22/12/2025

Los ciberataques salen cada vez más caros a las pymes: en los últimos años, su coste ha aumentado un 25%

En los últimos años, los ciberataques a las pymes no sólo han aumentado, también salen más caros. El coste económico de estos incidentes ha aumentado un 25%.

La ciberseguridad se ha convertido en uno de los principales desafíos digitales para las empresas a nivel mundial. En el año 2024, se gestionaron 97.348 incidentes, un 16,6% más que en 2023, según los últimos datos del Instituto Nacional de Ciberseguridad (Incibe).

De estos incidentes, más de 31.500 afectaron a empresas, cifra en las que se incluye a miles de pymes españolas. Los ciberataques a estas organizaciones no sólo siguen siendo frecuentes, si no que cada vez son más caros.

De hecho, según un informe de la compañía Secure&IT, el coste económico de recuperarse de un ciberataque para las pymes ha aumentado un 25% en los últimos años.

Según explicó Francisco Valencia, director general de Secure&IT, "el incremento del coste de un ciberataque se ha acelerado en los últimos años debido a la mayor complejidad técnica de los ataques, la dependencia digital del negocio y las crecientes exigencias regulatorias que afectan a cualquier empresa, independientemente de su tamaño".

¿Por qué los ciberataques suponen un coste cada vez mayor para las empresas?

El incremento del coste de un ciberataque responde a varios factores acumulados. Por un lado, la mayor sofisticación de los ataques, que combinan ingeniería social, secuestro de equipos, robo de credenciales y exfiltración de datos. Por otro, la dependencia digital, cualquier interrupción impacta en procesos esenciales como ventas, facturación, atención al cliente o cadena de suministro.

A esto se suman las nuevas obligaciones regulatorias como NIS2, DORA, ENS o CRA, que exigen notificar incidentes, demostrar diligencia y mantener medidas de seguridad adecuadas.

En este contexto, el director general de Secure&IT dio algunas claves para entender la magnitud del problema: "si analizamos la evolución de los últimos años, los principales estudios internacionales muestran que el coste medio de un incidente ha aumentado desde 2020, superando ya el 25 % de incremento a nivel global. Actualmente, recuperarse de un ataque es mucho más caro que hace 5 años porque, aunque la empresa no haya crecido, los ataques son más complejos y exigen más trabajo técnico, legal y organizativo".

Todo ello sitúa a las pymes en una posición de especial fragilidad, ya que la mayoría reconoce que no cuenta con un plan formal de respuesta a incidentes, según estudios europeos.

Así, la mayor parte de estas pequeñas y medianas empresas dependen de una única copia de seguridad (backup) o carecen de visibilidad sobre los accesos y dispositivos conectados a su red. La falta de prácticas básicas como copias de seguridad, autenticación robusta, monitorización continua o revisiones periódicas de proveedores, sigue siendo uno de los principales puntos débiles.

“La pyme sigue siendo uno de los objetivos prioritarios del cibercrimen, no por su tamaño, sino por su exposición.

El fraude digital, el principal problema de las pequeñas empresas

El 89 % de los ciberdelitos registrados en España son fraudes informáticos, y muchos de ellos están dirigidos a empresas, según el último Informe de Cibercriminalidad del Ministerio del Interior. Así, el fraude digital se ha convertido en uno de los principales problemas de los ciberataques que ocurren en nuestro país.

Según explicó Francisco Valera, "el incremento de la sofisticación de los ataques y la presión regulatoria han elevado el impacto real de los incidentes, especialmente en sectores que dependen de sistemas críticos para su actividad diaria. La combinación de estos factores está haciendo que estos ataques sean más efectivos, costosos y disruptivos para las organizaciones".

Este aumento de la gravedad delictiva golpea con fuerza a las pymes, que representan más del 99 % del tejido productivo español y cuya capacidad operativa depende cada vez más de sistemas digitales.

“La pyme española está más informatizada que nunca, pero también es más vulnerable”, advirtieron desde Secure&IT. “Una parada del ERP, un fraude por suplantación, un ataque de ransomware o la caída de un servicio, puede suponer días sin facturar, pérdida de clientes y posibles sanciones. Y ese coste no deja de crecer”, concluyeron los expertos.

Fuente: https://www.autonomosyemprendedor.es/

LINK DE L A NOTICIA