18/10/2026

El error humano se consolida como la mayor amenaza para la ciberseguridad

Más de dos tercios de los profesionales de TI y seguridad consideran que los errores cometidos por los usuarios representan hoy el principal riesgo para sus organizaciones, por delante incluso de amenazas específicas como el correo electrónico malicioso.

Kaseya ha presentado su informe Cybersecurity Report: Building Security That Survives Human Error, un estudio que analiza los obstáculos que siguen dificultando la construcción de entornos realmente seguros. La principal conclusión es que el error humano continúa siendo la amenaza de ciberseguridad más preocupante para las organizaciones. El 68% de los encuestados identifica factores como la distracción, la ingeniería social o las malas decisiones de los usuarios como el principal vector de riesgo para los próximos doce meses. El correo electrónico aparece en segunda posición, citado por el 55% de los participantes.

Además, entre las empresas que han sufrido algún incidente de seguridad durante los últimos tres años, cuatro de los cinco factores más determinantes estuvieron relacionados con las personas. Entre ellos destacan las malas prácticas de los usuarios o su vulnerabilidad frente al engaño, señaladas por el 41% de los encuestados, y la falta de formación en ciberseguridad, mencionada por el 40%.

Según David Baggett, vicepresidente senior y director general del área de seguridad de Kaseya, “el problema radica en que gran parte de la estrategia de ciberseguridad sigue confiando en que los usuarios tomen siempre la decisión correcta”. El directivo defiende que la verdadera resiliencia no consiste en eliminar los errores, sino en diseñar organizaciones capaces de resistirlos.

La confianza en el cumplimiento normativo no siempre refleja la realidad

El informe también pone en cuestión la percepción que muchas organizaciones tienen sobre su preparación regulatoria. Aunque cerca del 65% afirma que podría superar una auditoría de cumplimiento sin necesidad de preparación previa, casi la mitad reconoce que la documentación y las políticas incompletas podrían generar problemas durante una inspección.

Concretamente, el 49% identifica la falta de documentación adecuada como el principal obstáculo para superar una auditoría, mientras que el 34% menciona controles de seguridad implantados de forma incompleta. Otro 33% considera que la escasa concienciación o formación de los empleados representa un riesgo significativo para el cumplimiento normativo.

Estos resultados reflejan una diferencia relevante entre la confianza declarada por las organizaciones y el estado real de algunos de sus procesos de seguridad y gobernanza.

Otro de los hallazgos más destacados del estudio es la creciente brecha entre el nivel de riesgo y los recursos asignados para combatirlo. Solo el 20% de los departamentos de TI considera que su presupuesto de ciberseguridad está aumentando al mismo ritmo que evolucionan las amenazas.

En paralelo, el 77% de las organizaciones afirma sufrir algún tipo de limitación de recursos. Un 23% señala que su presupuesto permanece estancado mientras aumentan los riesgos, el 30% reconoce que las inversiones crecen demasiado lentamente y el 24% admite estar claramente infradotado en materia de seguridad.

La situación también afecta a los clientes de los proveedores de servicios gestionados. El 65% de los MSP encuestados considera que sus clientes están invirtiendo menos en ciberseguridad de lo que realmente exige su nivel de exposición al riesgo.

A partir de las conclusiones del estudio, Kaseya propone un enfoque basado en cinco principios para reforzar la resiliencia frente a amenazas y errores humanos. La compañía recomienda diseñar procesos teniendo en cuenta que los fallos ocurrirán, justificar las inversiones antes de que se produzca un incidente grave, eliminar fricciones para que las conductas seguras sean las más sencillas de adoptar, aprovechar la inteligencia artificial para ampliar las capacidades de equipos limitados y tratar el cumplimiento normativo como una actividad continua.

Fuente: El error humano se consolida como la mayor amenaza para la ciberseguridad | Seguridad | IT User