Isoph Negocio Ciberseguro: la apuesta de BOTECH para la protección de las pymes

Los acontecimientos de los últimos años han puesto a las pequeñas y medianas empresas en el foco de las miradas de los ciberdelincuentes. "La falta de recursos, su conocimiento tecnológico limitado y el reducido presupuesto con el que cuentan para defenderse de los ataques" son, para Miguel Ángel Rojo, CEO de BOTECH, las razones que han convertido a las pymes en uno de los principales objetivos de los *hackers*.

Olga Romero

IR A PÁGINA SIGUIENTE

Un goloso objetivo que en Europa representa el 99 % del tejido empresarial, según datos del Ministerio de Industria, Comercio y Turismo, y cuya vulnerabilidad se basa, por un lado, en su baja inversión en ciberseguridad y, por otro lado, en las numerosas obligaciones que recaen sobre los directivos. "Los propietarios de las pequeñas empresas tienen que hacer frente a cuestiones financieras, de producto o de marketing al mismo tiempo. Por ello, añadir la gestión de la ciberseguridad suele parecerles complicado", explica Rojo.

En cuanto al impacto que los ciberataques, causa principal que obliga a cerrar al 57 % de las pymes, pueden ocasionar en este colectivo, el directivo destaca como grandes consecuencias la interrupción del servicio al cliente, el debilitamiento del buen funcionamiento, la pérdida de reputación o el robo de datos, entre otros.

Ante esta situación, el responsable de BOTECH cree que "la concienciación en ciberseguridad es la asignatura pendiente de las pymes". Sin embargo, también recuerda que estas empresas necesitan tener a su disposición unas soluciones que les permitan hacer frente a las ciberamenazas adaptándose a sus presupuestos y conocimientos ya que, como afirma, "las herramientas actuales están orientadas a grandes corporaciones".

Miguel Ángel Rojo, CEO de BOTECH

"Las pymes necesitan más concienciación en ciberseguridad y disponer de herramientas que les permitan defenderse y se adapten a sus presupuestos y conocimientos"

Además, Rojo comenta que, en el escenario actual en el que el teletrabajo ha llegado para quedarse y la información se comparte, en la mayoría de las ocasiones, en diferentes dispositivos, "las herramientas de seguridad deben permitir a las pymes conocer su estado de seguridad, mejorarlo al máximo y mantener

protegida tanto su información como la de sus clientes".

El papel de los empleados en la defensa

Que las nuevas modalidades laborales han derrocado las fortalezas que las empresas levantaron durante años para garantizar la seguridad de sus negocios no es ningún secreto. La desaparición del tradicional perímetro de seguridad se ha convertido en todo un reto para las organizaciones que se esmeran por levantar una nueva muralla, pero esta vez sin un perímetro definido. En este nuevo escenario, los empleados juegan un papel fundamental en la defensa del fortín. Unos empleados a los que las empresas deben proporcionar las armas necesarias: concienciación y formación en ciberseguridad, así como habilidades digitales para el buen uso de las nuevas herramientas de trabajo, para que dejen de ser el eslabón más débil de la cadena de ciberseguridad. Los estudios demuestran que el 80 % de los ataques se producen por fallos humanos por lo que hay que convertirlos en el elemento clave de la defensa.

"Cada vez es más habitual leer sobre los problemas que causan a las empresas los incidentes de ciberseguridad y en este contexto hay que destacar la importancia de los empleados", comenta Rojo, quien añade que "aunque las pymes cada vez son más conscientes de la necesidad de proteger su negocio, aún queda mucho camino por recorrer".

Radiografía de los ciberataques contra las pymes

- **Según el Ministerio de Industria, Comercio y Turismo, el 99 % del tejido empresarial europeo son pymes.**
- **En España, el 44 % de las pymes fue víctima de, al menos, un ciberataque durante 2021, según Hiscox.**
- **El Instituto Nacional de Ciberseguridad (INCIBE) apunta a que cada día se producen unos 40.000 incidentes de ciberseguridad en España. Las pymes, debido a su vulnerabilidad por no contar con buenas infraestructuras digitales, reciben el 70 % de los ataques.**
- **El "Informe de ciberseguridad para las pymes", elaborado por la European Union Agency for Cybersecurity (ENISA), refleja que el 85 % de las pymes reconoce el grave impacto que producirían en sus negocios los problemas de ciberseguridad.**
- **En 2022 los ataques a pymes representaron, según datos de ENISA, el 17 % del total de ciberataques. En 2021 fue del 1 %.**
- **El 57 % de las pymes que se ve obligada a cerrar es por causa de un ciberataque.**
- **Los ciberataques más comunes son el *phishing*, *ransomware* y DNS.**

