

Protege tu despacho: Aprende de los errores de Microsoft y CrowdStrike



Cómo las fallas de Microsoft y CrowdStrike afectan a los despachos legales: Lecciones clave en ciberseguridad

El jueves 18 de julio por la noche, millones de usuarios alrededor del mundo comenzaron a reportar dispositivos Windows afectados por la “pantalla azul de la muerte” (BSOD), la cual fue provocada por una actualización defectuosa del antivirus Falcon, vendido y desarrollado por CrowdStrike.

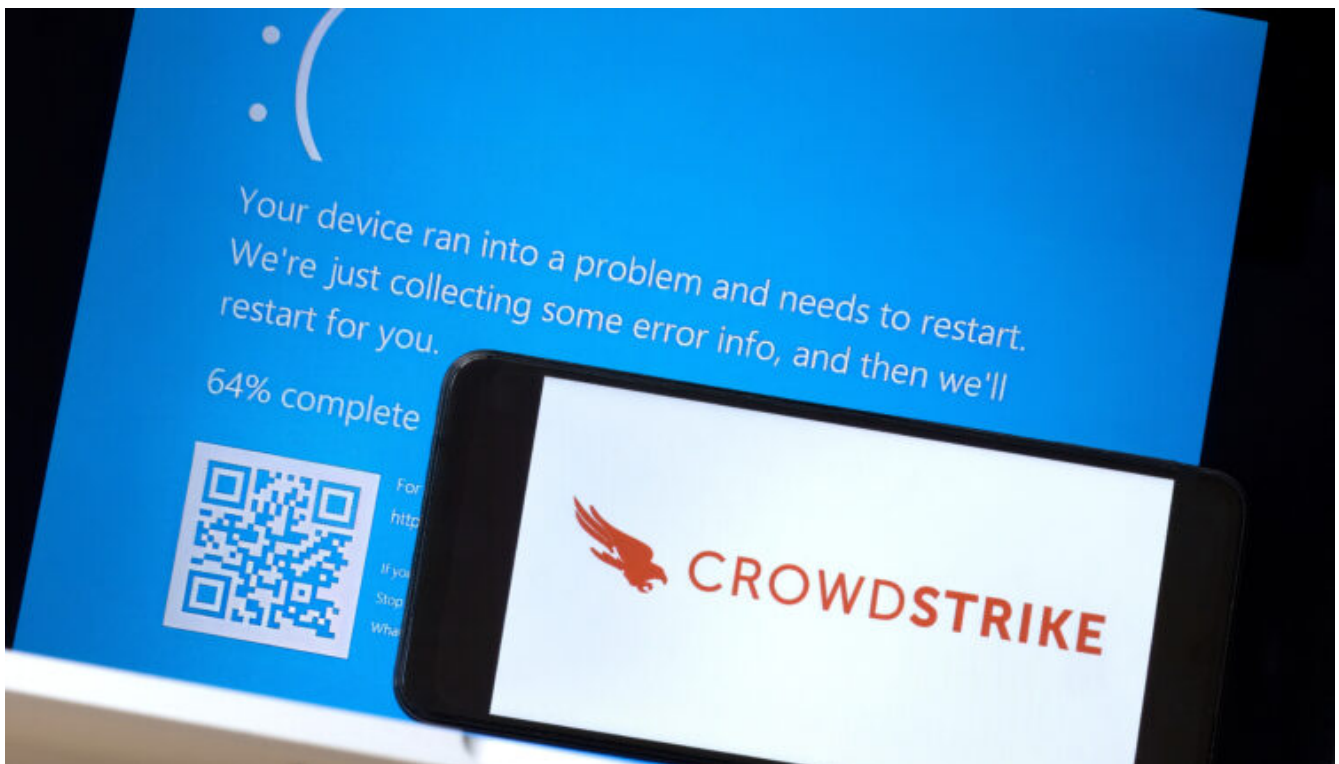
Para los despachos legales, esta es una llamada de atención sobre la importancia de la ciberseguridad. Aquí te cuento cómo estas brechas pueden afectar a tu bufete y qué lecciones podemos aprender.

Lección 1: Protege tus datos como un tesoro

En el mundo legal, los datos de los clientes son oro puro. Los despachos legales manejan información extremadamente sensible: estrategias legales, documentos confidenciales, y más. Las fallas de Microsoft y CrowdStrike nos enseñan que debemos

proteger estos datos a toda costa. ¿Cómo? Implementa medidas como la encriptación de la información, usa contraseñas seguras y limita el acceso solo a quien realmente lo necesita.

No toda la información tiene la misma importancia, y por eso, es clave establecer fronteras de seguridad. Clasifica los datos según su sensibilidad y aplica diferentes niveles de protección. Esto permite enfocar recursos en proteger lo más crítico.



60% de los pequeños despachos

Según el informe de ciberseguridad de Cisco 2022, el 60% de las pequeñas empresas, incluyendo despachos legales, que sufren un ciberataque cierran sus puertas en los seis meses siguientes.

Lección 2: Capacitación en ciberseguridad es esencial

El error humano es uno de los puntos más débiles en la seguridad de cualquier empresa. Según un informe de Verizon, el 85% de las brechas de seguridad involucran algún tipo de error

humano. Por eso, capacitar a tu equipo en prácticas de ciberseguridad, como identificar correos electrónicos sospechosos y manejar la información de manera segura, es fundamental.

Lección 3: Prepárate para responder rápido

Tener un plan de acción listo para cuando ocurra un incidente de seguridad es clave. Según el Instituto Ponemon, las empresas que cuentan con un plan de respuesta bien estructurado pueden reducir el costo de una brecha de datos en un 50%. Así que, asegúrate de tener un plan claro y equipos preparados para actuar de inmediato si se produce una violación de seguridad.

¿Tu despacho está listo para enfrentar una brecha de seguridad?

Esta pregunta es esencial para cualquier bufete de abogados. Realiza auditorías de seguridad regularmente y mantén tus sistemas y protocolos de seguridad actualizados para proteger la información legal.

Posts en Tendencia