de datos:** respete las leyes de protección de datos que dictan la divulgación responsable a las agencias de comisión de información y a los clientes o particulares afectados cuyos derechos sobre los datos puedan haberse visto comprometidos.
- **Conservación y destrucción de datos:** establezca políticas y procedimientos para conservar, almacenar y destruir de forma segura los datos recopilados durante las actividades de respuesta a incidentes de acuerdo con las leyes y regulaciones aplicables.
- **Acuerdos y contratos con terceros:** revise los contratos y acuerdos con proveedores y Partners para entender sus obligaciones en materia de respuesta a incidentes y los requisitos de notificación en el caso de que se produzca una filtración o incidente.
- **Protección de la propiedad intelectual (PI):** atienda a los aspectos legales de la protección de la propiedad intelectual de su organización, como secretos comerciales, patentes, derechos de autor y marcas comerciales, durante y después de un ciberincidente.
- **Transferencia y notificación de datos transfronterizas:** si su organización opera internacionalmente, considere las implicaciones y los requisitos legales de transferir y notificar datos entre distintas jurisdicciones.
- **Derechos y responsabilidades de los empleados:** defina los derechos y las responsabilidades legales de los empleados en el contexto de los incidentes de ciberseguridad, incluidas sus obligaciones de notificar incidentes y proteger información confidencial.
- **Documentación de pólizas de seguros:** conozca el proceso y los requisitos para realizar una reclamación a su ciberseguro.
  - Revise los términos y las condiciones de la póliza para determinar lo que incluye y excluye.
  - Consulte con los tomadores internos para asegurarse de que entiende perfectamente qué cubre el seguro.

Manuales de estrategias de respuesta a incidentes

Los manuales de estrategias de respuesta a incidentes ofrecen pautas detalladas paso a paso con las medidas que deben tomarse cuando se identifican amenazas concretas. Estos manuales deben desarrollarse en función de una estrategia basada en riesgos, teniendo en cuenta la probabilidad y el posible impacto de distintos escenarios de ataque. Debe considerar los siguientes elementos al desarrollar sus manuales de estrategias de respuesta a incidentes:

- **Adecuación a su organización:** asegúrese de que sus manuales de estrategias se adapten al entorno, los recursos y las capacidades únicos de su organización. Para ello debe tener en cuenta el tamaño, el sector y los riesgos concretos a los que se enfrenta su organización.
- **Amenazas y escenarios específicos:** en organizaciones más maduras, se recomienda desarrollar manuales de estrategias para amenazas específicas, como ciertos tipos de malware o ataques dirigidos. Sin embargo, en el caso de las organizaciones con recursos limitados, los manuales de estrategias han de ser más integrales y cubrir distintas amenazas para que puedan servir en diversos escenarios.
- **Instrucciones claras y concisas:** los manuales de estrategias deben proporcionar instrucciones claras y concisas para cada paso del proceso de respuesta. Así los encargados de la respuesta podrán entender y ejecutar rápidamente las acciones necesarias durante un incidente.

- **Roles y responsabilidades:** defina claramente los roles y las responsabilidades de cada miembro del equipo implicado en el proceso de respuesta. Esto garantizará que todos sepan qué se espera de ellos y que puedan colaborar de forma efectiva.
- **Comunicación y derivación:** incluya directrices para la comunicación y la derivación durante un incidente, por ejemplo, cuándo notificar a los directivos o recurrir al apoyo externo.
- **Integración con un plan de gestión de incidentes:** asegúrese de que sus manuales de estrategias estén alineados con su plan de gestión de incidentes y que lo apoyen. Esto ayuda a mantener la coherencia entre todas las acciones de respuesta a incidentes.
- Revisiones y actualizaciones regulares: los manuales de estrategias deben revisarse y actualizarse con regularidad para mantener su relevancia y efectividad frente a las amenazas en evolución y las cambiantes circunstancias organizativas.

Al incorporar estos elementos a sus manuales de estrategias de respuesta a incidentes, su organización estará mejor preparada para responder con eficacia a distintos incidentes de ciberseguridad y minimizar los posibles impactos.

Copias de seguridad

Las copias de seguridad son esenciales para garantizar la continuidad empresarial y minimizar el impacto de la pérdida de datos a causa de accidentes, fallos del sistema o ciberataques. Para implementar una estrategia de copias de seguridad robusta, es necesario crear y validar copias de seguridad regularmente, además de elegir distintas opciones de almacenamiento para maximizar la disponibilidad de los datos. Debe considerar los siguientes elementos al desarrollar su estrategia de copias de seguridad:

- **Frecuencia de las copias de seguridad:** determine la frecuencia adecuada para crear copias de seguridad en función de la criticidad de los datos y el nivel de riesgo aceptable. Las copias de seguridad periódicas ayudan a minimizar el posible impacto de la pérdida de datos.
- **Tipos de copias de seguridad:** utilice una combinación de copias de seguridad completas, incrementales y diferenciales para optimizar el espacio de almacenamiento y permitir una recuperación de datos eficiente.
- **Opciones de almacenamiento:** elija distintas opciones de almacenamiento, incluidas copias de seguridad locales, basadas en la nube y sin conexión. Esto ayuda a garantizar la disponibilidad de los datos y mitiga el riesgo de pérdida de datos debido a un punto único de error.
- **Priorización de los datos críticos para el negocio:** céntrese en realizar copias de seguridad de los datos y sistemas críticos para el negocio que sean esenciales para mantener las operaciones y los procesos empresariales clave.
- **Cifrado de copias de seguridad:** cifre las copias de seguridad para proteger los datos confidenciales y evitar accesos no autorizados durante el almacenamiento y la transmisión.
- **Validación de copias de seguridad:** valide las copias de seguridad con regularidad para asegurarse de que sean fiables y puedan restaurarse sin problemas cuando haga falta. Para ello puede ser necesario poner a prueba el proceso de restauración y verificar la integridad de los datos de las copias de seguridad.
- **Políticas de retención:** implemente políticas de retención de datos para gestionar el almacenamiento y la eliminación de las copias de seguridad de acuerdo con los requisitos legales, normativos y empresariales.
- **Planificación de recuperación de desastres:** integre su estrategia de copias de seguridad en el plan general de recuperación de desastres de su organización para permitir una respuesta coordinada y efectiva en caso de pérdida de datos.

Al incorporar estos elementos a su estrategia de copias de seguridad, su organización estará mejor preparada para recuperarse.

Endurecimiento del sistema y la red

El endurecimiento del sistema y la red implica reducir la superficie de ataque minimizando las funcionalidades, el acceso a los sistemas y las conexiones de red que no sean estrictamente necesarias. Al implementar unas prácticas de endurecimiento efectivas, su organización podrá reducir la probabilidad de sufrir un ataque. Considere los siguientes aspectos al desarrollar su estrategia de endurecimiento del sistema y la red:

Aplicación de parches

- **Programa de gestión de parches:** establezca un programa para garantizar que se aplican los parches necesarios a su red de manera puntual y sistemática a través de herramientas de aplicación de parches automatizadas y semiautomatizadas.
- **Documentación:** mantenga registros de los parches aplicados y de cualquier exclusión necesaria.
- **Priorización:** priorice los parches en función de un análisis de riesgos, centrándose en remediar las vulnerabilidades que puedan tener un mayor impacto en su organización.

Configuración

- **Auditoría de cumplimiento de seguridad:** realice auditorías internas y externas continuas para verificar la correcta configuración de las herramientas de seguridad e identificar posibles errores de configuración o exclusiones.
- **Control de aplicaciones:** implemente listas de aplicaciones permitidas y bloqueadas para limitar el número de versiones de aplicaciones que pueden ejecutarse en los hosts, a fin de reducir el riesgo de que se explote software no autorizado o vulnerable.
- **Control de acceso a la red:** configure herramientas de red para restringir el acceso a IP y puertos solo a los hosts internos y externos necesarios, y minimizar así posibles accesos no autorizados y exfiltraciones de datos.
- **Principio del mínimo privilegio:** asegúrese de que los usuarios de su organización tengan limitados sus derechos de acceso al nivel mínimo necesario para realizar las funciones de su cargo a fin de reducir la posibilidad de accesos no autorizados y de que los datos se vean comprometidos.

