NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS – 30 de julio de 2024 **ODF – Funcas 44 / 2024**

Resiliencia digital y vulnerabilidad tecnológica: lecciones del caso CrowdStrike

EL DATO

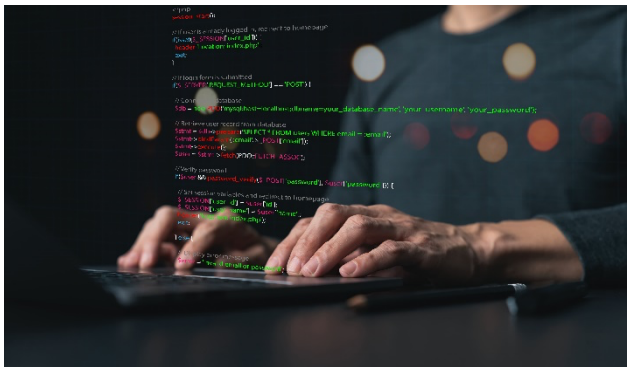
El fallo en la actualización de CrowdStrike afectó a 8,5 millones de dispositivos de todo el mundo[i].

CrowdStrike: una actualización problemática

El viernes 19 de julio, una actualización de software de CrowdStrike causó una interrupción masiva en sistemas Windows a escala global. Un fallo en una actualización de configuración de la plataforma Falcon de CrowdStrike provocó errores en 8,5 millones de dispositivos Windows de todo el mundo. La actualización, diseñada para mejorar la protección contra ataques maliciosos, causó un error de lógica que llevó al fallo del sistema operativo. En concreto, los usuarios al acceder a sus dispositivos se encontraron con "pantallas azules de la muerte" (BSOD, por sus siglas en inglés) y con reinicios continuos. CrowdStrike rápidamente identificó y solucionó el problema, asegurando que no fue un ciberataque, y proporcionó instrucciones para la recuperación de los sistemas afectados.

Impacto y consecuencias derivadas del fallo

Aunque, globalmente, el porcentaje de dispositivos afectados fue menor del 1%, el impacto fue considerable. Más de 5.000 vuelos fueron cancelados. En todo el mundo, varios centros de llamadas de emergencias y diversos sistemas de transporte público experimentaron problemas operativos. En el ámbito financiero, algunas entidades bancarias reportaron interrupciones en sus servicios debido al incidente. Aunque



es difícil cuantificar el impacto económico, los problemas derivados de este problema tecnológico generaron pérdidas económicas significativas para muchas empresas y usuarios.

Lecciones aprendidas

En un mundo cada vez más digital, el incidente de CrowdStrike ha proporcionado lecciones cruciales para la gestión de la ciberseguridad y la continuidad operativa. Estos problemas tecnológicos subrayan cómo la interconexión de los sistemas puede comprometer toda la economía debido a un fallo en un sistema operativo específico. Este evento ha recordado de una forma abrupta las vulnerabilidades a las que están expuestos nuestros modelos productivos y ha subrayado la importancia de mantener una infraestructura tecnológica robusta y resiliente.

¿Cómo estar preparados?

Este tipo de situaciones debe servir como una oportunidad para mejorar los planes de acción ante posibles fallos futuros. Es fundamental que todas las empresas desarrollen planes de contingencia para diferentes tipos de interrupciones, como ciberataques, fallos tecnológicos y desastres naturales. Además, la creciente sofisticación de las amenazas cibernéticas requiere una inversión continua en tecnologías avanzadas de ciberseguridad. En este aspecto, los bancos pueden contar con una ventaja, ya que tradicionalmente invierten en tecnología fuertemente y significativamente más que la media de otros sectores. La prevención es esencial para estar preparados ante estos eventos, que, aunque poco frecuentes, están volviéndose más probables.

[i] Helping our customers through the CrowdStrike outage. Microsoft. 20 julio 2024. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/