Respuesta a incidentes: ¿Está preparado?

Qué incluye

1. Sentirse seguro sobre la seguridad de la red
2. ¿Por qué es necesario un plan de respuesta a incidentes?
3. ¿Cuáles son los componentes de un plan de respuesta a incidentes sólido?
4. ¿Cómo puede ayudarlo Cisco?
5. Historias de éxito
6. Recursos adicionales

1. Sentirse seguro sobre la seguridad de la red

¿Sabe lo que hacen los empleados en su red? ¿Está al tanto del más reciente ataque de ransomware que está combatiendo el equipo de seguridad? ¿Qué puede decir de sus partners de negocio? ¿Están protegidos?

Con todas estas preguntas rondando en su cabeza, es difícil sentirse protegido en relación a la seguridad de la red. Sin embargo, hay algo que podría ayudar: un plan sólido.

Tal vez usted es consciente de que su organización debe tener un plan formal de respuesta a incidentes. O quizá ya cuenta con uno. Pero, ¿tiene totalmente claros todos los componentes que deben conformar dicho plan? ¿O qué hacer cuando las cosas salen mal? ¿O cómo obtener ayuda cuando la necesita?

Durante las próximas páginas, le ofreceremos información para que pueda construir y fortalecer el plan de respuesta a incidentes de su organización.

2. ¿Por qué es necesario tener un plan?

En primer lugar, eche un vistazo a este video para descubrir por qué es fundamental una estrategia sólida de respuesta a incidentes.

Ver el video

Da miedo, ¿no? Incluso más aterrador es el hecho de que una organización promedio demora entre 100 y 200 días para detectar un incidente de seguridad.[1] Y debido a las restricciones de recursos, casi la mitad de estos incidentes (44 por ciento) ni siquiera se investigan.[2]

[1] Informe anual sobre Ciberseguridad de Cisco 2016

[2] Informe anual sobre ciberseguridad de Cisco 2017

3. ¿Cuáles son los componentes de un plan de respuesta a incidentes sólido?

Detección de amenazas

El primer paso para responder a las amenazas es, por supuesto, detectarlas. Para esta tarea faraónica, debe contar con capacidad intelectual y tecnología. Asegúrese de que su equipo de seguridad esté al día sobre las últimas amenazas y sepa qué buscar en la red. Por supuesto que los seres humanos necesitan dormir, por lo que necesitará herramientas de análisis y monitoreo de la seguridad las 24 horas para ayudarlos a proteger la red. Y no olvide de capacitar a los empleados. Capacite a los usuarios a reconocer cuando algo no está bien, y considérelos una extensión de su equipo de seguridad. ***Cuando se trata de un incidente de seguridad, la preparación es tan importante como la respuesta.***

Evaluación y contención

Cuando aparece inevitablemente el incidente de seguridad, la fase de evaluación y contención puede significar la diferencia entre una corrección veloz y una escandalosa violación de datos públicos. Las herramientas de seguridad sólidas son fundamentales en esta fase, pero deben complementarse con un equipo perspicaz de profesionales en toda la empresa, así como procesos herméticos. No espere hasta tener un incidente de seguridad real para establecer este equipo y plan. Establezca el plan de antemano y, una vez implementado, recuerde que la práctica conduce a la perfección.

Componentes de respuesta a incidentes, continuación.

Análisis forense y otros análisis

Mientras elimina un incidente, asegúrese de prestar atención a cómo sucedió. Es aquí donde los análisis forense y de seguridad entran en juego. Para evitar futuros incidentes de la misma naturaleza, debe saber el *quién, qué, cuándo, dónde, por qué,* y *cómo*. Y una vez más, para lograr con eficacia este paso, se necesita la combinación adecuada de herramientas y talento.

Mejoras en la seguridad

Por último, asegúrese de aplicar lo aprendido durante el incidente. Si bien los incidentes de seguridad son muy incómodos y, a menudo, destructivos, también pueden proporcionar lecciones valiosas. ¿Descubrió algunas debilidades en sus tecnologías de seguridad? ¿Necesita reclutar ayuda adicional para hacer frente a futuros incidentes? ¿Puede ser que sus procesos de respuesta a incidentes necesiten ajustes? De ser así, ocúpese de estas cosas antes del próximo ataque.

¿Busca una forma sencilla de dar los primeros pasos en todo este tema?

