Persiste la baja preparación de las empresas españolas en ciberseguridad

Es una de las conclusiones del informe Cisco Cibersecurity Readiness Index 2025. Sólo un 2% de las organizaciones tienen un nivel maduro, cifra que preocupa en plena era de la IA y los riesgos que esta tecnología traerá consigo

Complejidad en la era de la IA

Nuevos y viejos retos

Comparación con otros mercados

Fuente: https://www.redestelecom.es/

LINK DE LA NOTICIA

Analizando estos resultados en comparación con otras economías, el informe constata que el nivel de preparación en ciberseguridad en nuestro país sigue siendo bajo. De los cuatro niveles de madurez que establece (principiante, formativo, progresivo y maduro), en España algunas compañías han pasado de incipiente a formativo y nos situamos en un 82% en una escala baja, frente al 70% global. Nuestro principal hándicap, las pymes. En estas pequeñas y medianas organizaciones “falta personal, no hay figura de CISO y resulta muy difícil estar al día de los ataques. Por eso, hay camino por recorrer en cuanto a desarrollar servicios gestionados que les permitan a esas empresas tener ese conocimiento”, matiza.

Y para rizar el rizo un dato que llama la atención: “el frenazo en la inversión en seguridad de las organizaciones”. Aunqueel 97% de las organizaciones españolas planean actualizar su infraestructura de TI, sólo el 28% destinan más del 10% de su presupuesto de TI a la ciberseguridad (45% a escala global). Entre los motivos que puedan explicar este hecho, el directivo alude al boom de inversión en ciberseguridad que hemos vivido hace años y la tendencia de muchas empresas a pensar que como ya se ha invertido, ya están protegidos. “Pero hay que mantener esa tensión, hay que seguir pedaleando en cuanto a inversiones en seguridad”, ha matizado Ortiz. Una segunda razón sería la tendencia hacia la “plataformización” del mercado. Muchos clientes han destinado presupuesto en base a amenazas que han ido surgiendo, pero ahora buscan algo más coherente y a largo plazo que le permita facilitar la gestión… eso supone parar la inversión y mirar dónde estamos para decidir. De ahí ir hacia una aproximación de plataforma y gobernanza. No obstante, “ir a una solución cien por cien del fabricante no es viable. El camino hacia plataformas abiertas es el futuro”, sentencia el ejecutivo de Cisco.

Al igual que la escasez de talento. El 74% de las empresas españolas indican como un desafío crucial la falta de profesionales

de ciberseguridad y casi la mitad (el 45%) tienen puestos vacantes por cubrir.

También prosigue la complejidad de la infraestructura de defensa en tanto en cuanto el 57% utilizan diez o más soluciones puntuales en su stack de seguridad, y el 10% utilizan treinta o más. En este contexto, el 73% de los participantes creen que la adopción de demasiadas soluciones de seguridad ralentiza la capacidad para detectar, responder y recuperarse de incidentes.

Pero mientras la IA va cobrando forma como nueva fuente de cibercrimen, los retos de seguridad que podríamos considerar "tradicionales" se mantienen. Así, el 87% de los consultados afirman que sus empleados acceden a la red corporativa desde dispositivos no gestionados y un 20% de estos trabajadores pasan un 20% o más conectados a las redes desde esos dispositivos. A ello hay que añadir que el 22% usan de media seis redes distintas por semana para trabajar (Wi-Fi, banda ancha…).

La otra cara de la moneda es de la IA es su empleo como herramienta de ciberseguridad. En este sentido, el 84% de las organizaciones españolas ya la utilizan para comprender y responder mejor a las amenazas: el 81% para su detección y el 67% para tareas de respuesta y recuperación.

¿Esto qué supone? Pues no conocer qué datos están usando los empleados, no saber que se puede manipular el modelo de IA con el que se trabaja y otras tantas amenazas implícitas… Y es que, como ha señalado Ángel Ortiz, "hay que tomar la IA como un nuevo vector de ataque porque su llegada supone una revolución que va a cambiar el paradigma de la seguridad como se entendía hasta ahora".

Sin embargo, los peligros están ahí y más conociendo que el 20% de las organizaciones reconoce que acceden sin restricciones a las aplicaciones de IAGen de uso público y que el 65% desconoce el uso de esas plataformas. Y aunque el 55% utilizan aplicaciones de terceros aprobadas internamente y ponen ciertos controles de uso, sólo el 16% obligan a sus usuarios a utilizar la IA generativa interna como alternativa a las herramientas públicas.

Durante su intervención, el directivo ha aludido a la poca conciencia que existe en las empresas españolas de los peligros que implica la IA. No en vano, según el estudio, el 83% de las organizaciones españolas reconoce haber sufrido un incidente asociado con IA en el último año; el 34% afirma tener recursos internos y la experiencia para realizar evaluaciones integrales de seguridad de la IA; y tan sólo el 8% identifica la IA como el pilar más difícil de proteger. Es más, el 44% de las empresas consultadas en España confían en que sus empleados comprendan plenamente las amenazas relacionadas con la IA, mientras que únicamente el 42% consideran que sus equipos saben realmente cómo los ciber-delincuentes utilizan la IA para ejecutar ataques sofisticados.

Estas son las **tres principales conclusiones** extraídas del informe anual **Cisco Cibersecurity Readiness Index 2025**, realizado en una treintena de países y cuyos resultados ha presentado en rueda de prensa **Ángel Ortiz**, director de Ciberseguridad en Cisco España.

El nivel de **preparación de las empresas españolas en materia de ciberseguridad** sigue siendo bajo. Algo preocupante en plena **era de la IA** por los riesgos que esta tecnología incorpora a la seguridad de las organizaciones. De hecho, las compañías siguen enfrentándose a las complejidades que introduce esta innovación, sobre todo el despliegue de la **inteligencia artificial generativa**. A ello se suman otros retos más tradicionales, pero que continúan vigentes, como el **empleo de dispositivos no gestionados para acceder a la red corporativa**.