SOPHOS
Cybersecurity delivered.

Cuatro consejos clave de los expertos en respuesta a incidentes

Sepa de antemano cómo responder a un ciberataque crítico

Responder a un ciberincidente crítico puede suponer un período increíblemente intenso y estresante. Aunque nada puede aliviar completamente la presión de tener que lidiar con un ataque, entender estos consejos clave de los expertos en respuesta a incidentes ayudará a dar ventaja a su equipo a la hora de defender su empresa.

En este documento se ponen de relieve las mayores lecciones que debería aprender cualquier persona en cuanto a cómo responder a los incidentes de ciberseguridad. Se basan en experiencias del mundo real de los equipos de Sophos Managed Detección and Response y Sophos Rapid Response, que han respondido de forma conjunta a miles de incidentes de ciberseguridad.

Consejo n.º 1: Reaccione lo antes posible

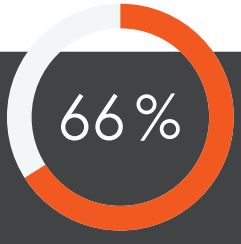
Cuando una empresa sufre un ataque, cada segundo cuenta.

Hay varias razones por las que los equipos pueden tardar demasiado en reaccionar. La más común es que no entienden la gravedad de la situación en la que se encuentran, y esta falta de conciencia se traduce en una falta de urgencia.

Los ataques suelen darse en los momentos más inoportunos: vacaciones, fines de semana y en mitad de la noche. Puesto que la mayoría de equipos de respuesta a incidentes sufren una notable escasez de personal, es comprensible que se adopte la actitud de dejarlo para mañana. Pero, por desgracia, mañana podría ser demasiado tarde para hacer algo que pueda minimizar el impacto del ataque.

Los equipos sobrecargados también tienen más posibilidades de reaccionar lentamente a los indicadores de ataque porque sufren fatiga por alertas, lo que significa que las señales se pierden entre el ruido. Incluso al abrirse un caso inicialmente, es posible que no se priorice correctamente debido a la falta de visibilidad y contexto. Esto lleva tiempo, y el tiempo no beneficia al defensor a la hora de responder a incidentes.

Incluso en situaciones en que el equipo de seguridad es consciente de que está sufriendo un ataque y que hay que hacer algo de inmediato, quizás no tenga la experiencia para saber qué hacer a continuación, lo que también ralentiza su respuesta. Lo mejor para luchar contra esto es la planificación previa a los incidentes.



Prácticamente dos tercios de las organizaciones fueron víctimas del ransomware el año pasado, y los atacantes lograron cifrar archivos en el 65 % de los casos.[1]

Consejo n.º 2: No cante victoria demasiado pronto

En lo que a la respuesta a incidentes se refiere, no basta con tratar solo los síntomas. Es importante tratar también la enfermedad.

Cuando se detecta una amenaza, lo primero que hay que hacer es clasificar el ataque inmediato. Esto puede significar limpiar un ejecutable con ransomware o un troyano bancario, o bloquear la exfiltración de datos. Sin embargo, los equipos suelen detener el ataque inicial sin darse cuenta de que realmente no han resuelto la causa raíz.

Conseguir eliminar el malware y descartar una alerta no implica que el atacante haya sido expulsado del entorno. También es posible que lo detectado fuera tan solo una incursión de prueba por parte del atacante para comprobar con qué defensas se enfrenta. Si el atacante sigue teniendo acceso, es probable que vuelva a atacar, pero de forma más destructiva.

Los equipos de respuesta a incidentes deben asegurarse de que resuelven la causa raíz del incidente original que han mitigado. ¿Sigue afianzado en el entorno el atacante? ¿Está planeando un segundo embate? Los gestores de respuesta a incidentes que han solventado miles de ataques saben cuándo y dónde investigar más a fondo. Buscan cualquier otra cosa que los atacantes estén haciendo, hayan hecho o estén planeando hacer en la red, y también lo neutralizan.