Seguridad de la red

- **Segmentación de la red:** divida su red en segmentos más pequeños y aislados para limitar el posible impacto de una infracción de seguridad y ponérselo más difícil a los atacantes para moverse lateralmente dentro de su red.
- **Configuración de los firewalls:** configure los firewalls para que bloqueen todo el tráfico entrante y saliente innecesario, y revise y actualice regularmente las reglas para mantener una postura de seguridad óptima.
- **Sistemas de detección y prevención de intrusiones (IDPS):** despliegue IDPS para supervisar el tráfico de red en busca de indicios de actividad maliciosa y tomar las medidas necesarias.

Supervisión y telemetría

La supervisión y la telemetría son componentes cruciales de una estrategia de respuesta a incidentes efectiva, ya que ofrecen información valiosa sobre el entorno de la organización y permiten detectar con prontitud las posibles amenazas. Al entender su entorno e implementar las capas de detección y defensa adecuadas, mejorará la capacidad de respuesta de su organización frente a los incidentes.

Su entorno

Entender su entorno es la base de una supervisión y telemetría efectivas. Esto incluye:

- Inventario de recursos: mantenga un registro actualizado de los endpoints, los servidores y su cobertura con las plataformas de seguridad que correspondan.
- Topología de la red: desarrolle una visión clara de su red, incluidos los puntos de entrada/salida, la segmentación y los puntos de control, preferiblemente por medio de un diagrama actualizado.

Capas de detección y defensa

Establecer múltiples capas de detección y defensa es esencial para una estrategia de seguridad integral. Considere las siguientes fuentes de telemetría y procure sincronizar las marcas de tiempo de todas ellas, siendo UTC la zona horaria estándar recomendada:

- **Dispositivos perimetrales:** firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusiones (IDS), VPN y proxies.
- **Protección de endpoints:** antivirus (AV), antivirus next-gen (NGAV), detección y respuesta para endpoints/ampliadas (E/XDR).
- **Registros centralizados:** herramientas de información de seguridad y gestión de eventos (SIEM), servidores de Syslog y almacenamiento de datos en la nube.
- **Autenticación:** servicios de autenticación multifactor y servicios de gestión de identidad y acceso (IAM).
- **Información sobre amenazas:** información táctica para la correlación y el seguimiento de marca para alertar de exposiciones externas.

Herramientas y técnicas de supervisión

Implementar las herramientas y técnicas de supervisión correctas es vital para una identificación y respuesta a incidentes efectivas. Considere las siguientes estrategias:

- **Supervisión continua:** despliegue una combinación de supervisión en tiempo real y periódica para mantener una visión completa de su entorno.
- **Detección de anomalías:** sírvase de análisis avanzados y algoritmos de Machine Learning para identificar patrones y comportamientos inusuales que puedan indicar una posible amenaza.
- **Correlación de registros:** agregue y correlacione datos de registro de múltiples fuentes para identificar patrones y tendencias que puedan indicar un ataque.
- **Priorización de alertas:** desarrolle un proceso para priorizar las alertas según factores como la criticidad, el impacto potencial y el nivel de amenaza.

Al centrarse en su entorno, establecer unas capas de detección y defensa robustas y desplegar herramientas y técnicas de supervisión efectivas, podrá mejorar significativamente la capacidad de su organización para identificar y responder a los incidentes de seguridad con prontitud y eficiencia.

Comunicación

Una comunicación efectiva es crucial durante la respuesta a incidentes, ya que permite que las partes interesadas puedan coordinarse y colaborar sin demora. En esta sección se detallan las cuestiones más importantes para la comunicación tanto interna como externa en el contexto de la respuesta a incidentes, teniendo en cuenta los requisitos legales.

Comunicación interna

- **Plan de comunicación:** establezca un plan de comunicación integral que detalle las vías de derivación, los canales de comunicación y los puntos de contacto clave. Este plan debe revisarse y actualizarse periódicamente para garantizar su eficacia durante un incidente.
- **Equipo de respuesta a incidentes:** reúna un equipo de respuesta a incidentes (IRT) y designe un responsable para que se encargue de la coordinación de las acciones de respuesta. Asegúrese de que los miembros del equipo entiendan sus roles y responsabilidades, y que mantengan abiertas las líneas de comunicación durante todo el incidente.
- **Canales seguros:** utilice canales de comunicación seguros y fiables para impedir el acceso no autorizado a información confidencial. Plantéese implementar aplicaciones de mensajería cifrada, correo electrónico seguro o plataformas de comunicación dedicadas.
- **Plantillas de respuesta:** cree una biblioteca de plantillas predefinidas de respuesta a incidentes para varios escenarios a fin de permitir una comunicación más rápida y homogénea. Estas plantillas deben ser fácilmente accesibles y personalizables y estar alineadas con las pautas de comunicación de la organización.
- **Puesta al día de las partes interesadas:** comuníquese periódicamente con las partes interesadas durante todo el proceso de gestión del incidente para informarles de la situación, las medidas tomadas y los resultados esperados. Esta transparencia puede ayudar a mantener la confianza en la gestión del incidente por parte de la organización.

Comunicación externa

- **Estrategia de notificación:** desarrolle una estrategia de notificación a clientes, proveedores, Partners y fuerzas del orden en caso de que se produzca una infracción de seguridad u otros incidentes que puedan afectarles. Esta estrategia debe especificar los criterios para la notificación, los canales adecuados y las personas responsables de gestionar las comunicaciones.
- **Cumplimiento legal y normativo:** asegúrese de que las comunicaciones externas cumplan los requisitos legales y normativos, como las leyes de protección de datos, las directrices de divulgación responsable y las regulaciones específicas del sector. Obtenga asesoramiento jurídico para confirmar que las comunicaciones respetan todas las obligaciones que correspondan.
- **Portavoz designado:** designe a un portavoz o equipo de relaciones públicas que se encargue de las consultas de los medios y las declaraciones públicas a fin de transmitir un mensaje coherente y preciso. Esta persona o equipo debe tener formación en comunicaciones en caso de crisis y relaciones con los medios.
- **Preparaciones para comunicaciones externas:** prepare plantillas de comunicaciones para diversos escenarios de incidentes a fin de permitir

una notificación rápida y clara a las partes externas. Adapte estas plantillas de modo que cubran las necesidades específicas de las distintas partes interesadas, como clientes, Partners y entidades reguladoras.

- **Colaboración con otros departamentos:** trabaje en estrecha colaboración con el departamento jurídico, de relaciones públicas y otros departamentos relevantes para asegurarse de que las comunicaciones externas cumplen las regulaciones, protegen la reputación de la organización y mantienen la transparencia con las partes afectadas.

Al implementar estas estrategias de comunicación, su organización podrá garantizar una respuesta coordinada y efectiva a los incidentes de ciberseguridad, lo que en última instancia preservará la confianza en la gestión de dichos eventos por parte de su organización.

Concienciación y formación sobre seguridad

Sensibilizar a los empleados sobre las amenazas de ciberseguridad y las prácticas recomendadas es crucial para la postura de seguridad general de una organización. En esta sección, hablaremos de los componentes clave de un programa integral de concienciación y formación sobre seguridad, como las iniciativas de concienciación sobre seguridad, el contenido y la frecuencia de la formación, y los ejercicios e incidentes simulados.

Programas de concienciación sobre seguridad

- **Objetivos del programa:** establezca objetivos claros para su programa de concienciación sobre seguridad, centrándose en el conocimiento y los comportamientos que deben adoptar los empleados para proteger los recursos y la información de la organización.
- **Formación específica:** desarrolle materiales de formación adaptados para distintos roles y departamentos dentro de la organización teniendo en cuenta sus responsabilidades únicas y el acceso a la información confidencial.
- **Actualizaciones continuas:** actualice regularmente el programa de concienciación sobre seguridad de modo que refleje el cambiante panorama de las amenazas e incorpore las últimas tendencias y prácticas recomendadas.
- **Métricas y evaluación:** supervise y mida la efectividad del programa de concienciación sobre seguridad usando indicadores clave de rendimiento (KPI) como la participación de los empleados, los índices de finalización de la formación y la mejora de los comportamientos en materia de seguridad.

