Escuela Superior de Guerra “General Rafael Reyes Prieto”

Evento Crowdstrike

MY. Gustavo Adolfo Cañón Romero

MY. Rubén Darío Guarnizo Torres

MY. Edison Fernando Jiménez Rosero

MY. Cristian David Rengifo Diaz

DO. Jaider Ospina Navas

Habilidades Practicas en el Ciberespacio

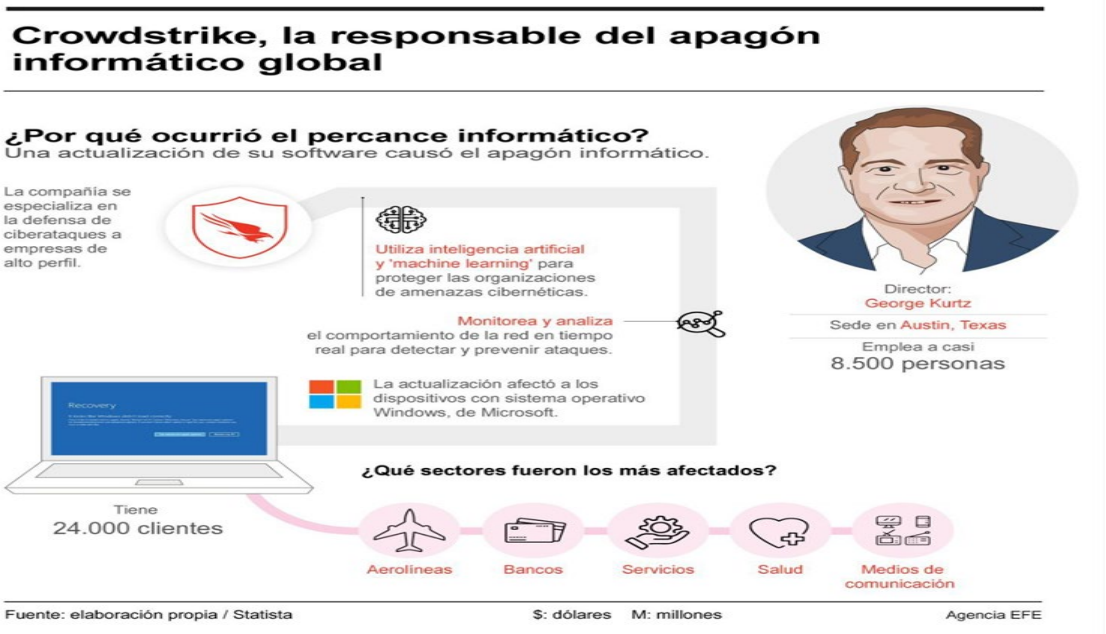
Maestría en Ciberseguridad y Ciberdefensa

30 de julio de 2024

El Evento Crowdstrike

La empresa de crowdsourcing Crowdstrike emitió una actualización defectuosa para su software de sensor Falcon en sistemas Windows el 19 de julio de 2024. La falla del sistema que ocurrió con esta actualización fue causada por un error lógico, lo que provocó la aparición de pantallas azules de la muerte en millones de dispositivos Windows a nivel mundial.

Aproximadamente 8,5 millones de dispositivos Windows se vieron afectados, según el informe de Microsoft. Líneas aéreas, bancos, hospitales, servicios de emergencia y otros sectores vitales se vieron gravemente afectados por el suceso. El suceso subrayó la vulnerabilidad de la infraestructura de TI interconectada y el potencial de actualizaciones automáticas de software de seguridad con acceso profundo al sistema. Se cree que el evento causó pérdidas a las empresas por miles de millones de dólares, pero aún no se conocen las consecuencias económicas exactas. Este hecho desencadenó debates sobre las mejores prácticas para actualizaciones de software críticas y gestión de riesgos cibernéticos. Este evento no malicioso fue uno de los incidentes de interrupción cibernética más importantes de los últimos años y afectó a organizaciones de todo el mundo.



