MY JAVIER HIDALGO REALPE
MY LAGOS ASCANIO LEONARDO ARTURO
CC PABLO ANDRES MORENO RODRIGUEZ
CC EDGAR E. ZAMBRANO GONZALEZ
MAECI 2024

El Gran Apagón de Microsoft: Cómo un error de software en crowdStrike paralizó el mundo tecnológico

Como alumnos de la maestría de Ciberseguridad y Ciberdefensa se hace necesario analizar el evento informático que se presentó en julio de 2024, donde un grave incidente afectó al mundo de la tecnología, causando grandes problemas en varios servicios importantes. Este incidente fue causado por una actualización defectuosa del software de seguridad Falcon de CrowdStrike, que impactó a alrededor de 8.5 millones de dispositivos Windows. Por lo que analizaremos en términos sencillos qué causó el problema, cómo se desarrollaron los eventos, un análisis de la situación, lecciones aprendidas y las acciones tomadas para solucionarlo.

Causas del Incidente

El problema comenzó con una actualización del software Falcon Sensor de CrowdStrike, que es usado para proteger dispositivos contra malware y otros ataques cibernéticos. Esta actualización tenía un error importante que no fue detectado antes de ser enviada a los usuarios. Este error causó que muchos dispositivos Windows dejaran de funcionar correctamente, mostrando la "Pantalla Azul de la Muerte" (BSOD), un error crítico del sistema operativo (CrowdStrike, 2024; Weston, 2024).

Cronología del Incidente

1. 18 de julio de 2024: CrowdStrike lanzó una actualización de su software Falcon Sensor. Poco después, usuarios de dispositivos Windows comenzaron a reportar problemas graves, como la Pantalla Azul de la Muerte y la imposibilidad de iniciar sesión en sus sistemas.

2. 19 de julio de 2024: Los problemas se extendieron rápidamente, afectando a muchos sectores importantes. Estaciones de televisión, aerolíneas y servicios hospitalarios estuvieron entre los más afectados, causando cancelaciones de vuelos y citas médicas (Griffin, 2024).

3. 20 de julio de 2024: Microsoft empezó a trabajar de cerca con CrowdStrike para encontrar la causa del problema y desarrollar una solución. Se enviaron cientos de ingenieros de Microsoft para ayudar directamente a los clientes afectados, proporcionando soporte técnico y orientación para arreglar los sistemas (Weston, 2024).

4. 25 de julio de 2024: CrowdStrike explicó públicamente que el problema se debió a un fallo en su sistema de control de calidad, lo que permitió que la actualización defectuosa fuera aprobada y enviada a los usuarios. Anunciaron nuevas medidas para evitar que errores similares ocurran en el futuro (CrowdStrike, 2024; Griffin, 2024).

Análisis del Incidente

El análisis del incidente mostró varias áreas importantes que necesitan mejorar en la gestión de actualizaciones de software y los procesos de control de calidad:

1. Control de Calidad Insuficiente: El fallo en el sistema de control de calidad de CrowdStrike permitió que la actualización defectuosa se distribuyera a los usuarios. Este error resalta la necesidad de tener mecanismos de control más fuertes y redundantes para detectar y prevenir errores antes de que lleguen a los clientes (CrowdStrike, 2024).

2. Interdependencia Tecnológica: El incidente mostró cómo los sistemas tecnológicos están interconectados. La dependencia de muchos servicios importantes en una sola solución de seguridad amplificó el impacto del error, demostrando cómo un fallo en un componente puede causar grandes interrupciones (Weston, 2024).

3. Respuesta a Incidentes: La rápida y coordinada respuesta de Microsoft y CrowdStrike ayudó a mitigar los efectos del incidente. La colaboración con otros proveedores de servicios en la nube, como Google Cloud Platform (GCP) y Amazon Web Services (AWS), también

fue crucial para compartir información y desarrollar soluciones efectivas (Weston, 2024; Griffin, 2024).

Lecciones Aprendidas

1. Mejorar los Procesos de Control de Calidad: CrowdStrike implementó nuevas verificaciones en su proceso de control de calidad para prevenir errores similares en el futuro. Estas medidas incluyen pruebas adicionales y validaciones antes de lanzar actualizaciones (CrowdStrike, 2024).