Contenido y frecuencia de la formación

- **Desarrollo de contenido:** cree contenido de formación ameno e informativo que cubra una amplia variedad de temas, como la gestión de las contraseñas, la concienciación sobre el phishing, la ingeniería social y la navegación segura por Internet.
- **Impartición de la formación:** ofrezca varios formatos de formación, incluidos cursos online, talleres presenciales y webinars interactivos, para cubrir distintas preferencias y horarios de aprendizaje.
- **Frecuencia:** programe sesiones de formación regulares a lo largo del año, con una frecuencia mínima recomendada de una por trimestre. Ofrezca también sesiones de formación puntuales en respuesta a incidentes concretos o amenazas emergentes.
- **Formación continua:** promueva una cultura de aprendizaje continuo dando acceso a los empleados a recursos adicionales, como artículos, vídeos y podcasts que les ayuden a ampliar sus conocimientos sobre ciberseguridad.

Ejercicios e incidentes simulados

- **Escenarios realistas:** diseñe ejercicios e incidentes simulados basados en escenarios realistas con los que puedan encontrarse los empleados en su trabajo diario. Estos escenarios pueden ayudar a los empleados a entender mejor el posible impacto de una infracción de seguridad y poner en práctica sus habilidades de respuesta.
- **Colaboración interdepartamental:** involucre a diversos departamentos en ejercicios simulados y fomente la colaboración y la comunicación entre equipos de distintas áreas de competencia.
- **Evaluación y comentarios:** realice una evaluación exhaustiva del rendimiento de los empleados durante los ejercicios e incidentes simulados, y ofrezca comentarios constructivos e identifique áreas de mejora.
- **Lecciones aprendidas:** comparta las lecciones aprendidas de los ejercicios simulados con toda la organización para consolidar conceptos clave y prácticas recomendadas.

Al implementar un programa robusto de concienciación y formación sobre seguridad, las organizaciones pueden conferir a sus empleados los conocimientos y las habilidades necesarios para identificar y responder a amenazas de ciberseguridad y, en última instancia, reducir el riesgo de ataques consumados.

Equipo de respuesta a incidentes

Un equipo de respuesta a incidentes eficiente es fundamental para dar una respuesta puntual y coordinada a los incidentes de ciberseguridad. En esta sección, hablaremos de los roles y las responsabilidades, la composición del equipo, y la importancia del soporte y los conocimientos externos en la respuesta a incidentes.

Roles y responsabilidades

- **Gestor de respuesta a incidentes:** supervisa el proceso de respuesta a incidentes, coordina las actividades del equipo y vela por una comunicación efectiva entre los miembros del equipo y con las partes interesadas externas.
- **Analistas de seguridad:** investigan y analizan incidentes de seguridad y aportan conocimientos técnicos especializados para identificar la causa raíz, el alcance y el impacto del incidente.
- **Analistas forenses:** realizan tareas forenses digitales, incluidos la recopilación, el análisis y la conservación de pruebas, para dar apoyo a las investigaciones y los procedimientos judiciales.
- **Operaciones de TI:** ayudan en las labores de contención, erradicación y recuperación mediante la gestión de la infraestructura del sistema y la implementación de los cambios necesarios para impedir futuros incidentes.
- **Cumplimiento legal y normativo:** proporciona asesoramiento en cuanto a los requisitos legales y normativos relacionados con la respuesta a incidentes y garantiza una divulgación y notificación correctas.
- **Relaciones públicas y comunicaciones:** gestionan las comunicaciones internas y externas y preparan mensajes adecuados para las partes afectadas, como empleados, clientes, Partners y reguladores.

Composición del equipo de respuesta a incidentes

- **Representación interdepartamental:** reúna un equipo diverso con representación de distintos departamentos, como TI, seguridad, legal, RR. HH. y comunicaciones, de acuerdo con el carácter multidisciplinar de la respuesta a incidentes.
- **Habilidades y conocimientos:** asegúrese de que los miembros del equipo cuentan con las habilidades y los conocimientos necesarios para desempeñar sus funciones designadas ofreciéndoles oportunidades de desarrollo y formación continuas.
- **Disponibilidad y rotación:** establezca un equipo que esté disponible 24/7 usando rotaciones de guardia o turnos específicos para mantener una cobertura continuada.

Apoyo y especialistas externos

- **Proveedores externos:** contrate a expertos externos, como consultores de ciberseguridad o proveedores de servicios de seguridad administrada (MSSP), para complementar sus capacidades internas y aportar conocimientos especializados en áreas como los servicios forenses digitales o la información sobre amenazas.
- **Asesoría jurídica:** recurra a una asesoría legal externa con experiencia en ciberseguridad y leyes de privacidad de datos para recibir orientación en cuanto a los requisitos de divulgación y cumplimiento normativo, y para que represente a la organización en cualquier procedimiento jurídico relacionado con un incidente de seguridad.
- **Fuerzas del orden y agencias reguladoras:** establezca relaciones con las fuerzas del orden y las agencias reguladoras correspondientes y facilite la cooperación y el intercambio de información durante las investigaciones de incidentes.
- **Colaboración con el sector:** participe en foros de ciberseguridad y grupos de intercambio de información específicos del sector para compartir información sobre amenazas y prácticas recomendadas con otras organizaciones a fin de mantenerse al tanto de las tendencias y amenazas emergentes.

Al formar un equipo de respuesta a incidentes equilibrado y servirse de apoyo y especialistas externos, las organizaciones pueden gestionar mejor los incidentes de ciberseguridad y minimizar su posible impacto.

Identificación

La fase de identificación es crucial para detectar la presencia de un atacante dentro de una red o un sistema. La supervisión continua de la telemetría de red es esencial para minimizar el tiempo que transcurre entre la intrusión y la identificación. Cuanto más rápido responda el equipo, menor será el impacto en la confidencialidad, integridad y disponibilidad de los datos, sistemas y redes. Las soluciones de detección y respuesta gestionadas (MDR) pueden ser de gran ayuda en este proceso al ofrecer capacidades especializadas de detección y respuesta a amenazas.

Componentes clave de la identificación

- **Telemetría de dispositivos y red:** una supervisión exhaustiva de las distintas fuentes potenciales, como se menciona en la sección sobre telemetría, es fundamental para la detección y respuesta a amenazas en tiempo real. Implementar una solución MDR puede mejorar este proceso.
- **Notificaciones externas:** la colaboración con las fuerzas del orden y otras fuentes externas para recopilar y analizar información sobre amenazas permite una identificación más rápida de las posibles intrusiones.
- **Información sobre amenazas:** supervisar sitios clandestinos y de la Web Oscura para identificar posibles datos de empresa robados para su venta refuerza aún más las capacidades de detección.
- **Notificación por parte de los usuarios:** anime a los usuarios a denunciar correos electrónicos o enlaces sospechosos y a responder rápidamente a estas posibles amenazas para garantizar que los gestores de incidentes reciban inmediatamente los datos contextuales importantes.

Deben establecerse procesos rigurosos para categorizar el nivel de gravedad de un incidente en función de los siguientes criterios:

- **Fiabilidad:** hace referencia a la fiabilidad de la fuente (p. ej., IPS, FW, AV, XDR).
- **Criticidad:** tiene en cuenta la importancia del sistema afectado.
- **Malignidad:** evalúa el comportamiento sospechoso, lo que puede ofrecer pistas para descubrir una vulneración que de otra forma pasaría desapercibida.
- **Tipo de incidente:** utilice marcos como Cyber Kill Chain y MITRE ATT&CK para clasificar incidentes.
- **Marca de tiempo:** garantice la sincronización de las marcas de tiempo usando UTC, NTP y otros estándares comunes para normalizar los datos.

