CincoDías

Publicación	Cinco Días General, 15	Fecha	12/12/2022
Soporte	Prensa Escrita	País	España
Circulación	30 782	V. Comunicación	19 718 EUR (20,795 USD)
Difusión	21 772	Tamaño	389,56 cm² (62,5%)
Audiencia	44 000	V.Publicitario	9560 EUR (10 083 USD)

Retos de ciberseguridad que habrá que enfrentar en 2023

Protegerse de un ciberataque se ha convertido ya en una necesidad para las pymes y los autónomos

NEREA MERINO SACRISTÁN
MADRID

Las pymes y los autónomos son un blanco fácil para los ciberdelincuentes. La ciberseguridad continúa siendo una asignatura pendiente. Muchos negocios no perciben el riesgo y otros no cuentan con los conocimientos y con el presupuesto suficiente para hacer frente a los ciberataques.

Según un estudio realizado por IDC (International Data Corporation) Research España, los ciberataques en 2021 afectaron al 90% de las empresas y se prevé que este año las cifras hayan aumentado. En IDC estiman que 2022 cerrará con una inversión media del 7,7% en ciberseguridad por parte de las empresas, es decir, más de 1.700 millones de euros.

La ciberdelincuencia continuará creciendo en los próximos años. Nos encontramos en un mundo cada vez más abierto y digitalizado donde el robo de datos resulta más sencillo para los ciberdelincuentes. Aunque muchas empresas aún no son conscientes del riesgo. Datos del estudio *La ciberseguridad en 2022 y el efecto pospandemia en las pymes españolas*, realizado por Google en colaboración con The Cocktail Analysis, revelan que las pymes y los autónomos se han relajado tras la crisis sanitaria. Muchos consideraban que la causa era el teletrabajo. Al disminuir este modelo de trabajo hace creer que los riesgos ya no existen, pero están equivocados.

Desafíos

Para mejorar la ciberseguridad hay que conocer los principales desafíos. A causa del Día Mundial de la Seguridad en la Información, que tuvo lugar el pasado miércoles 30 de noviembre, Innovery, una multinacional que ofrece soluciones TIC, ha explicado los retos a los que se han de enfrentar las empresas en 2023.

►La procedencia de alrededor del 85% de los ciberataques es el error humano. Por este motivo, desde Innovery indican que la clave para superar este riesgo es concienciar y formar a los empleados en materia de seguridad. Todos los miembros de la empresa deben tener un mínimo conocimiento para poder llevar a cabo las medidas básicas de ciberseguridad. Por ejemplo, actualizar las contraseñas con cierta periodicidad, no entrar en webs que no sean seguras, etc.

►Cualquiera puede ser víctima. Se tiende a pensar que son las grandes empresas las únicas que pueden ser atacadas, pero nada más lejos de la realidad. Cualquiera, también las pymes, puede ser atacado. Hay que tener en cuenta que los ciberdelincuentes son conscientes de que, a menor tamaño, las probabilidades de no tener políticas de seguridad son más altas y, por tanto, más fáciles de atacar. Además, son las firmas que forman la mayor parte del tejido empresarial español, por lo que salvaguardar su seguridad es importante. Por ello, independientemente del tamaño, todas deben invertir en ciberseguridad.

►Las copias de seguridad, conocidas como soluciones *backup*, son uno de los mejores remedios para evitar problemas. Poder recuperar todos los datos ante una brecha de seguridad es imprescindible para todas las empresas. Además, en la mayoría de los ataques es la última línea a la que se enfrentan los atacantes. Por tanto, invertir en copias de seguridad y contar con personal dedicado a ello es una de las claves en materia de ciberseguridad.

►Saber gestionar todos los aspectos relacionados con la ciberseguridad. El tejido empresarial y la sociedad española se encuentran en un momento de incertidumbre económica y en un mundo globalizado donde la transformación digital es casi obligatoria para sobrevivir. Invertir en tecnología para ser competitivo es importante, pero más lo es saber gestionar y trabajar con esa tecnología. Saber utilizar los recursos es uno de los desafíos más importantes.

►Contratar expertos en ciberseguridad. En primer lugar, y en línea con el punto anterior, las empresas deben contratar a personas que tengan conocimientos tecnológicos o proporcionarles la formación correspondiente. Y también han de ser conscientes de la importancia de tener expertos en materia de seguridad. Este es uno de los grandes retos debido a que faltan profesionales de esta materia, ya que la demanda es muy alta. Como señalan desde el Instituto Nacional de Ciberseguridad de España (Incibe) y el Observatorio Nacional de Tecnología y Seguridad (Ontsi), el país necesita más de 80.000 expertos en ciberseguridad para llegar a cubrir la demanda actual.

Inversiones

De esta manera queda reflejado que toda empresa, grande o pequeña, debe invertir en ciberseguridad. Para ello, es necesaria una inversión económica, tecnológica y, por supuesto, humana. De no hacerlo, el funcionamiento de la compañía puede peligrar y, en consecuencia a su forma de actuar, también su reputación.

La tecnología ha venido para quedarse y los ciberdelincuentes son conscientes de ello. Por tal motivo, cada vez tienen más capacidad y conocimientos para atacar a las empresas. Sobre todo, con la actual modalidad de ataque, el *ransomware*. Un software malicioso que cifra los datos de una empresa a cambio de un rescate económico. La única solución para acabar con ellos y con cualquier tipo de ciberataque es que todas las compañías inviertan en ciberseguridad. Se ha convertido en una necesidad para todas las empresas y para los autónomos.

Otras claves

► Los autónomos dedicados a la venta ambulante mantienen su cotización reducida. Unos 80.000 trabajadores de la venta ambulante conservarán su cotización rebajada gracias al trabajo de la Unión de Profesionales y Trabajadores Autónomos (UPTA). El cambio ha llegado en forma de transacción a los Presupuestos Generales del Estado. Desde la asociación indican que en el proyecto de ley se establecían las bases de cotización; sin embargo, en la propuesta inicial que el Gobierno presentó al Congreso no aparecía ninguna regulación especial para quienes percibieran menos ingresos.

► Qué tecnologías impulsan a las pymes a digitalizarse. Las tecnologías visuales e inmersivas fomentan la digitalización. Así se ha puesto de manifiesto tras el estreno en Madrid del primer laboratorio GAMELabsNET en España, al que se ha sumado otro de Bilbao coordinado por GAIA. Su creación se enmarca dentro del proyecto europeo Interreg Sudoe. Ambos laboratorios están promovidos por el Centro Español de Logística (CEL) y la Confederación Española de Empresas de Tecnologías de la Información, Comunicación y Electrónica (Conectic).