Fuente: https://boyaca7dias.com.co/2024/07/20/infografia-crowdstrike-la-responsable-del-apagon-informatico-global/

Causas:

- Un error en la actualización de configuración de Crowdstrike para sistemas Windows provocó la instalación de una actualización que no funcionaba correctamente para el sensor Falcon. El archivo de canal "c-00000291*sys" provocaba fallos debido a que no coincidía o estaba dañado después de la actualización.
- Los defectos en las actualizaciones no se detectaron durante el riguroso proceso de prueba antes del lanzamiento. La rápida difusión del error se vio facilitada por las actualizaciones automáticas periódicas del software de seguridad que se introdujeron.
- En Windows, el software Falcon opera a nivel del kernel, lo que significa que un solo error puede provocar problemas graves en el sistema.
- La ausencia de mecanismos de reversión rápida significaba que la actualización problemática no podía revertirse rápidamente una vez descubierta.
- La interdependencia de los sistemas informáticos modernos facilitó la rápida propagación y escalada del problema.
- El hecho de que Microsoft haya firmado criptográficamente esta actualización implica que puede haber habido deficiencias en los procesos de revisión multipartita, lo que puede no haber sido el caso. La complejidad inherente del software de seguridad a nivel del sistema aumenta la probabilidad de errores críticos
- La necesidad de actualizaciones frecuentes para mantenerse al día con las nuevas amenazas puede haber provocado un retraso en el proceso de lanzamiento

Cronología.

19 de julio de 2024

- 04:09 UTC: Crowdstrike actualiza los sistemas Windows con un sensor Falcon defectuoso.
- Entre las 04:09 y las 05:27 UTC: La configuración actualizada en los sistemas que se descargaron automáticamente comenzó a fallar y mostrar pantallas azules de muerte BSOD.

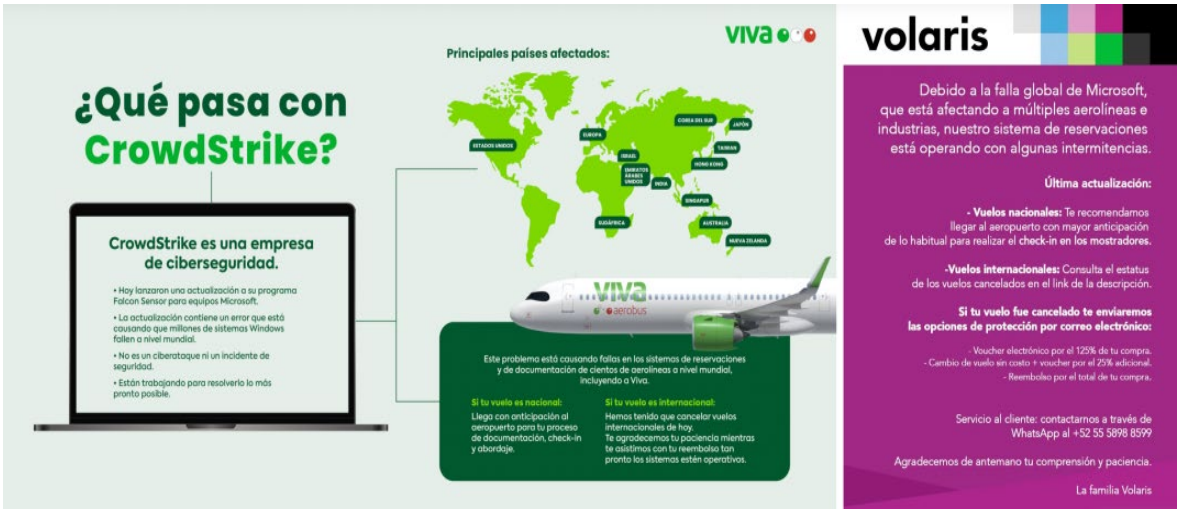
- 05:27 UTC: El problema se puede evitar actualizando la configuración del sensor mediante correcciones de Crowdstrike deteniendo su propagación.
- Horas siguientes: Comienzan a surgir informes generalizados de interrupciones en aerolíneas, bancos, hospitales y otros servicios críticos en todo el mundo.
- Crowdstrike emite comunicados reconociendo el problema y proporcionando información para la recuperación.
- Días posteriores: Continúan los esfuerzos de recuperación, mientras las empresas y organizaciones se esfuerzan por restaurar sus sistemas afectados a su máximo potencial.
- Semanas posteriores: Comienzan los estudios sobre las consecuencias económicas y operativas del evento.