Tipos de incidentes

NIST define dos categorías de incidentes:

- **Precursor:** detecte señales de reconocimiento, como actividad de escaneado que busca identificar puertos abiertos y vulnerabilidades de software. Las soluciones MDR pueden ser especialmente útiles en este contexto. Identifique exploits conocidos de vulnerabilidades de ejecución de código remoto presentes en la infraestructura de la organización.
- **Indicador:** identifique varios incidentes de tipo indicador, como alertas de malware, cambios en archivos o Active Directory o comportamientos extraños de los usuarios como inicios de sesión vía RDP en momentos inusitados, e inicie una respuesta a incidentes adecuada. La MDR puede ofrecer soporte adicional a la hora de detectar y responder a este tipo de incidentes.

Al implementar una estrategia de supervisión integral, utilizar notificaciones externas e información sobre amenazas, fomentar la notificación por parte de los usuarios y utilizar criterios bien definidos para la categorización de incidentes, las organizaciones pueden mejorar su postura de seguridad general. Asimismo, incorporar soluciones MDR puede ofrecer soporte adicional para detectar y responder a los incidentes de manera efectiva. Una fase de identificación robusta no solo reduce el impacto de los incidentes de seguridad, sino que también promueve una cultura de la seguridad proactiva dentro de la organización, lo que en última instancia favorece la continuidad empresarial y protege los recursos valiosos.

Archivos, directorios, procesos y persistencia potencialmente sospechosos

Entender e identificar archivos, directorios, procesos y mecanismos de persistencia potencialmente sospechosos puede ayudar a detectar incidentes con prontitud.

- **Archivos y directorios:** los archivos y directorios inusuales o inesperados podrían indicar un incidente de seguridad. Ejemplos:
  - Archivos con extensiones o nombres inusuales
  - Archivos en ubicaciones inesperadas

- Directorios que contienen datos confidenciales que no deberían ser accesibles

- **Procesos:** los procesos sospechosos podrían ser un indicio de actividad maliciosa en un sistema. Ejemplos:
  - Procesos con un uso de CPU o memoria elevado
  - Procesos que se ejecutan desde ubicaciones inesperadas
  - Procesos que intentan acceder a datos o recursos confidenciales
- **Persistencia:** los atacantes suelen establecer mecanismos de persistencia para mantener el acceso a un sistema comprometido. Estos son algunos ejemplos de persistencia:
  - Tareas programadas o trabajos cron que ejecutan scripts maliciosos
  - Malware que se reinstala a sí mismo al eliminarlo o al reiniciar
  - Claves del registro o elementos de inicio que lanzan procesos maliciosos
- **Acceso a credenciales:** el acceso no autorizado a credenciales puede llevar a la vulneración de más sistemas y datos confidenciales. Ejemplos:
  - Ataques por fuerza bruta a cuentas de usuarios
  - Campañas de phishing para robar credenciales de empleados
  - Volcado de credenciales de sistemas comprometidos
- **Otros puntos de afianzamiento/acceso:** los atacantes pueden intentar afianzarse en más puntos dentro del entorno de una organización para ampliar su acceso y control. Ejemplos:
  - Cuentas de usuario comprometidas con privilegios elevados
  - Explotación de vulnerabilidades sin parchear en sistemas o aplicaciones
  - Propagación lateral dentro de la red para acceder a recursos adicionales

Al reconocer estos tipos de incidentes y sus ejemplos, las organizaciones pueden identificar de forma más efectiva las posibles amenazas y responder en consecuencia. Conocer los distintos tipos de incidentes es fundamental para que una organización pueda detectar y mitigar los incidentes de seguridad sin demora.

Análisis forense

El análisis forense es un aspecto crucial del proceso de respuesta a incidentes, ya que ayuda a las organizaciones a identificar la causa raíz de un incidente, entender su impacto y recopilar pruebas para ayudar en subsiguientes investigaciones o acciones judiciales. A continuación se describen algunos de los elementos clave del análisis forense.

Herramientas y técnicas forenses

Existen varias herramientas y técnicas forenses que ayudan a analizar los sistemas y las redes durante la respuesta a un incidente. Estas herramientas pueden ayudar en la recopilación, el análisis y la conservación de los datos. Estos son algunos ejemplos de herramientas y técnicas forenses:

- Herramientas de creación de imágenes y clonación de discos para preservar el estado de un sistema comprometido
- Herramientas de análisis de memoria para investigar datos volátiles e identificar procesos maliciosos
- Herramientas de análisis del tráfico de red para examinar la actividad de la red e identificar posibles indicadores de peligro
- Herramientas de análisis de registros para revisar los registros del sistema y de las aplicaciones en busca de actividad sospechosa

Recopilación y conservación de pruebas

La correcta recopilación y conservación de pruebas es fundamental en el análisis forense para garantizar la integridad de los datos y mantener su admisibilidad en procedimientos judiciales. Entre las prácticas recomendadas para recopilar y conservar pruebas se incluyen:

- Documentar cada paso del proceso de recopilación de pruebas, incluidas las herramientas y técnicas utilizadas.
- Crear una cronología detallada de los eventos relacionados con el incidente.
- Utilizar bloqueadores de escritura y otras herramientas forenses para impedir que se alteren las pruebas durante la recopilación.

- Proteger los datos recopilados en contenedores a prueba de manipulaciones o soportes de almacenamiento cifrado.
- Asegurarse de almacenar cualquier dato recopilado en un entorno seguro y controlado.

Cadena de custodia

Mantener una cadena de custodia correcta es esencial para garantizar la integridad de las pruebas y su admisibilidad en procedimientos judiciales. La cadena de custodia hace referencia a la documentación y al seguimiento del manejo, el almacenamiento y la transferencia de las pruebas durante toda la investigación. Para mantener una cadena de custodia adecuada, las organizaciones deben:

- Registrar los datos de cada persona que maneja las pruebas, incluidos su nombre, rol e información de contacto.
- Documentar la fecha, hora y ubicación de cada transferencia o manipulación de las pruebas.
- Mantener un registro de cualquier acción realizada con las pruebas, como copiarlas, analizarlas o almacenarlas.
- Asegurarse de que las pruebas se almacenan y transportan siempre de manera segura, utilizando precintos de seguridad o almacenaje cifrado según sea necesario.

Al incorporar el análisis forense en el proceso de respuesta a incidentes, las organizaciones pueden obtener información muy valiosa sobre la naturaleza y el alcance de los incidentes de seguridad, recopilar pruebas cruciales y ayudar en futuras investigaciones o acciones judiciales. Entender e implementar herramientas, técnicas y prácticas forenses adecuadas es fundamental para llevar a cabo un análisis riguroso y efectivo.

Exfiltración de datos

La exfiltración de datos hace referencia a la transferencia no autorizada de información o datos confidenciales de los sistemas o la red de una organización a una ubicación externa, normalmente controlada por un atacante. Detectar e impedir la exfiltración de datos es esencial para minimizar el impacto de una infracción de seguridad y proteger recursos valiosos. Para hacer frente a la exfiltración de datos de manera efectiva, las organizaciones deben considerar los siguientes aspectos:

- **Supervisión y alertas:** implemente un sistema de supervisión integral para detectar transferencias de datos o patrones de tráfico de red inusuales, como transferencias de archivos grandes, comunicaciones con direcciones IP sospechosas o múltiples intentos de inicio de sesión fallidos. Asegúrese de contar con mecanismos de alerta adecuados para notificar al personal que corresponda los posibles incidentes de exfiltración de datos.
- **Soluciones de prevención de pérdida de datos (DLP):** despliegue soluciones DLP para identificar e impedir que se transfieran datos confidenciales fuera de la red de la organización. Las soluciones DLP pueden ayudar a detectar y bloquear la transferencia no autorizada de información confidencial en función de políticas y reglas predefinidas.
- **Cifrado:** cifre los datos confidenciales tanto en reposo como en tránsito para reducir el valor de los datos para un atacante en el caso de que consiga exfiltrarlos.
- **Formación y concienciación de empleados:** forme a los empleados acerca de los riesgos de la exfiltración de datos y la importancia de cumplir las políticas de seguridad, como no compartir información confidencial a través de canales no seguros o con personas no autorizadas.

