KPMG

Navegando las consecuencias: Lecciones de la interrupción de Crowdstrike

Más 7 acciones clave de backup y recuperación.

En una era en la que la tecnología sustenta casi todos los aspectos de las operaciones empresariales, la resiliencia de los sistemas informáticos para soportar interrupciones repentinas es vital. El apagón informático del viernes 19 de julio, provocado por una actualización automática de software desplegada por la empresa de ciberseguridad CrowdStrike subraya la fragilidad de estos sistemas.

Al parecer, el código que paralizó temporalmente las operaciones financieras, sanitarias, del 911, de transporte y comerciales a escala mundial no fue el resultado de un fallo de ciberseguridad.

Irónicamente, la interrupción generalizada fue causada por un parche de software destinado a detectar y analizar amenazas.

Numerosas organizaciones de los sectores público y privado que utilizan el omnipresente sistema operativo Windows de Microsoft sufrieron el viernes una interrupción informática.

En las primeras horas -empezando en Australia y continuando hacia el oeste- una actualización de software defectuosa de la empresa de ciberseguridad CrowdStrike hizo que los ordenadores basados en Windows se bloquearan continuamente.

Aunque CrowdStrike ha declarado públicamente que el problema no estaba relacionado con un ciberataque, lo que resulta tranquilizador, su impacto en los sistemas informáticos mundiales es significativo y revela lecciones críticas para las empresas en torno a las estrategias de preparación y respuesta.

Y ha hecho que muchas empresas reexaminen los procesos del ciclo de vida de desarrollo de software (SDLC) de sus socios externos y sus propios planes de continuidad de negocio.

El incidente al descubierto

En este caso, CrowdStrike publicó una actualización defectuosa de su software de seguridad de sensores Falcon para Windows.

Para miles de ordenadores en muchas organizaciones, esto inició un bucle del infame. La "pantalla azul de la muerte" de Windows, un indicador de caída del sistema.

La solución simplificada consiste en arrancar la máquina infectada en modo seguro, eliminar el archivo defectuoso y reiniciar. El obstáculo es que la mayoría de los sistemas actuales de Microsoft están cifrados con BitLocker, que requiere una clave de recuperación (si no está familiarizado con una clave BitLocker, es una cadena de caracteres excesivamente larga).

Como resultado, los administradores de TI de todo el mundo se vieron obligados a ir de servidor en servidor -y en algunos casos, físicamente de escritorio en escritorio- con unidades USB que contenían claves de BitLocker para volver a poner en marcha manualmente estos sistemas. Se trata de un proceso laborioso y muy manual. Lleva mucho tiempo ir punto por punto para reiniciar cada sistema afectado.

No se trató simplemente de un fallo técnico. Fue una llamada de atención a las organizaciones de todo el mundo sobre la importancia de contar con protocolos de SDLC sólidos y estables y sobre la necesidad de una planificación exhaustiva de la continuidad de la actividad.

Planificación de copias de seguridad y recuperación

Mientras muchas organizaciones siguen trabajando para restablecer sus operaciones, el incidente pone aún más de relieve la importancia de mantener una estrategia de copia de seguridad y recuperación eficaz y con capacidad de respuesta para mitigar el impacto de tales interrupciones.

Esto incluye evaluar la capacidad de recuperación a gran escala y bajo presión.

En este contexto, destacamos siete medidas clave:

1. Desarrolle una estrategia de copia de seguridad y recuperación adaptada a su organización.

2. Realice pruebas periódicas de su estrategia de copia de seguridad y recuperación para asegurarse de que se mantiene correctamente y está actualizada.

3. Evalúe su capacidad para ejecutar su estrategia a escala en función de sus objetivos de recuperación.

4. Incorpore escenarios de pérdida de acceso en su planificación de recuperación ante desastres, incluidas situaciones en las que puede ser necesario el acceso físico, así como la pérdida de acceso a la red de la empresa para entornos alojados en la nube y de terceros.

5. Realice evaluaciones de impacto periódicas para comprender mejor el radio de explosión si falla un servicio o una aplicación específica o se produce una brecha en la red.

6. Revise su lista de proveedores de software y otros terceros críticos para evitar una dependencia excesiva o una concentración excesiva en uno o un número reducido de proveedores y realice evaluaciones periódicas de los controles en terceros críticos.

7. Revise las pólizas de seguros en relación con los cortes de suministro de terceros para determinar si el impacto financiero puede reducirse mediante la cobertura del seguro de interrupción de la actividad empresarial.