Cabe señalar que la recuperación de todos los sistemas afectados puede haber tardado días o semanas en algunos casos debido a la necesidad de restauración manual de muchos dispositivos.

Acciones de remediación.

1. CrowdStrike solucionó una actualización que fallaba aproximadamente 1 hora y 20 minutos después de su lanzamiento inicial.
2. CrowdStrike emitió una declaración reconociendo el problema y brindando orientación a los clientes afectados.
3. CrowdStrike publico instrucciones detalladas para los clientes sobre cómo recuperar los sistemas afectados. Esto incluía:
    - Arrancar los sistemas Windows en modo seguro.
    - Buscar y eliminar el archivo problematico "C-00000291*.sys".
    - Reiniciar la máquina normalmente.

4. Crowdstrike trabajo directamente con los clientes para asegurar que volvieran a estar en línea, según lo declarado por el CEO Geroge Kurtz.
5. Microsoft anuncio el lanzamiento de una herramienta que le permite eliminar automáticamente archivos de canales problemáticos utilizando una memoria USB de arranque.
6. En muchos casos, se requirió la intervención manual del equipo de TI de la organización afectada para reiniciar el sistema y eliminar el archivo problema.
7. CrowdStrike y otras organizaciones de seguridad monitorearon activamente la situación en busca de posibles intentos de explotar la vulnerabilidad.
8. Se emitieron alertas sobre posibles ataques de phishing que intentan aprovechar la interrupción causada por el incidente.
9. Es posible que CrowdStrike haya iniciado un análisis interno detallado para comprender la causa raíz y prevenir incidentes similares en el futuro.
10. El proceso de actualización de CrowdStrike implemento medidas adicionales de seguridad y control de calidad.



Fuente: https://verificado.com.mx/el-apagon-informatico-falla-crowdstrike-falcon/

Análisis.

El evento se considera uno de los incidentes de ciberdisrupción no maliciosa más importantes de los últimos años.

El impacto afectó a aproximadamente 8,5 millones de dispositivos Windows en todo el mundo y también afectó a sectores críticos como la aviación, la banca, la atención médica y los servicios de emergencia, destacando las vulnerabilidades de la infraestructura digital conectada. El problema se debió a una falla en la actualización de CrowdStrike del software Falcon Sensor. Los archivos de canal mal formateados provocaron que los sistemas Windows fallaran y provocaran la infame "Pantalla Azul de la Muerte".

La rápida propagación de esta falla se debió a la naturaleza de este software, que opera a nivel de kernel y se actualiza automáticamente, exponiendo los sistemas de seguridad con acceso profundo y actualizaciones frecuentes a riesgos inherentes.

El impacto económico y operativo fue significativo, con pérdidas para las empresas afectadas estimadas en miles de millones de dólares.

La interrupción de servicios críticos como aerolíneas y hospitales tuvo un impacto importante, destacando la importancia de la resiliencia de la infraestructura digital crítica.

CrowdStrike resolvió el problema en poco más de una hora, pero la recuperación fue un proceso más largo y complicado. Muchos sistemas requirieron intervención manual, lo que aumentó el tiempo de inactividad y dificultó la recuperación. Este aspecto de este incidente resalta la necesidad de planes más sólidos de continuidad del negocio y recuperación ante desastres.

Este evento proporciono información valiosa sobre la gestión de riesgos cibernéticos. Esto resalta la importancia de pruebas rigurosas y procesos de garantía de calidad para actualizaciones de software críticas, mecanismos de reversión rápida y la necesidad de diversificar los proveedores de seguridad para reducir el riesgo del sistema.

Para la industria de seguros, este caso podría llevar a una reevaluación de las pólizas de seguro cibernético, particularmente con respecto a la cobertura de “fallo del sistema” y los períodos de espera por interrupción del negocio. También plantea preguntas

fundamentales sobre el equilibrio entre la necesidad de actualizaciones de seguridad frecuentes y el riesgo de falla del sistema.