Validación y priorización

Una vez identificado un posible incidente de seguridad, es imperativo validarlo y priorizar la respuesta según la gravedad y el impacto potencial en la organización. La validación y priorización implican estos pasos:

- **Validación del incidente:** verifique que el incidente identificado es un evento de seguridad real y no un falso positivo. Esto se consigue analizando los datos disponibles, correlacionándolos con información sobre amenazas conocidas y revisando el contexto del evento.
- **Priorización del incidente:** evalúe el posible impacto del incidente en los recursos, las operaciones y la reputación de la organización. Considere factores como el tipo de datos o sistemas implicados, el alcance de la vulneración y las posibles consecuencias del incidente.

- **Niveles de gravedad:** asigne un nivel de gravedad al incidente en función de la evaluación de prioridades. Los niveles de gravedad pueden establecerse usando una escala predefinida, como bajo, medio, alto o crítico, y deben guiar al equipo de respuesta a incidentes a la hora de determinar los recursos adecuados y la urgencia de la respuesta.
- **Plan de respuesta:** según el nivel de gravedad y la naturaleza del incidente, seleccione el plan de respuesta más apropiado del manual de estrategias de respuesta a incidentes de la organización. Este plan debe explicar los pasos necesarios para contener, investigar y remediar el incidente, además de cualquier procedimiento de comunicación y notificación requerido.

Al identificar, validar y priorizar los incidentes de seguridad de manera efectiva, las organizaciones pueden asegurarse de que sus recursos se asignan eficientemente y las labores de respuesta se centran en los incidentes más críticos, lo que minimiza el impacto en la organización.

Contención

El principal objetivo de la contención es mitigar daños adicionales aislando los sistemas que se han identificado como comprometidos o que se sospecha que lo están. Este paso ayuda a evitar la propagación de los incidentes, como la proliferación del malware o la exfiltración continua de datos, y permite preservar el sistema en un estado del que se puedan recopilar pruebas adicionales. Unas estrategias de contención adecuadas pueden resultar útiles para la investigación, como la recopilación de indicadores de peligro (IOC) que se documentarán y utilizarán en otros análisis.

Contención a corto plazo

La contención a corto plazo implica la toma de medidas inmediatas para limitar el impacto del incidente. Estas se suelen aplicar al identificarse el equipo comprometido y tienen como principal objetivo contener la amenaza inmediata. Algunos ejemplos de medidas de contención a corto plazo son:

- **Aislamiento basado en el host:** utilice las funciones de las plataformas de seguridad para aislar los hosts comprometidos, como Sophos Intercept X Advanced, al tiempo que mantiene una conexión activa para seguir investigando.
- **Bloqueo de hashes SHA256:** utilice Sophos Intercept X Advanced para bloquear archivos maliciosos por sus hashes SHA256 e impedir que se ejecuten.
- **Red aislada:** cambie las políticas de enrutamiento del switch, el enrutador o el firewall para prohibir al segmento de red que contiene el equipo identificado que se comunique con otros equipos y propague la amenaza.
- **Aislamiento manual:** desconecte el cable Ethernet de la red o desactive la tarjeta de red (Wi-Fi) del equipo para responder a una vulneración confirmada.
- **Restablecimiento de cuentas:** restablezca cualquier cuenta de usuario que se sepa o se sospeche que se ha visto comprometida.

Contención a largo plazo

La contención a largo plazo se centra en evitar la propagación del mismo incidente a otros equipos y recursos de la red tras finalizar las investigaciones iniciales. Algunos ejemplos de medidas de contención a largo plazo son:

- Bloquear conexiones de red a URL maliciosas y servidores de comando y control (C2) identificados en la investigación.
- Suspender cuentas de dominio comprometidas, restablecer/suspender contraseñas de cuentas de administrador local o de dominio, y restablecer las contraseñas en todo el dominio si no se puede determinar la magnitud del incidente.
- Implementar el aislamiento automático de dispositivos en función de un estado de seguridad mínimo predefinido.
- Instalar agentes de seguridad en equipos no protegidos o en equipos cuyos datos se han borrado para garantizar la visibilidad y protección.

Prácticas recomendadas

Para garantizar una contención efectiva, tenga en cuenta estas prácticas recomendadas:

Debe

- Aislar el equipo siguiendo una de las opciones anteriores.
- Documentar los pasos realizados, registrando la hora, la acción y quién la ha realizado.
- Tener en cuenta sus planes de respuesta a incidentes y su estrategia de contención, especialmente en caso de litigio. Plantearse tomar imágenes forenses e implicar a su ciberseguro.
- Clasificar la amenaza según su nivel de gravedad y notificar al equipo directivo si se trata de un incidente grave.
- Determinar los IOC para ayudar en la investigación y recopilar pruebas.

- Comunicarse con las partes interesadas, como los equipos directivo, jurídico y de relaciones públicas, según corresponda en función de la gravedad y el posible impacto del incidente.
- Estar atento a cualquier señal de represalia o intensificación por parte del atacante durante el proceso de contención, ya que podría intentar infligir más daños al darse cuenta de que le han descubierto.
- Asegurarse de que las medidas de contención son reversibles en caso necesario, por si se producen falsos positivos o consecuencias imprevistas.
- Realizar un análisis exhaustivo del incidente para identificar las causas raíz y aprender de la experiencia para mejorar su postura de seguridad y su proceso de respuesta a incidentes.

No debe

- Apagar ni reiniciar el equipo comprometido.
- Actuar precipitadamente sin consultar con el gestor de respuesta a incidentes de acuerdo con su plan.
- Restaurar inmediatamente el sistema a partir de una copia de seguridad sin concluir antes la recopilación de IOC y las investigaciones iniciales.
- Hacer público el incidente ni compartir información confidencial con personas no autorizadas, ya que esto podría alertar al atacante y posiblemente frustrar el proceso de contención.
- Utilizar únicamente herramientas y procesos automatizados para la contención; recurra a la experiencia y al juicio de profesionales para tomar decisiones informadas.
- Olvidarse de considerar el posible impacto empresarial de las acciones de contención, como el tiempo de inactividad o la pérdida de funcionalidad, y sopesar estos factores frente a los riesgos de no tomar medidas.
- Descuidar la actualización de su plan y procedimientos de respuesta a incidentes en función de las lecciones aprendidas del proceso de contención para prepararse mejor para futuros incidentes.

Recuerde que una estrategia genérica puede no resultar adecuada y que debe considerarse el tipo de incidente, el panorama de la red y la accesibilidad a la red para decidir qué medidas han de tomarse. La contención detiene la amenaza inminente y permite ganar tiempo para realizar otras acciones, pero normalmente no es el último paso en la gestión de un incidente. Las empresas deben permanecer alerta ante el riesgo continuado que supone un ciberincidente, ya que los atacantes podrían intensificar su ofensiva al darse cuenta de que les han descubierto.

Erradicación

La erradicación es el proceso por el cual se elimina completamente la amenaza o al atacante del entorno. Suele implicar varias etapas y tiene como objetivo identificar, documentar y erradicar todas las actividades, modificaciones en el sistema, malware y ejecuciones en la red y los equipos realizados por el ciberdelincuente. Puesto que la mayoría de los ciberataques de gran repercusión utilizan múltiples métodos de infiltración y se sirven de maniobras manuales, es fundamental identificar cualquier irregularidad que no puedan detectar los escaneados. Al erradicar una amenaza, es crucial tener en cuenta todos los posibles efectos subsiguientes.

Hay dos estrategias principales para la erradicación: la reconstrucción o el restablecimiento de la imagen inicial de los equipos, y la eliminación selectiva. Cada una tiene sus ventajas e inconvenientes y suelen aplicarse de manera conjunta para obtener los mejores resultados.

Reconstrucción o restablecimiento de la imagen inicial de los equipos

La forma más eficiente de erradicar recursos comprometidos es reconstruir o restablecer la imagen inicial de los hosts para garantizar una reversión total a un estado no comprometido. Este proceso es más sencillo si las organizaciones despliegan imágenes de software estándar en los hosts y tienen acceso a la imagen maestra para la recuperación. La imagen maestra debe crearse antes del despliegue en producción para evitar vulneraciones previas.