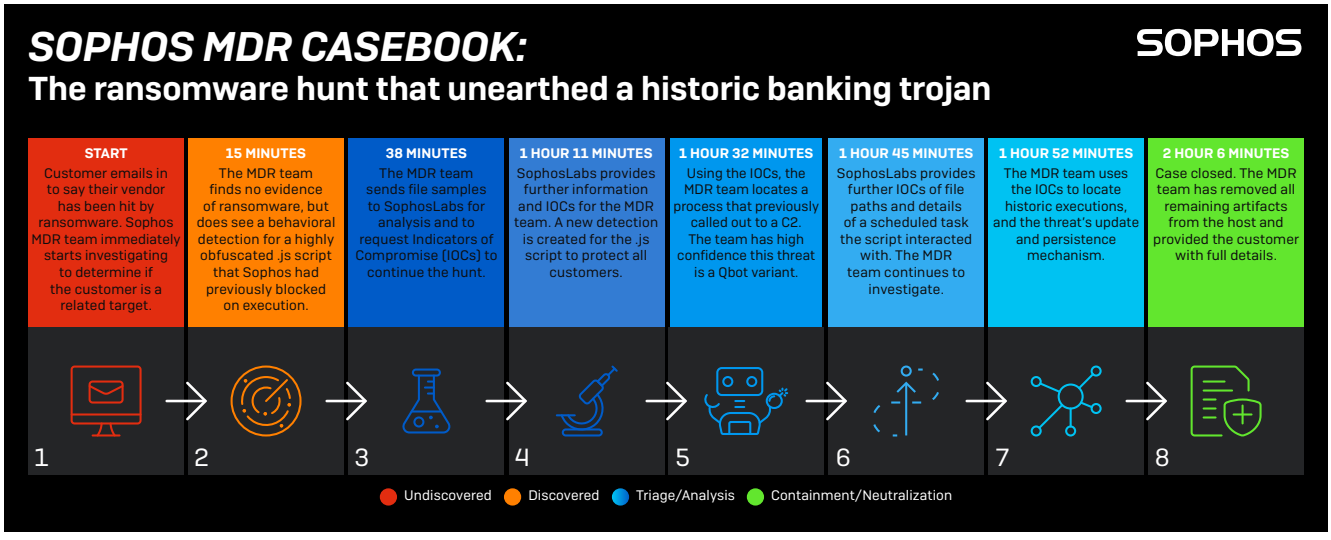
Por ejemplo, en una ocasión, los especialistas en respuesta a incidentes de Sophos consiguieron frustrar un ataque que duró nueve días y observaron tres intentos distintos por parte de los atacantes para arremeter contra una organización utilizando ransomware.

Como en ese momento todavía no era cliente de Sophos MDR, fue el equipo de Sophos Rapid Response el que intervino en primer lugar.

En la primera fase del ataque (que en última instancia fue bloqueada por la solución de protección para endpoints de la empresa), los atacantes dirigieron el ransomware Maze contra 700 ordenadores y pidieron un rescate de 15 millones de dólares. Al percatarse del ataque, el equipo de seguridad del objetivo implicó al equipo de Sophos Managed Detection and Response (MDR) para servirse de su avanzada capacidad de respuesta a incidentes.

Los especialistas en respuesta a incidentes de Sophos identificaron rápidamente la cuenta de administrador comprometida, identificaron y eliminaron varios archivos maliciosos y bloquearon los comandos y las comunicaciones de C2 (comando y control) del atacante. Después, el equipo de Sophos MDR logró neutralizar dos fases de ataque más por parte del adversario. Si los atacantes hubieran logrado su propósito y la víctima hubiera pagado, podría haber sido uno de los pagos de ransomware más caros hasta la fecha.

En otro ejemplo, el equipo de Sophos MDR respondió a una posible amenaza de ransomware, pero determinó rápidamente que no había indicios de ransomware. Llegados a este punto, algunos equipos habrían cerrado el caso y pasado a otra tarea. Sin embargo, el equipo de Sophos MDR siguió investigando y descubrió un troyano bancario histórico. Por suerte para este cliente, la amenaza ya no estaba activa, pero sirve como ejemplo de por qué es importante mirar más allá de los síntomas iniciales a fin de determinar la causa raíz completa, ya que podría tratarse de un indicador de un ataque más amplio.



Consejo n.º 3: Una visibilidad completa es crucial

Al evaluar un ataque, no hay nada que haga más difícil defender una empresa que moverse a ciegas. Es importante tener acceso a los datos de alta calidad correctos, que permiten identificar de forma precisa los posibles indicadores de ataque y determinar la causa raíz.