2. Colaboración y Comunicación Eficiente: La importancia de la colaboración y la comunicación entre los proveedores de servicios y los clientes fue evidente durante la respuesta al incidente. Microsoft y CrowdStrike mantuvieron una comunicación constante con los clientes afectados, proporcionando actualizaciones regulares y soporte técnico (Weston, 2024).

3. Preparación y Resiliencia: Las organizaciones deben desarrollar planes de contingencia sólidos y mejorar su capacidad para enfrentar incidentes tecnológicos. Esto incluye realizar simulacros regulares de respuesta a incidentes y tener soluciones de respaldo para minimizar el impacto de futuras interrupciones (Griffin, 2024; Weston, 2024).

Acciones de Remediación

1. Soluciones Temporales y Permanentes: CrowdStrike recomendó soluciones temporales para mitigar los efectos inmediatos del error y trabajó en una solución permanente para corregir la actualización defectuosa. Microsoft también envió ingenieros para ayudar a los clientes a implementar estas soluciones y restaurar los servicios (Weston, 2024).

2. Revisión y Mejora de los Procesos Internos: CrowdStrike revisó y mejoró sus procesos internos de desarrollo y control de calidad para asegurarse de que se detecten y corrijan errores similares antes de llegar a los clientes. Esto incluyó agregar nuevas capas de validación y pruebas automatizadas más exhaustivas (CrowdStrike, 2024).

3. Colaboración Continua con Proveedores de Nube: La colaboración continua con otros proveedores de servicios en la nube fue esencial para desarrollar soluciones efectivas y compartir información sobre el estado del impacto. Esta colaboración también ayudó a acelerar el proceso de remediación y reducir el tiempo de inactividad para los clientes afectados (Weston, 2024).

Para concluir, la respuesta rápida y coordinada de Microsoft y CrowdStrike fue crucial para mitigar los efectos del incidente. La colaboración con otros proveedores de servicios en la nube, como Google Cloud Platform y Amazon Web Services, también fue esencial para desarrollar soluciones efectivas y restaurar los sistemas afectados rápidamente. Esta cooperación subraya la importancia de la colaboración en el ecosistema tecnológico para abordar y resolver problemas complejos de manera eficiente.

Las lecciones aprendidas incluyen la necesidad de mejorar los procesos de control de calidad para prevenir futuros errores similares, la importancia de la comunicación y colaboración eficiente entre proveedores de servicios y clientes, y la necesidad de planes de contingencia sólidos para mejorar la resiliencia ante incidentes tecnológicos. CrowdStrike ha implementado nuevas verificaciones y auditorías en sus procesos internos para asegurar que los errores se detecten y corrijan antes de llegar a los usuarios finales. Microsoft, por su parte, ha reforzado sus mecanismos de soporte técnico y comunicación para responder de manera más efectiva a incidentes similares en el futuro.

Referencias bibliográficas.

CrowdStrike. (2024, July 25). CrowdStrike reveals how IT outage that led to global chaos happened. The Independent. Recuperado de https://www.independent.co.uk

Griffin, A. (2024, July 25). CrowdStrike reveals how huge Microsoft outage that led to global chaos actually happened. The Independent. Recuperado de https://www.independent.co.uk

Weston, D. (2024, July 20). Helping our customers through the CrowdStrike outage. The Official Microsoft Blog. Recuperado de https://blogs.microsoft.com

Microsoft. (2024, July 19). Managing the CrowdStrike outage. Microsoft Tech Community. Recuperado de https://techcommunity.microsoft.com

Homeland Security Committee. (2024, July 26). Inquiry into CrowdStrike incident. U.S. House of Representatives. Recuperado de https://homeland.house.gov

AWS. (2024, July 21). Collaborative efforts during the CrowdStrike outage. AWS Security Blog. Recuperado de https://aws.amazon.com

Google Cloud Platform. (2024, July 22). Supporting customers during the CrowdStrike incident. Google Cloud Blog. Recuperado de https://cloud.google.com/blog