En el caso de los servidores críticos, como sistemas ERP, servidores de correo y servidores de archivos, no se suele realizar la restauración a partir de una imagen maestra antigua debido a la posible pérdida de datos y costes asociados. En lugar de ello, las organizaciones pueden llevar a cabo la restauración desde un archivo de copia de seguridad limpio (p. ej., servidor de copia de seguridad, unidad de cinta, la nube u otros medios). En este proceso es necesario verificar la disponibilidad y la integridad de los archivos de copia de seguridad y elegir un estado de recuperación que no esté infectado. Para aplicar una estrategia de reconstrucción o restablecimiento de imágenes lo más efectiva posible, las organizaciones deben investigar los IOC y las tácticas, técnicas y procedimientos (TTP) en toda la red, prestando especial atención a los equipos vulnerables.

Eliminación selectiva

La estrategia de eliminación selectiva tiene como objetivo identificar todas las aplicaciones de malware y artefactos, determinar los cambios más importantes que ha realizado el adversario en el sistema y eliminar el malware o revertir los sistemas a su estado previo al ataque. Este enfoque es necesario para aquellos equipos que forman parte de sistemas de producción, sistemas de control industrial u otras funciones empresariales críticas en que la pérdida de datos y el tiempo de inactividad serían perjudiciales.

La eliminación selectiva suele desplegarse usando una combinación de herramientas y especialistas en respuesta a incidentes que buscan amenazas en función de IOC observados inicialmente, información sobre amenazas asociada y su experiencia con las TTP de los adversarios. Las organizaciones pueden utilizar la eliminación selectiva para entender mejor el ataque y sacar conclusiones para implementar mejoras a largo plazo y reducir el riesgo de futuros ciberataques.

Por ejemplo, si un atacante consigue comprometer un host explotando vulnerabilidades existentes, errores de configuración o vulneraciones latentes previas, la erradicación también debe incluir la mitigación de dichos puntos débiles para evitar que el host se convierta en un vector de reinfección o de un nuevo ataque. Un análisis de causa raíz puede ayudar a las organizaciones a entender los pasos que siguió el atacante hasta que se percataron del impacto y a encontrar al paciente cero para evitar futuros ataques.

Es recomendable que las empresas sigan documentando sus conclusiones y utilicen marcos, como la plataforma MITRE ATT&CK, para conceptualizar la estructura de un ataque. Esta estrategia estructurada ayuda a identificar la causa raíz de un incidente y permite a las organizaciones mejorar su postura de seguridad general.

Recuperación

El objetivo de la fase de recuperación es devolver de forma gradual los equipos y sistemas afectados a las operaciones empresariales normales y restaurar la plena funcionalidad de la organización a su estado previo a la infiltración. La estrategia de recuperación depende del incidente, ya que algunos pueden conllevar el aislamiento de unos pocos equipos y tener un impacto operativo mínimo, mientras que otros ataques más contundentes como el ransomware podrían afectar a varios equipos y provocar un impacto operativo y un tiempo de inactividad empresarial importantes. Por tanto, los planes de recuperación deben adaptarse a cada ataque.

- Un único host afectado por un correo electrónico de phishing con una carga detectada y eliminada por el agente de protección de endpoints puede requerir el aislamiento del equipo mientras un analista de seguridad lo investiga y limpia, lo que tendría un impacto operativo general mínimo.
- La pronta detección de una red de bots que ha infectado dos estaciones de usuario en los que se han instalado mecanismos de persistencia podría requerir el aislamiento inmediato y la reconstrucción de los ordenadores implicados, lo que conllevaría un periodo de inactividad para los empleados, pero el impacto operativo en el negocio sería mínimo.
- Un ataque de ransomware a nivel de red con un tiempo de permanencia de varias semanas y una causa raíz identificada se traducirá en el aislamiento no solo de los endpoints y servidores, sino también del correo electrónico, las VPN, las cuentas de Active Directory y otros servicios. En este caso, los expertos en respuesta a incidentes deben adoptar medidas de contención hasta que el ataque esté controlado después de identificar los puntos de afianzamiento, aplicar parches y restablecer la imagen inicial de los equipos. Las estrategias pueden incluir la creación de una red "limpia" alternativa, su reconstrucción sin ninguno de los equipos afectados y la reincorporación de los dispositivos uno a uno. La decisión de volver a incorporar equipos aislados debe basarse en un riesgo bajo de reentrada o reinfección, y los responsables de la respuesta a incidentes deben comunicar este riesgo al equipo directivo para poder planificar un calendario y un enfoque adecuados al riesgo y a la empresa.

Precaución ante todo

La tarea de recuperar equipos requiere concentración y atención a los detalles críticos del sistema, ya que un exceso de confianza en la erradicación de la amenaza y la fatiga que conlleva el trabajo en el incidente pueden jugar a la contra. Es esencial permanecer alerta y prestar atención a lo siguiente:

- El estado de seguridad general del sistema de cualquier equipo afectado al reincorporarse en la red mediante pruebas de integridad de los datos y estabilidad del sistema.
- La aplicación de parches para corregir vulnerabilidades de seguridad, especialmente después de restaurar un equipo desde una versión previa que pueda ser susceptible a sufrir un nuevo ataque.
- La verificación de que se han aplicado políticas y controles de seguridad adecuados a cada equipo:
  - El agente de seguridad debe desplegarse en todos los equipos reincorporados.
  - Las exclusiones de escaneado deben ser mínimas, personalizando las exclusiones y aplicaciones específicas en función del elemento, ordenador o grupo de usuarios excluido.
- El escaneado y la búsqueda de presencia de IOC identificados del ataque y cualquier punto de afianzamiento que el ciberdelincuente haya podido dejar a su paso.

Además, los expertos en respuesta a incidentes y los analistas de seguridad deben seguir supervisando el entorno para detectar más actividades de la amenaza y buscar proactivamente actividades comunes de los atacantes para identificar amenazas de manera preventiva y responder a ellas a medida que aparezcan.

La fase de recuperación no tiene por qué llevarse a cabo una vez finalizada la fase de erradicación, sino que las dos fases deben realizarse indistintamente, ya que los equipos restaurados a un estado seguro del sistema se pueden reincorporar en el entorno de producción.

Evaluación tras el incidente y lecciones aprendidas

Después de recuperarse con éxito de un incidente de ciberseguridad, es crucial realizar una evaluación a posteriori e identificar las lecciones aprendidas. Este proceso ayudará a su organización a analizar la efectividad de su respuesta a incidentes, identificar áreas de mejora e implementar cambios en el plan de respuesta a incidentes. Al hacerlo, podrá prepararse mejor para futuros incidentes y minimizar el riesgo de ataques similares.

Evaluación tras el incidente

Análisis de la efectividad de la respuesta a incidentes

Para evaluar la efectividad de la respuesta a incidentes de su organización, revise las acciones realizadas por el equipo de respuesta a incidentes y mida sus resultados. Considere los siguientes aspectos:

- Tiempo invertido en detectar, contener y remediar el incidente
- Comunicación y coordinación entre los miembros del equipo y con partes externas (p. ej., fuerzas del orden y proveedores)
- Idoneidad de las estrategias de contención, erradicación y recuperación
- Fiabilidad y utilidad de la información proporcionada por las herramientas de supervisión y detección

Identificación de áreas de mejora

Una vez analizada la efectividad de la respuesta a incidentes, identifique áreas en las que su organización pueda mejorar sus procesos y procedimientos. Algunas áreas de mejora comunes son:

- Programas de formación y concienciación de empleados
- Capacidades de supervisión y detección de incidentes
- Actualizaciones del plan de respuesta a incidentes
- Controles técnicos y medidas de seguridad
- Roles y responsabilidades del equipo de respuesta a incidentes
- Comunicación y colaboración externas con las partes interesadas

Implementación de cambios y actualizaciones en el plan de respuesta a incidentes

Tras identificar las áreas de mejora, es clave que se implementen cambios en el plan de respuesta a incidentes de su organización. Asegúrese de:

- Actualizar el plan con nuevos procedimientos, directrices o medidas técnicas según sea necesario.
- Comunicar los cambios a todas las partes relevantes, incluidos empleados, directivos y partes interesadas externas.
- Realizar ejercicios y formación regulares para garantizar que el plan actualizado se entiende y puede ejecutarse de manera efectiva.
- Supervisar y evaluar la efectividad de los cambios a lo largo del tiempo y realizar más cambios según sea necesario.