Configuración de un programa de respuesta ante incidentes

1. Identifique a un líder de respuesta a incidentes que posea una sólida comprensión de su negocio y la estrategia de seguridad de su organización, y que, además, sepa resolver problemas de manera eficaz y responsable.
2. Forme y capacite a un equipo de integrantes fundamentales de todo el entorno empresarial, con funciones y responsabilidades claramente definidas.
3. Documente el proceso de respuesta a incidentes. La clave es la consistencia. No tiene que ser complicado. Solo asegúrese de que funciona para la cultura de su organización y los requisitos empresariales.
4. Asigne sus capacidades requeridas de respuesta a incidentes al personal, el programa de seguridad y herramientas que ya existen en su organización.
5. Comprenda las brechas más importantes de capacidad en su proceso de respuesta a incidentes y desarrolle un plan para abordarlas. Comience con un mínimo proceso viable y, luego, auméntelo con el tiempo.

4. ¿Cómo puede ayudarlo Cisco?

Tecnología

Cisco ofrece un exhaustivo portafolio de soluciones de seguridad integradas que lo ayudarán a detectar y solucionar incidentes con mayor rapidez. Si necesita bloquear incidentes o identificar posibles ataques con antelación, eche un vistazo:

- Cisco Umbrella: es su primera línea de defensa, ya que ofrece seguridad web por donde sea que vayan sus usuarios *(y pasarán por muchos lugares).*
- Cisco Stealthwatch: la visibilidad de la red y el análisis de seguridad le permiten ver finalmente qué hacen los usuarios en su entorno.
- Cisco Threat Grid: Ahora que sabe lo que hacen los usuarios, averigüe lo que hace el malware. *(Sí, por desgracia, probablemente tiene malware.)*
- Cisco AMP para terminales: La seguridad contra malware avanzado protege a sus usuarios y las máquinas *(cuando inevitablemente entran en contacto con esos elementos desagradables en línea)*.

Esta es la mejor parte: Cisco ha coordinado todos estos productos para que funcionen juntos y formen una barrera más resistente contra atacantes. A través de la integración y la automatización, puede proteger su red con más confianza durante todo el ciclo de un ataque.

Cisco también ofrece . . .

Inteligencia de amenazas

Las herramientas no son nada sin la inteligencia. Todos nuestros productos y servicios de seguridad están respaldados por una investigación de amenazas implacable, llevada a cabo por el grupo Cisco Talos™. De hecho, Talos mantiene la red de detección de amenazas más grande del mundo.

Servicios profesionales de seguridad

¿Necesita más ayuda? Nuestro equipo de servicios de seguridad avanzados está disponible para ayudarlo a prepararse, responder y recuperarse de incidentes de seguridad. Los miembros experimentados de nuestro equipo tienen pleno acceso a tecnologías de seguridad de Cisco para mejorar la visibilidad y la velocidad, y proporcionar una comprensión más amplia de todas las amenazas en su red. No tiene que hacerlo solo.

5. Historias de éxito

¿Desea saber cómo lo hicieron otras personas? Consulte nuestro sitio interactivo para enterarse de cómo grandes empresas de renombre mundial como Yelp, Elavon e incluso Cisco han reforzado sus defensas con la seguridad de Cisco.

Visite la experiencia interactiva

Mientras tanto, aquí le ofrecemos algunos presupuestos para que empiece:

“El valor de usar Umbrella es que es una excelente primera línea de defensa frente al malware y el ransomware. Pasamos de ver varios incidentes de malware por día a ver solo unos pocos.”

Vivek Raman
Jefe de Seguridad, Yelp

El mayor activo de Stealthwatch para mi equipo siempre ha sido el hecho de que, cuando nadie está prestando atención, Stealthwatch sigue observando en segundo plano.

Phil Agcaoili
Director general de seguridad de la información, Elavon

AMP tiene la capacidad única de observar no solo cuando un archivo ingresa en su red, sino también todos los lugares por donde pasa mientras está en su red, y esto es fundamental para que funcione la respuesta a incidentes.

Michael Scheck
Gerente del equipo de respuesta de seguridad informática, Cisco

6. Recursos adicionales

Evaluación de la eficacia en seguridad

Realice esta breve prueba para aprender a mejorar la eficacia en materia de seguridad de su organización.

Iniciar prueba

Fortalecer la defensa contra la violación de datos

Obtenga más información sobre el Servicio de conservación de respuesta a incidentes de Cisco en este video de dos minutos.

Ver video

Sitio interactivo de respuesta a incidentes

¿No se cansa de nuestro contenido de respuesta a incidentes? Para más información, consulte nuestro sitio interactivo.

Visite la experiencia interactiva

¿Está experimentando un incidente ahora?

Póngase en contacto con nosotros inmediatamente. Estamos disponibles a nivel mundial, las 24 horas del día, todos los días del año.

Correo electrónico
IncidentResponse@cisco.com

C96-739835-01 01/18