La importancia de la gestión del riesgo de terceros

La interrupción de CrowdStrike es un claro recordatorio de la necesidad de actuar con diligencia a la hora de seleccionar y supervisar los proveedores externos, especialmente los que son fundamentales para la infraestructura de TI.

En este caso, un fallo en el SDLC y en el proceso de gestión de cambios de CrowdStrike provocó interrupciones en cascada en todo el mundo.

Utilizar proveedores con procesos rigurosos de SDLC y gestión de cambios no es opcional, sino una necesidad.

Las empresas deben intensificar su escrutinio de las prácticas de los proveedores externos.

En concreto, se anima a las empresas a mejorar sus programas para incluir:

- **Evaluación rutinaria de riesgos:** Mantenga un amplio inventario y realice una evaluación de riesgos de terceros implicados en el suministro de software y servicios empresariales para evaluar su viabilidad operativa, salud financiera, prácticas de seguridad, historial de cumplimiento e incidentes anteriores.
- **Protecciones contractuales:** Defina acuerdos de nivel de servicio claros que definan las expectativas de rendimiento, los requisitos de tiempo de actividad y las sanciones por incumplimiento.
- **Auditoría y supervisión periódicas:** Realice revisiones periódicas de los controles implantados en terceros, incluidas auditorías periódicas, revisiones de los SOC1/SOC2 y un diálogo permanente con los proveedores críticos para abordar de forma proactiva los problemas y preocupaciones. Son especialmente importantes los procesos de actualización y certificación de software: es crucial pedir a los proveedores que realicen pruebas y validaciones exhaustivas antes de desplegar las actualizaciones.

Planes de resiliencia y contingencia

Más allá de las soluciones técnicas inmediatas, las organizaciones deben cultivar una cultura de resiliencia, incorporando sólidos planes de contingencia que abarquen no sólo la infraestructura informática, sino también las operaciones empresariales clave.

La capacidad de recuperación no significa que nunca vaya a producirse otro incidente: es probable que sí. Significa estar mejor equipado para gestionar futuros incidentes de forma rápida, eficaz y con un impacto limitado en la empresa.

Las organizaciones no pueden controlar las amenazas externas, pero sí su propia preparación.

En conclusión

La interrupción de CrowdStrike es un recordatorio convincente de la naturaleza interconectada de los ecosistemas informáticos modernos y de los efectos en cascada que un único punto de fallo puede tener en las operaciones globales.

A medida que las empresas se adentran en la era digital, invertir en infraestructuras resistentes, en una rigurosa gestión de riesgos de terceros y en planes de recuperación amplios y coordinados no sólo es prudente, sino esencial. De este modo, las organizaciones pueden protegerse más eficazmente de las consecuencias de futuros incidentes y mejorar su capacidad para mantener la continuidad ante retos imprevistos.

Cómo puede ayudar KPMG

Las empresas inteligentes no sólo gestionan el riesgo, sino que lo utilizan como fuente de crecimiento y ventaja competitiva. La tecnología hace que muchas cosas sean posibles, pero lo que es posible no siempre es seguro. Podemos ayudarle a crear un entorno digital resiliente y de confianza frente a las vulnerabilidades y amenazas cambiantes. En concreto,podemos:

- Revisar y probar sus planes de continuidad de la actividad y recuperación de datosBCP/DR).
- Revisar y poner a prueba su estrategia de ciberresiliencia.
- Revisar su estrategia de gestión de riesgos de terceros y de gestión de la cadena de suministro.
- Colaborar en la reparación de Crowdstrike para esta interrupción actual. Tenemos un acuerdo global con Crowdstrike y podemos apoyarlo, sin costo, en la recuperación de sus servicios tecnológicos.
- Añadir capacidad de respuesta rápida a través de nuestros servicios de Ciberseguridad para Gestión y Recuperación ante Ciber Incidentes (por demanda o prepagados) para mejorar su habilidad para gestionar y mitigar los futuros incidentes."

Nuestros profesionales aportan una combinación de experiencia tecnológica, profundos conocimientos empresariales, creatividad y pasión por proteger y hacer progresar su negocio.
Estamos a su disposición para ayudarle a proteger y optimizar su entorno digital.

Póngase en contacto con nosotros

Jaime Vásquez
Socio Líder Advisory
javasquez@kpmg.com

Alain Almeida
Socio Technology Enablement
abalmeida@kpmg.com

Felipe Silgado
Director Cyber Security Services
fsilgado@kpmg.com

KPMG. Marca la diferencia.

Fecha de publicación: Julio 2024