La magnitud del impacto pone de relieve la interconexión de los sistemas de TI modernos y cómo un único punto de falla puede tener efectos en cascada.

Este incidente brinda una oportunidad para que la industria mejore sus prácticas, incluido el desarrollo de mejores procesos de lanzamiento y prueba de actualizaciones, el aumento de la transparencia y la comunicación del incidente y el desarrollo de estrategias de recuperación cibernética más sólidas. Además, este evento creó las siguientes amenazas secundarias, como ataques de phishing destinados a aprovechar la confusión provocada por el incidente. Resaltando la necesidad de una vigilancia constante incluso mientras se recupera de un evento no malicioso.

En última instancia, el incidente de CrowdStrike es un recordatorio importante de las vulnerabilidades potenciales de los sistemas digitales conectados y la necesidad de una gestión de riesgos cibernéticos más sólida y holística. Esto resalta la importancia crítica de la preparación, la resiliencia y las capacidades de respuesta rápida en el entorno digital actual y proporciona lecciones valiosas para empresas, gobiernos, proveedores de tecnología y otros por igual.

Explicación del slide.

Este slide proporciona una breve explicación del evento CrowdStrike desde una perspectiva técnica y práctica.

Según la imagen, el anillo representa la arquitectura de protección en capas del sistema operativo conocida como "anillo de protección".

Esta estructura separa diferentes niveles de interacción dentro del sistema operativo y proporciona una capa de seguridad y aislamiento.

Anillo 0 (procesos e hilos): Esta es la capa más centralizada y privilegiada conocida como “Trust Layer – Operating System Kernel”. Aquí es donde se ejecutan los procesos más importantes y confiables del sistema operativo.

Anillo 1 (Nivel de confianza): Este anillo contiene componentes del sistema operativo que requieren altos privilegios, pero no requieren acceso directo al hardware.

Anillo 2: (nivel de abstracción de hardware): controladores del sistema de archivos y utilidades del sistema operativo. Esto incluye controladores de dispositivos y otras utilidades del sistema que interactúan directamente con el hardware, pero que no requieren el nivel más alto de permisos.

Anillo 3: (Nivel de usuario): Aquí, las aplicaciones normales del usuario se ejecutan con privilegios mínimos y acceso al sistema.

Esta arquitectura en anillo está destinada a brindar protección contra fallas entre usuarios, componentes, aplicaciones y procesos informáticos y cada uno de estos anillos tienen diferentes niveles de privilegio y acceso, y los anillos interiores tienen más control y acceso al sistema que los anillos exteriores. Esto mantiene la estabilidad y seguridad del sistema operativo al restringir el acceso directo de las aplicaciones del usuario a los componentes críticos del sistema.

En el contexto del incidente de CrowdStrike, este problema ocurre en un nivel más profundo de esta estructura (posiblemente en el anillo 0 o 1), lo que explica por qué tuvo un impacto tan severo en todo el sistema operativo.

En el lado derecho se muestra un diagrama que ilustra los diferentes tipos de impacto que puede tener un ciberincidente. Este diagrama proporciona una visión integral de cómo un incidente puede afectar diferentes aspectos del sistema.

Está organizado en cuatro cuadrantes alrededor de un círculo central denominado "INCIDENTE". Estos cuadrantes representan diferentes tipos de impactos que pueden resultar de un incidente cibernético.

Contiene unos ejes que representan los aspectos clave de la gestión de incidentes cibernéticos.

Implicaciones para la gestión de riesgos:

Este modelo sugiere que los incidentes cibernéticos pueden tener una variedad de efectos, desde localizados y predecibles hasta sistémicos y ocultos. La gestión efectiva del riesgo cibernético debe considerar y prepararse para todos estos tipos de efectos.

Equilibrio entre factores:

El diagrama implica la necesidad de equilibrar la contención y la resiliencia, así como la continuidad y el aislamiento en la respuesta a incidentes cibernéticos.