

**BLOG**
OPINIÓN

El incidente CrowdStrike y la vulnerabilidad de la tecnología

JULIO CESAR MIGUEL PEREZ

El pasado 19 de junio todos los informativos se hicieron eco de un incidente a escala mundial que había paralizado más de 8 millones de dispositivos Windows en todo el mundo, provocando el colapso en los sistemas de aerolíneas, hospitales, bancos, cadenas de supermercados y un largo etcétera de sectores a los que un fallo en la actualización del producto Falcon de CrowdStrike estaba afectando de forma dramática, originando la aparición de la conocida «pantalla

azul de la muerte», que impedía encender el equipo para poder utilizarlo.

El problema se originó en una actualización del software antivirus Falcon de CrowdStrike (uno de los fabricantes más importantes del mundo en el sector de la ciberseguridad). La actualización contenía un error que, al instalarse, provocaba un fallo crítico en el sistema operativo Windows impidiendo utilizarlo. Aunque el remedio para solucionar esto es rápido, hay que aplicarlo

equipo por equipo, no pudiéndose corregir de forma masiva.

Se estima que el fallo afectó a 8,5 millones de dispositivos Windows en todo el mundo, convirtiéndose este incidente en uno de los mayores apagones informáticos de la historia, impactando significativamente en las empresas y usuarios afectados, generando pérdidas económicas, retrasos y frustración.

Además, ha puesto de relieve la necesidad de contar con procesos de control de calidad rigurosos para prevenir este tipo de errores.

Por otro lado, este suceso también ha evidenciado el nivel de dependencia en la tecnología de las organizaciones y la sociedad en general, siendo un recordatorio contundente de las vulnerabilidades inherentes en nuestra infraestructura tecnológica y la importancia crítica de tener planes de continuidad de negocio.

A medida que las amenazas evolucionan, también deben hacerlo nuestras estrategias



de defensa y recuperación. Las organizaciones, independientemente de su tamaño, deben adoptar un enfoque proactivo, no solo para prevenir ataques, sino para garantizar que puedan continuar operando y recuperarse rápidamente de cualquier interrupción. En última

instancia, la resiliencia y la preparación son claves para navegar con éxito por el panorama tecnológico actual.

En un contexto de digitalización masiva y de complejidad tecnológica creciente, es esperable que este tipo de incidentes masivos se den con más frecuencia.

Y tú, querido lector, ¿estás ya preparado para el siguiente incidente?

Julio César Miguel Pérez es experto en ciberseguridad y privacidad, CEO de Grupo CFI y presidente de AETICAL. grupocfi.es.