Informe Fallo global en Microsoft

INDICE

Introducción

En julio de 2024, una actualización defectuosa del software Falcon Sensor de CrowdStrike, utilizado por Microsoft, provocó una falla global que afectó a millones de dispositivos Windows, causando interrupciones masivas en empresas y organismos gubernamentales. Se estimó que las pérdidas financieras podrían superar los 15,000 millones de dólares.

¿Qué ocurrió y cuándo?

El problema surgió específicamente por una actualización defectuosa del Falcon de CrowdStrike, que es el software encargado de proteger los sistemas de Microsoft. Esta actualización introdujo errores en los controladores del sistema, lo que provocó inestabilidad en los sistemas operativos Windows y en la plataforma Azure. Como consecuencia de esta falla, muchos dispositivos comenzaron a experimentar la "pantalla azul de la muerte", un error crítico que indica que el sistema no puede recuperarse de un fallo grave. Este tipo de error es habitual cuando hay problemas con los controladores de hardware, software o el sistema en general, y resultó en la desconexión de millones de dispositivos.

¿Cuáles fueron las causas principales del fallo?

Actualización defectuosa del agende Falcon de CrowdStrike causando un inevitable destino interminable de pantalla azul mortal.

¿Qué impacto tuvo (económico, de seguridad, de servicio, etc.)?

Tuvo un gran impacto en todos los sectores alrededor de todo el mundo, afectando tanto a usuarios como a empresas, incluidos aeropuertos causando la caída de los sistemas de gestión de vuelos y de los controladores de vuelo, provocando retrasos y hasta cancelaciones en los vuelos, bancos, causando interrupciones en sus servicios como por ejemplo impidiendo transacciones, organizaciones médicas, sistemas ferroviarios, hoteles, estaciones de televisión, dependencias del gobierno etc.

Con todo esto se calcula que afecto alrededor de 8.5 millones de dispositivos y que causo unas pérdidas de 15.000 millones de dólares a nivel mundial siendo entorno a un 57% a sectores de la salud y bancarios.

Este incidente causo que se aumentaran la vigilancia cibernética y la revisión de medidas de seguridad por parte de empresas e instituciones para prevenir futuros fallos.

¿Cómo se podría haber evitado con herramientas de monitorización adecuadas?

Unas de las herramientas de monitorización adecuadas podrían haber evitado este tipo de fallos al permitir una detección temprana de problemas antes de que afectaran masivamente, unos de las herramientas son como:

- **Pruebas previas a las actualizaciones**: Herramientas que prueban las actualizaciones en un entorno de prueba antes de instalarlas en todos los equipos. Esto ayuda a detectar errores en los controladores antes de que lleguen a los usuarios.
- **Monitoreo en tiempo real**: Sistemas que analizan constantemente el rendimiento del equipo y detectan fallos en los controladores, enviando alertas a los administradores antes de que el problema se vuelva grave.
- **Corrección automática de errores**: Herramientas que identifican problemas de compatibilidad y aplican parches de forma automática para evitar fallos en el sistema.
- **Revisión continua del sistema**: Implementar pruebas periódicas para asegurarse de que el sistema sigue funcionando correctamente después de una actualización.

Con estas medidas, se podrían haber identificado y solucionado los errores antes de que afectaran a los usuarios.

¿Qué herramientas podrían haber ayudado en ese caso?

Sistemas de Respaldo
Mantener sistemas de respaldo que puedan activarse en caso de fallo de los sistemas principales, asegurando continuidad de operaciones críticas.

Backups Automáticos
Programar copias de seguridad automáticas diarias de datos críticos y mantener copias en múltiples ubicaciones físicas y en la nube.

Conclusión

Para concluir esperamos que sirva para aprender, que es totalmente fundamental probar una actualización antes de provocar un colapso global en todos los clientes que se tiene, no solo por las posibles repercusiones económicas y sociales, sino por los

posibles graves problemas que se pueden llegar a tener en sectores delicados como hospitales, aeropuertos, servicios de emergencia, por ejemplo. Es por eso por lo que es importante la preparación y la capacidad de respuestas ante fallos.

Bibliografía

https://www.qualoom.es/analisis-fallo-global-microsoft-crowdstrike/

https://www.infobae.com/tecno/2024/07/20/falla-global-de-microsoft-afecto-a-casi-9-millones-de-dispositivos-windows-en-el-mundo/

https://es.wired.com/articulos/el-apagon-de-microsoft-dejaria-perdidas-a-nivel-mundial-de-al-menos-15000-millones-de-dolares#:~:text=La%20falla%20de%20Microsoft%20que,ejecutivo%20de%20la%20aseguradora%20Parametrix.