Isoph Negocio Ciberseguro es una solución que combina tres tecnologías de ciberseguridad: Isoph DNS, Isoph Pyme e Isoph Mobile

Isoph Negocio Ciberseguro: seguridad total

Ofrecer una seguridad total a las pymes con la máxima facilidad y adaptándose a sus ajustados presupuestos y limitados conocimientos es el objetivo de BOTECH. Para ello la compañía, experta en investigación, desarrollo y fabricación de software de ciberseguridad, ha desarrollado Isoph Negocio Ciberseguro. Una solución que combina tres tecnologías de ciberseguridad: Isoph DNS, Isoph Pyme e Isoph Mobile y que la compañía ha lanzado tras dos años de trabajo e investigación que los llevó a presentar su tecnología Isoph Cybersecurity.

"Hemos desarrollado Isoph Negocio Ciberseguro para proteger a las pymes a un coste que puedan asumir y sin necesidad de conocimientos tecnológicos o de ciberseguridad", explica el responsable de BOTECH. Esta solución, la cual pueden descubrir las pymes probándola gratis durante un mes sin compromiso, destaca por su tecnología ágil, flexible y por no requerir conocimientos técnicos.

Sobre la prueba gratuita, Rojo asegura que "la respuesta está siendo muy satisfactoria porque no es necesario incluir datos bancarios ni estar

pendiente para darse de baja antes de que te cobren". Las pymes interesadas únicamente necesitan un correo electrónico para empezar a disfrutar de sus 30 días gratis.

> *"El 80 % de los ciberataques se producen por fallos humanos, por ello los empleados son claves en la estrategia de ciberseguridad"*

Detección + escaneo

"La ciberseguridad 100 % no existe", afirma el directivo. Sin embargo, destaca la importancia de "contar con herramientas que eleven la seguridad corporativa al máximo nivel". En este sentido Isoph Pyme e Isoph DNS, dos de las tecnologías que integran Isoph Negocio Ciberseguro, son capaces de "detectar cualquier vulnerabilidad, página de navegación no segura, *phishing* o problema de seguridad", explica Rojo. Además, gracias al informe semanal que ofrecen a los usuarios, las pymes pueden proteger sus dispositivos, *emails*, navegar de manera segura y formar a sus empleados.

En cuanto a la tercera lanza de este tridente de tecnologías, Isoph Mobile, Rojo comenta que "permite escanear tantas veces como quieras tu dispositivo para conocer su estado de seguridad".

Tres tecnologías que se unen en Isoph Negocio Ciberseguro y que ofrecen a las pequeñas empresas una protección de calidad a un precio asequible y que se adapta a su estructura. "Las pymes no cuentan con elevados presupuestos, pero para ellas es una prioridad disponer de una herramienta que les permita protegerse de fraudes y mantener una buena reputación e imagen con clientes y proveedores", asegura el directivo de BOTECH.

En cuanto al futuro, Rojo lamenta los cada vez más frecuentes incidentes de ciberseguridad y sus graves consecuencias para las compañías. Consecuencias que van desde problemas con la protección de datos o confidencialidad de terceros, pérdidas económicas y de reputación hasta el cierre de la empresa. Por ello el directivo insiste en que "las pymes deben ser conscientes de que una parte de su presupuesto tiene que destinarse a la ciberseguridad". Aspecto que ya no es una opción sino una obligación.

“Trabajamos para que nuestra tecnología evolucione a la par que los ciberataques”

La ciberseguridad 100 % no existe y menos en un escenario en el que la ciberseguridad no deja de evolucionar porque los ataques no dejan de hacerlo. Por ello desde BOTECH trabajan, como asegura Miguel Ángel Rojo, CEO de la compañía, para que su tecnología evolucione al mismo ritmo que los ataques con un claro objetivo: que las compañías dispongan de una herramienta que les permita hacer frente a cualquier incidente de ciberseguridad.

Además, en este vídeo, Rojo recuerda que desde BOTECH buscan ofrecer una seguridad total con la máxima facilidad que se adapte tanto a los presupuestos de las pymes como a su nivel de conocimiento en la materia.

Miguel Ángel Rojo, CEO de BOTECH