Al realizar una evaluación exhaustiva tras el incidente e identificar las lecciones aprendidas, su organización podrá mejorar su postura de ciberseguridad y prepararse mejor para futuros incidentes. Recuerde que el proceso de respuesta a incidentes es continuo, y que revisar y actualizar regularmente su plan contribuirá a garantizar la resiliencia de su organización frente a las ciberamenazas en evolución.

Lecciones aprendidas

Las lecciones aprendidas dependerán del tipo de incidente y del proceso de gestión del mismo, y representan áreas de mejora identificadas. La fase de lecciones aprendidas es una etapa crítica que suele omitirse una vez que el estado de máxima emergencia ha pasado, y los directivos ya no están directamente implicados cuando se recupera la normalidad operativa. Por consiguiente, es todavía más importante que la fase de lecciones aprendidas se produzca inmediatamente después de la fase de recuperación, y que cuente con la atención de los directivos para entender los detalles del incidente y ponerse de acuerdo en cuanto a las mejoras necesarias para mitigar futuros riesgos.

En la mayoría de casos, podría tratarse de un escrito sobre el incidente con un resumen ejecutivo que pueda compartirse con las partes interesadas no técnicas de la empresa y que estas puedan entenderlo. Este escrito debe ser colaborativo, es decir, admitir comentarios y ediciones por parte de las distintas partes interesadas, y debe acabar con un consenso sobre el informe final, incluidos los detalles técnicos y las lecciones aprendidas.

Dada la gran diversidad de áreas de mejora, a continuación se enumeran algunas de las más comunes, pero esta lista no debe considerarse específica ni exhaustiva.

Prácticas de seguridad recomendadas:

- Retire el software, las aplicaciones y el hardware obsoletos de la infraestructura corporativa para minimizar el riesgo de explotación.
- Establezca un proceso sólido de gestión de parches para el software y el hardware que se ajuste a las necesidades de la organización y garantice la actualización periódica de los parches.
- Instale agentes de protección de endpoints basada en la nube en todos los ordenadores de la infraestructura corporativa para detectar y neutralizar amenazas maliciosas.
- Implemente la autenticación multifactor (MFA) para VPN, RDP y otros dispositivos que requieran autenticación para incrementar la seguridad.
- Proteja la infraestructura implementando mecanismos de control de seguridad centrales y protegiendo los servicios conectados a Internet contra accesos no autorizados.
- Refuerce la gestión de credenciales aplicando requisitos de complejidad, usando gestores de contraseñas y rotando las credenciales con regularidad.
- Implemente protocolos de autenticación de correo, como DMARC, DKIM y SPF, para protegerse de correos electrónicos de phishing y suplantaciones.

Configuración de la red:

- Implemente sistemas de control de acceso a la red (NAC) para incorporar una capa de seguridad adicional y defenderse de dispositivos no autorizados y amenazas maliciosas.
- Segmente las redes utilizando redes VLAN para proteger sistemas críticos y datos confidenciales y aislar las plataformas y los servicios conectados a Internet dentro de una DMZ.

Endurecimiento:

- Implemente el bloqueo de IP geográficas en los firewalls para evitar tráfico de red no deseado en función de su origen geográfico.
- Despliegue soluciones de control de aplicaciones como AppLocker para impedir que aplicaciones y archivos no autorizados se instalen o se ejecuten en la infraestructura corporativa.
- Endurezca los controladores de dominio revisando y eliminando servicios innecesarios, software no compatible y protocolos heredados que puedan suponer un riesgo para la seguridad.

Gestión proactiva y precauciones de seguridad:

- **Auditoría de la infraestructura:** realice auditorías periódicas de las configuraciones de puertos de toda la infraestructura conectada a Internet dentro de la organización, a fin de garantizar que solo se permiten los servicios de protocolos necesarios y que los puertos de los flujos de red están correctamente configurados.
  - Por ejemplo, eth0 tiene conexión a Internet, mientras que eth1 solo es accesible internamente.
- **Auditoría de control web:** revise regularmente las configuraciones del tráfico web en servidores proxy y plataformas de flujos de tráfico web similares. Refuerce los controles de seguridad según sea aplicable, ajustándose al principio del mínimo privilegio. Implemente una política predeterminada de denegación o bloqueo. Por ejemplo:
  - Bloquee tipos de archivo que planteen riesgos innecesarios para la organización.
  - Revise las políticas de clasificación predeterminadas para URL y dominios sin categoría.
  - Exporte datos estadísticos para identificar anomalías, patrones o eventos sospechosos y maliciosos recurrentes.
  - Asegúrese de que los grupos y las políticas de seguridad se actualizan de acuerdo con el principio RBAC (control de acceso basado en roles).
- **Auditoría de cuentas:** realice auditorías periódicas de las cuentas de administrador local no aprobadas y no estándar o equivalentes dentro de la organización y elimínelas.

- **Registros de eventos de Windows:** configure los registros de eventos de Windows para preservar datos; por ejemplo, incrementando el tamaño de los principales registros de eventos de Windows a través de la Directiva de grupo o creando nuevos registros de eventos cuando se alcancen los límites de tamaño. Los registros de eventos de Windows ofrecen información forense valiosa.
- **Plan de respuesta a incidentes:** desarrolle, implemente, ponga a prueba y mantenga un plan de respuesta a incidentes de ciberseguridad para la organización. Revise y ponga a prueba el plan con regularidad, y actualice y ajuste su contenido según sea necesario.
- **Gestión de recursos de hardware y software:** implemente sistemas de gestión de recursos tanto de hardware como de software en toda la organización. Incorpore índices de priorización/criticidad dentro de la solución de gestión de recursos para identificar rápidamente los recursos de alto valor. Mantenga un inventario actualizado de los recursos de hardware y software, lo que ayuda a identificar posibles riesgos y posibilita la elaboración de planes estratégicos para abordarlos.
- **Topología de la red:** mantenga un diagrama de la topología de la red detallado y actualizado para la organización, que servirá de referencia para revisar las configuraciones y los tipos de infraestructura existentes y formular planes estratégicos para los cambios e implementaciones en la red. Durante un ataque de ciberseguridad, un diagrama de la topología de la red puede ayudar a los expertos en respuesta a incidentes a entender la estructura de la red de la organización, lo que permitirá acciones de respuesta a incidentes más específicas y oportunas.

Integridad de los datos

Copias de seguridad:

- Proteja los datos de copias de seguridad implementando distintas soluciones de copia de seguridad, almacenando los datos de copias de seguridad en ubicaciones de red aisladas/ tipos de soporte independientes de la infraestructura corporativa, y gestionando el acceso con controles de seguridad adecuados.
  - Empiece por establecer soluciones de redundancia de copias de seguridad basándose en la regla 3-2-1 y aplicando un correcto cifrado de los datos de copias de seguridad en reposo: cree tres copias de los datos, almacene los datos en al menos dos tipos de soporte diferentes y almacene al menos una copia de los datos fuera de las instalaciones de la organización.

Cifrado:

- Implemente el cifrado completo de disco en ordenadores, dispositivos móviles y unidades USB para proteger los datos de accesos no autorizados en caso de pérdida o robo de los dispositivos.
- Proteja los datos en reposo dentro de la organización implementando el cifrado de datos en reposo (DARE), priorizando los datos altamente confidenciales. Asegúrese de contar con mecanismos de cifrado adecuados para los datos de red en tránsito, como utilizar la versión más reciente de TLS (Seguridad de la capa de transporte) para los intercambios de comunicaciones cifradas que impliquen certificados digitales, e impedir que los servidores degraden suites de cifrado para adaptarse a tipos de navegador no compatibles.