Los equipos eficaces recopilan los datos correctos para ver las señales, pueden distinguir las señales del ruido y saben qué señales es más importante priorizar.

Recopilación de señales

Una visibilidad limitada sobre un entorno es una forma segura de perderse los ataques. A lo largo de los años, se han introducido en el mercado muchas herramientas de datos masivos para tratar de resolver esta dificultad concreta. Algunas utilizan datos centrados en eventos como los eventos de registro, otras se sirven de datos basados en amenazas y otras aplican un enfoque híbrido. Sea como sea, el objetivo es el mismo: recopilar suficientes datos para generar información significativa a fin de investigar y responder a los ataques que de otra forma se pasarían por alto.

Recopilar los datos de alta calidad correctos de una amplia variedad de fuentes garantiza una completa visibilidad sobre las herramientas, las tácticas y los procedimientos (TTP, por sus siglas en inglés) del atacante. De lo contrario, es probable que solo se observe una parte del ataque.

Reducción del ruido

Por el temor de no poder disponer de los datos que necesitan para conseguir una visión completa de un ataque, algunas organizaciones (y las herramientas de seguridad que emplean) lo recopilan todo. Sin embargo, esto no hace más fácil encontrar la aguja en el pajar, sino que, al amontonarse más paja de la necesaria, aún resulta más difícil. Esto no solo incrementa los costes de la recopilación y el almacenamiento de los datos, sino que también crea mucho ruido, lo que se traduce en fatiga por alertas y en tiempo desperdiciado investigando falsos positivos.

Aplicación de contexto

Hay un dicho popular entre los profesionales de la detección y respuesta a amenazas: “Si el contenido es el rey, el contexto es la reina.” Ambos son necesarios para ejecutar un programa de respuesta a incidentes efectivo. Aplicar metadatos significativos asociados a las señales permite a los analistas determinar si estas señales son maliciosas o benignas.

Uno de los componentes más críticos de una detección y respuesta a amenazas efectiva es priorizar las señales que más importan. La mejor forma de localizar las alertas que más importan es con una combinación de contexto proporcionado por herramientas de seguridad (por ejemplo, soluciones de detección y respuesta para endpoints), inteligencia artificial, información sobre amenazas y la base de conocimiento del operador humano.

El contexto ayuda a determinar con precisión dónde se ha originado una señal, la fase actual del ataque, eventos relacionados y el posible impacto para el negocio.

Consejo n.º 4: No pasa nada por pedir ayuda

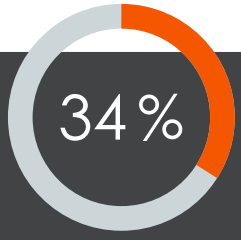
Ninguna empresa quiere enfrentarse a los intentos de infiltración. Sin embargo, no hay nada que pueda sustituir a la experiencia a la hora de responder a los incidentes. Esto significa que los equipos de TI y seguridad a los que se asigna frecuentemente la respuesta a incidentes de alta presión se ven abocados a situaciones para las que simplemente carecen de las habilidades necesarias, situaciones que a menudo tienen un enorme impacto sobre el negocio.

La falta de recursos cualificados para investigar y responder a incidentes es uno de los mayores problemas a los que se enfrenta el sector de la ciberseguridad hoy día. Este problema está tan extendido que, según ESG Research2, "el 34 % afirma que su mayor reto es que carecen de recursos cualificados para investigar un incidente de ciberseguridad que afecte a un endpoint a fin de determinar la causa raíz y la cadena de ataque".

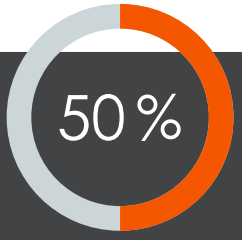
Este dilema ha dado paso a una nueva alternativa: los servicios de seguridad gestionados y, en concreto, los servicios de detección y respuesta gestionadas (MDR). Los servicios de MDR son operaciones de seguridad subcontratadas que lleva a cabo un equipo de especialistas, el cual actúa como una extensión del equipo de seguridad del cliente. Estos servicios combinan investigaciones realizadas por humanos, la búsqueda de amenazas, la supervisión en tiempo real y la respuesta a incidentes con una pila tecnológica para recopilar y analizar información. Según Gartner, "para el 2025, el 50 % de las organizaciones utilizará servicios de MDR"3, lo que apunta a la tendencia de que las organizaciones se están dando cuenta de que necesitarán ayuda para ejecutar un programa de operaciones de seguridad y respuesta a incidentes completo.

