

La sobrecarga tecnológica compromete la ciberseguridad empresarial en España

El 67% de las organizaciones sufrió al menos una brecha de seguridad en el último año. La media de 75 herramientas de ciberseguridad por empresa ha generado un ecosistema complejo y difícil de gestionar, una saturación tecnológica que reduce la eficacia o

Las empresas españolas destinan cada vez más recursos a soluciones de ciberseguridad, pero esta inversión no siempre se traduce en una mayor protección. La digitalización avanza más rápido que la capacidad humana para gestionarla, y la proliferación de tecnologías y servicios está generando una “sobrecarga tecnológica” que añade complejidad operativa y dificulta la coordinación entre sistemas.

El State of Pentesting Report 2025 confirma que el 67% de las organizaciones sufrió al menos una brecha de seguridad en los últimos 24 meses, incluso contando con múltiples soluciones de protección. De hecho, las compañías utilizan una media de 75 herramientas de seguridad, y el 45% ha incrementado ese número en el último año. El 59% reconoce que sus proveedores les han exigido incorporar nuevas defensas, lo que ha derivado en un ecosistema cada vez más fragmentado.

La complejidad como nuevo vector de riesgo

La expansión del teletrabajo, los modelos híbridos y el uso de dispositivos personales (BYOD) han ampliado la superficie de ataque. A ello se suma la introducción acelerada de soluciones impulsadas por inteligencia artificial, que sin una estrategia ordenada pueden provocar pérdida de visibilidad, duplicidades y configuraciones inconsistentes.

Josep Albors, director de Investigación y Concienciación de ESET España, advierte que “no se trata de tener más herramientas, sino de disponer de las adecuadas y gestionarlas de forma coordinada. La sobrecarga tecnológica provoca ceguera operativa, ralentiza la respuesta y aumenta el riesgo de que un error humano desencadene una brecha”.

La falta de perfiles especializados agrava la situación. Estudios de Deloitte y Forrester señalan un aumento del agotamiento del talento en ciberseguridad, impulsado por la presión operativa, el volumen de alertas y la dificultad para gestionar entornos fragmentados. Cuando los equipos dedican más tiempo a mantener herramientas que a prevenir ataques, la seguridad se vuelve frágil por definición.

La saturación de soluciones no solo complica la prevención, sino que ralentiza la identificación y contención de incidentes. Los equipos de seguridad reconocen dificultades para priorizar vulnerabilidades críticas, mantener configuraciones coherentes y responder de forma coordinada ante un ataque real. Según ESET, esta pérdida de eficacia operativa puede traducirse en brechas más costosas, fallos en la continuidad del negocio y un incremento del riesgo reputacional.

ESET propone medidas para racionalizar el ecosistema tecnológico y mejorar la resiliencia organizativa, entre ellas consolidar herramientas y eliminar duplicidades, evaluar la necesidad real antes de adoptar nuevas soluciones, y fortalecer la arquitectura base con segmentación, control de accesos y MFA, además de formar a los equipos para reducir el impacto del error humano.

“Reducir la complejidad y mejorar la visibilidad es esencial para mantener la seguridad y evitar que la tecnología, paradójicamente, se convierta en una vulnerabilidad más”, concluye Albors.

Fuente: https://www.ituser.es/

LINK DE LA NOTICIA