Endpoint, datos y SOC, la combinación que conforma el **MDR de Sophos** para proteger a las **pymes**

"En el mercado de la ciberseguridad todos esperábamos mucho más del programa Kit Digital", asegura Carlos Galdón, director de canal de Sophos Iberia. Tal y como explica, la mayoría de las inversiones realizadas por las pequeñas y medianas empresas han sido destinadas a la mejora de las páginas web, por lo que "entendemos que la inversión en ciberseguridad por parte de las pymes ha sido menor de lo que se podía esperar".

Olga Romero

El directivo espera que los resultados mejoren durante 2024, las empresas pueden solicitar estas ayudas hasta diciembre, y asegura que desde el sector deben "seguir exigiendo a la Administración pública una mayor implicación en el desarrollo de los programas de inversión y concienciación para pymes en ciberseguridad porque son la mayor parte de nuestro tejido empresarial".

Una concienciación en la que Galdón insiste ya que, junto con la información, es la única manera de que pymes y autónomos sean conocedores de los peligros que existen en la red, así como de los sistemas de protección de los que disponen los fabricantes para ayudarles a hacerles frente. Asimismo, el directivo recuerda la gran capacidad de adaptación que tienen los ciberdelincuentes y que les permiten "desarrollar técnicas de intrusión que vulneran los constantes desarrollos en ciberdefensa de los fabricantes", indica.

Carlos Galdón, director de canal de Sophos Iberia

En cuanto a cómo deberían diseñar pymes y autónomos sus planes de ciberseguridad, Galdón asegura que, a pesar de ser "un modelo un poco más reducido", estas empresas deberían seguir, como hoja de ruta, los puntos clásicos de todo plan de seguridad: análisis de riesgos, objetivos del plan, tecnologías y políticas. Además, "tienen que contar, por un lado, con un contrato de ciberseguridad como servicio, como el MDR de Sophos, y, por otro lado, con una ciberseguridad gestionada por un tercero que vigile en

todo momento cuál es el estado de protección de la empresa", detalla.

MDR para pymes

El responsable de canal de Sophos Iberia recuerda que las soluciones de ciberseguridad como servicio permiten monitorizar, detectar, detener y remediar posibles ciberataques. Sobre si las pymes deben optar por una solución de ciberseguridad como servicio o un servicio de ciberseguridad gestionada, el directivo está convencido de que la mejor solución para pymes y autónomos es la combinación de ambas, es decir, "disponer de una herramienta de seguridad como servicio que esté gestionada dentro de un modelo MSSP". De esta manera, como señala, "tienen una protección total frente a amenazas dentro de un modelo flexible y financieramente muy atractivo".

"Debemos seguir exigiendo a la Administración pública mayor implicación en el desarrollo de los programas de inversión y concienciación para pymes en ciberseguridad"

¿Cómo deben las pymes elegir un servicio de MDR? Galdón considera que estas organizaciones deben fijarse en tres aspectos claves. Por un lado, asegurarse de que el servicio dispone de diferentes SOC a nivel mundial y que están disponibles todos los días a cualquier hora, es la

única manera de garantizar que el servicio podrá responder al ciberataque en cualquier momento.

Por otro lado, "la resolución de incidencias tiene que ser lo más completa posible y acabar completamente el trabajo que se le encomiende", destaca. En este sentido, el directivo explica detalladamente que no es lo mismo que el servicio envíe un *email* para avisar de la incidencia a que sea capaz de eliminarla. Por eso, aconseja "estar muy atentos porque hay mucha diversidad en la oferta".

Por último, Galdón recuerda a pymes y autónomos que deben "elegir servicios que tengan la mayor cantidad de fuentes de información posible". Gracias a estas conexiones con terceros el servicio tendrá más capacidad de datos, es decir, más posibilidades de encontrar conductas sospechosas.

"Las pymes deben disponer de una herramienta de seguridad como servicio que esté gestionada dentro de un modelo MSSP"

La propuesta de Sophos

El valor diferencial de la propuesta MDR de Sophos se encuentra en tres pilares, los cuales están estrechamente relacionados con los puntos claves que debe cumplir este servicio para garantizar la máxima protección de pymes y autónomos. En primer lugar, el *endpoint*, "agente principal del servicio, que nos permite frenar los ataques y decidir cómo gestionar los ciberataques", explica Galdón.

La telemetría de terceros es el segundo pilar. El servicio MDR de Sophos cuenta con dicha telemetría a través de los conectores de la mayoría de fabricantes. De esta manera, la compañía cuenta con una amplia cantidad de datos que le permite trabajar, tanto aplicando algoritmos de IA como personas, en la búsqueda de actividad sospechosa.

La tercera pata sobre la que se asienta este servicio son los SOC. Concretamente Sophos ha equipado a su servicio MDR con seis SOC repartidos por todo el mundo que están operati-

vos en cualquier momento con el fin de frenar los ciberataques.

Galdón, además, recuerda que en el servicio MDR tanto la detección como la respuesta "son dos parámetros fundamentales" porque, como explica, "la detección se basa en la cantidad de información que sea capaz de recopilar y la cantidad de recursos que puedan poner a trabajar sobre dicha información". En cuanto a la respuesta, el directivo de Sophos Iberia comenta que "debe incluir la notificación, contención y la completa limpieza del sistema". En ambos aspectos pymes y autónomos deben comprobar qué soluciones ofrecen y a qué proveedor pertenecen.

"Nuestro MDR se diferencia por nuestro endpoint, la telemetría de terceros y los 6 SOC que incorpora"

Pero, aunque la propuesta de servicio MDR de Sophos es sólida, el fabricante sigue trabajando para mejorarla y con este objetivo en los próximos años "seguiremos evolucionando nuestro MDR hacia un nivel de mayor automatización gestionado por personas en labores de búsqueda o patrones con ayuda de la IA", indica.

También integrarán tecnologías de red, *firewalls* y NDR, e incorporarán tecnologías que permitan obtener más información de la nube pública. Todo esto, sumado a la unificación de la plataforma y los procesos, son las vías de trabajo que la compañía tiene abiertas para los próximos años.