Para las empresas que aún no han contratado un servicio de MDR y están respondiendo a un ataque activo, los servicios especializados en respuesta a incidentes son una excelente opción. Los gestores de respuesta a incidentes intervienen cuando el equipo de seguridad está abrumado y necesita expertos externos para clasificar el ataque y garantizar la neutralización del adversario.

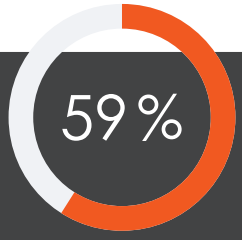
Incluso las empresas que cuentan con un equipo de analistas de seguridad cualificados pueden beneficiarse de la colaboración con un servicio de respuesta a incidentes para cubrir lagunas en la cobertura (por ejemplo, noches, fines de semana o vacaciones) y roles especializados que son necesarios al responder a incidentes.



Según la firma de análisis ESG, el 34 % de empresas afirma que su mayor reto es que carecen de recursos cualificados para investigar un incidente de ciberseguridad que afecte a un endpoint a fin de determinar la causa raíz y la cadena de ataque".[2]



Para el 2025, el 50 % de las empresas utilizará servicios de MDR (en 2019, la cifra era inferior al 5 %).[3]



En una encuesta a 5600 profesionales de TI en 2022, el 59 % afirmó que los ataques a su organización habían aumentado durante el último año.[4]

Cómo puede ayudar Sophos

Servicio Sophos Managed Detection and Response (MDR)

¿Le preocupa la capacidad de su empresa para responder a un posible incidente grave? En caso afirmativo, el servicio Managed Detection and Response (MDR) es una opción que vale la pena considerar.

Sophos MDR es un servicio totalmente administrado prestado por un equipo de expertos que ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas. Más allá de la simple notificación de ataques o comportamientos sospechosos, el equipo de Sophos MDR adopta medidas específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas. Si llega a producirse un incidente, el equipo de MDR emprenderá acciones para interrumpir, contener y neutralizar de forma remota la amenaza. El equipo de expertos en operaciones de seguridad también brindan asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Más información en es.sophos.com/mdr

Servicio Sophos Rapid Response

Si su empresa está sufriendo un ataque y necesita ayuda inmediata para responder al incidente, Sophos puede asistirle.

Sophos Rapid Response es un servicio prestado por un equipo experto de gestores de respuesta que proporciona una asistencia ultrarrápida con identificación y neutralización de amenazas activas contra empresas. La incorporación empieza en cuestión de horas, y la mayoría de clientes son clasificados en un plazo de 48 horas. El servicio está disponible tanto para los actuales clientes de Sophos como para los que no lo son.

El equipo remoto de gestores de respuesta a incidentes de Sophos Rapid Response toma medidas rápidamente para clasificar, contener y neutralizar las amenazas activas. Los adversarios son expulsados de su entorno para evitar más daños a sus recursos.

Más información en es.sophos.com/rapidresponse

Sophos XDR

Sophos XDR es la única solución XDR del sector que sincroniza la protección nativa de endpoints, servidores, firewalls, correo electrónico, la nube y M365. Obtenga una visión holística del entorno de su organización con conjuntos de datos exhaustivos y un análisis profundo para la detección, investigación y respuesta a las amenazas, tanto para los equipos SOC dedicados como para los administradores de TI.

Más información y evaluación gratuita en es.sophos.com/xdr

[1] El estado del ransomware 2020, resultados de una encuesta independiente y desvinculada de cualquier proveedor a 5600 directores de TI de 31 países: https://www.sophos.com/es-es/whitepaper/state-of-ransomware
[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1
[3] Gartner, Guía de mercado de servicios de detección y respuesta gestionados, 26 de agosto de 2020; Analistas: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson y Mitchell Schneider
[4] El estado del ransomware 2020, resultados de una encuesta independiente y desvinculada de cualquier proveedor a 5600 directores de TI de 31 países: https://www.sophos.com/es-es/whitepaper/state-of-ransomware

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

22-08-08 WPES (PC)

SOPHOS