Inversiones en seguridad

Utilice las lecciones aprendidas de los incidentes de seguridad para reivindicar financiación y mejoras presupuestarias en la postura de seguridad de la organización.

- Invierta en la formación y concienciación de los empleados. Puesto que las personas son a menudo el vector inicial de un ataque, invierta en:
  - Soluciones o formación de concienciación sobre el phishing que instruyan y pongan a prueba a los usuarios finales con respecto a las técnicas de phishing más comunes. Integre esa formación en la empresa como un ejercicio continuado a través de implementaciones programadas o simulaciones de ataque automatizadas, y proporcione la información necesaria para que el equipo de TI entienda a las víctimas más habituales y ofrezca orientación adicional.
  - Ampliación de competencias de los empleados en materia de seguridad TI, especialmente en análisis de seguridad, búsqueda de amenazas y respuesta a incidentes.

Servicios de ciberseguridad gestionados

- Contrate a profesionales de ciberseguridad especializados en análisis de seguridad, búsqueda de amenazas, respuesta a incidentes, ingeniería de herramientas de detección y seguridad, etc. Implementar un centro de operaciones de ciberseguridad permite a la empresa supervisar amenazas y responder a ellas 24/7.
- Invierta en una solución de ciberseguridad gestionada, como Sophos Managed Detection and Response (MDR). Los servicios de MDR son operaciones de seguridad subcontratadas que lleva a cabo un equipo de especialistas, el cual actúa como una extensión del equipo de seguridad del cliente.

Inversión en herramientas

- Sophos XDR (detección y respuesta ampliadas) es una solución que almacena y permite consultar información crítica procedente de productos para endpoints, servidores, firewalls, correo electrónico y otros productos habilitados para la XDR, lo que agiliza los flujos de trabajo de detección y respuesta a amenazas.
- La tecnología de información de seguridad y gestión de eventos (SIEM) ofrece funciones de detección de amenazas, cumplimiento normativo y gestión de incidentes recopilando eventos e información de varias fuentes de datos en un repositorio centralizado de datos de amenazas.
- Pueden realizarse otras inversiones en función de las lecciones aprendidas, y deben contribuir a mejorar la postura de seguridad, un requisito que se medirá por la capacidad de estas inversiones para subsanar carencias de protección/filtrado, detección y supervisión. Entre estas herramientas se incluyen los antivirus, sistemas de prevención/detección (IPS/IDS), firewalls, etc.

Al abordar estas áreas de mejora comunes, su organización podrá reforzar significativamente su postura de seguridad y protegerse mejor de futuros ciberincidentes. Recuerde que las lecciones aprendidas son un proceso continuo, y que revisar y actualizar regularmente sus prácticas de seguridad contribuirá a garantizar la resiliencia de su organización frente a las ciberamenazas en evolución.

Notificación de incidentes

Después de un incidente de ciberseguridad, es vital comunicar los detalles, las conclusiones y los pasos de remediación a las distintas partes interesadas. Notificar el incidente internamente, a las autoridades reguladoras y a las fuerzas del orden es crucial para mantener la transparencia, garantizar el cumplimiento normativo y ayudar en las investigaciones.

Notificación interna

Para fomentar una cultura de mejora y aprendizaje continuos, las organizaciones deben establecer un proceso de notificación interna claro. Este proceso debe incluir:

- Documentación del incidente, incluida la cronología de los eventos, los sistemas afectados y la naturaleza del ataque.
- Resumen del impacto del incidente en las operaciones, finanzas y reputación de la organización.
- Descripción de los pasos seguidos para contener, erradicar y recuperarse del incidente.
- Identificación de las lecciones aprendidas y recomendaciones para futuras mejoras en la postura de seguridad de la organización.
- Envío del informe del incidente a las partes interesadas relevantes, como el equipo directivo, los equipos de TI y los empleados y departamentos afectados.

Notificación a las autoridades reguladoras

Dependiendo de la jurisdicción y el sector, las organizaciones podrían tener la obligación de informar de los incidentes de ciberseguridad a las autoridades reguladoras. El cumplimiento de estos requisitos es esencial para evitar multas, sanciones y daños a la reputación de la organización. Al informar a las autoridades reguladoras, las organizaciones deben:

- Determinar cuál es la autoridad o autoridades a las que deben notificar, en función de la naturaleza del incidente y del sector y la ubicación de la organización.
- Revisar cualquier requisito de notificación relevante, incluidos la información necesaria y los plazos para informar.
- Preparar un informe detallado que se ajuste al formato y contenido requeridos especificados por la autoridad reguladora.
- Enviar el informe dentro del plazo que corresponda y mantener una comunicación abierta con la autoridad reguladora durante todo el proceso de investigación y resolución.

Notificación a las fuerzas del orden

En casos de actividad delictiva o ciberataques importantes, las organizaciones deben plantearse notificar el incidente a las fuerzas del orden. Esto puede ayudar en las investigaciones y posiblemente llevar a la detención de los atacantes. Al informar a las fuerzas del orden, las organizaciones deben:

- Identificar al organismo u organismos de las fuerzas del orden adecuados, como la policía local, las unidades de ciberdelincuencia nacionales o agencias especializadas (p. ej., el FBI).
- Recopilar pruebas relevantes, incluidos registros, imágenes del sistema y capturas del tráfico de red, preservando la cadena de custodia y cumpliendo cualquier requisito legal aplicable.
- Preparar un informe con los detalles del incidente, incluidos la naturaleza del ataque, los sistemas y datos afectados, la cronología de los eventos y cualquier información que se tenga sobre los atacantes.
- Cooperar con las fuerzas del orden durante toda la investigación, proporcionando información y asistencia adicionales según sea necesario.

Al seguir estas pautas para la notificación de incidentes, las organizaciones pueden garantizar que mantienen la transparencia, cumplen los requisitos normativos y contribuyen a la lucha contra la ciberdelincuencia.

Conclusión

Resumiendo, esta guía de planificación de la respuesta a incidentes ofrece un marco de acción integral para ayudar a las organizaciones a prepararse ante los incidentes de seguridad, gestionarlos y recuperarse de ellos de manera efectiva. Al implementar una gestión proactiva y precauciones de seguridad, garantizar la integridad de los datos, invertir en formación para empleados y herramientas de seguridad, y establecer unos procedimientos de notificación claros, las organizaciones pueden mejorar significativamente su resiliencia frente a las ciberamenazas.

Una planificación de la respuesta a incidentes efectiva no solo ayuda a las organizaciones a minimizar los daños provocados por los ciberataques, sino que también fomenta una cultura de mejora y aprendizaje continuos. Ante un panorama de ciberamenazas en constante evolución, las organizaciones deben revisar y actualizar regularmente sus planes de respuesta a incidentes para anticiparse a las amenazas y vulnerabilidades emergentes.

Seguir diligentemente las directrices incluidas en esta guía permitirá a las organizaciones estar mejor preparadas para detectar, contener y remediar los incidentes de ciberseguridad, proteger sus datos y recursos valiosos, mantener el cumplimiento de los requisitos normativos y salvaguardar su reputación en un mundo cada vez más interconectado.

Para obtener más información sobre el servicio Sophos Incident Response,

¿Está sufriendo un incidente activo?

Llame a nuestros números regionales de abajo en cualquier momento para hablar con uno de nuestros asesores de incidentes:

Australia: +61 272084454

Austria: +43 73265575520

Canadá: +1 7785897255

Francia: +33 186539880

Alemania: +49 61171186766

Italia: +39 0294752897

Países Bajos: +31 162708600

Suecia: +46 858400610

Suiza: +41 445152286

Reino Unido: +44 1235635329

EE. UU.: +1 4087461064

Correo electrónico: RapidResponse@Sophos.com

Nuestros asesores de incidentes responderán a su solicitud lo más rápido posible.

2023-09-01 (IRG-MP)

SOPHOS