"La **formación** es la **primera barrera** de **seguridad**, sin ella da igual la **estrategia** que empleemos"

2020; el año en el que el trabajo remoto se erigió como la solución para garantizar la continuidad de negocio. Sin embargo, la implantación masiva y forzosa de esta modalidad laboral provocó numerosas brechas de seguridad ya que el perímetro, como se conocía hasta ese momento, desapareció y dejó a los usuarios y a los datos descentralizados. Olga Romero

IR A PÁGINA SIGUIENTE

Además, para muchas empresas, especialmente pymes, la seguridad pasó a un segundo plano porque, como reconoce Eduardo García Sancho, *Sales & Channel Manager* de Syneto España, "la pyme se vio totalmente desbordada y sin un plan de contingencia". El directivo asegura que estas empresas primaron equipar a sus trabajadores con los dispositivos necesarios para el teletrabajo. "También hay que tener en cuenta que las pymes no tienen la flexibilidad ni la capacidad económica de las grandes corporaciones, por eso la adaptación se ha ido haciendo de manera paulatina", explica. Un proceso que García Sancho comenta que ha sido largo y en el que "han surgido muchos problemas que poco a poco se han ido solucionando y, sobre todo, entendiendo".

Este nuevo escenario, así como la situación de desconocimiento y caos, fueron aprovechados por los *hackers* para desplegar sus armas. Unos ataques que han evolucionado y han dejado de ser ataques dirigidos a grandes empresas para convertirse en sistemas generalizados destinados a miles de organizaciones. Gracias a esta evolución los ciberdelincuentes se ahorran el análisis y la investigación previos para encontrar posibles brechas y fallos.

"Dirigiendo el ataque a miles de empresas la posibilidad de que alguien caiga es mayor", afirma García Sancho. Sobre las consecuencias de estos ciberataques, el directivo comenta que al no ser dirigidos varían, "pero suelen implicar ciberdelincuencia grave, es decir, exponer al empresario a problemas legales y económicos", explica.

Seguridad, ¿inversión o gasto?

La seguridad siempre ha sido vista más como un gasto que como una inversión, especialmente en el sector de las pymes. Una concepción que, como asegura García Sancho, cambia tras sufrir un incidente de ciberseguridad. El directivo explica que "un ciberataque significa una parada de producción en una empresa, es decir, dejar de prestar el servicio que das a tus clientes".

Eduardo García Sancho, *Sales & Channel Manager* de Syneto España

Esta parada supone unas pérdidas, pero también conlleva un gasto para recuperarse de di-

Los hackers han dejado de desarrollar ataques dirigidos para emplear sistemas generalizados de ataques

cho incidente. "Este gasto es, aproximadamente, entre 10 y 50 veces mayor que si se realiza la inversión con antelación", comenta. Y este es el mensaje que desde Syneto están dando a las pymes: "Hay muchas empresas que lo entienden e invierten en su estrategia de seguridad y otras muchas que lo comprenden cuando ya han sido atacadas y ya no hay remedio".

Concienciación y formación: pilares fundamentales

"En cualquier charla sobre seguridad y ciberdelincuencia este es el primer aspecto que detallamos como fundamental todos los fabricantes", afirma. Y es que la formación y concienciación de los empleados, y de los usuarios en general, son claves para evitar ciertos ataques, especialmente los que emplean el correo electrónico como vector de ataque.

En este sentido García Sancho es claro y rotundo: "Da igual lo que hagamos las empresas que como se carezca de formación sobre el comportamiento de la tecnología y sus riesgos, todo lo demás no sirve de nada". Por ello el directivo asegura que las organizaciones necesitan formar a sus trabajadores, así como analizar sus comportamientos y hacerles conscientes de los continuos riesgos a los que se exponen, por muy inofensiva que parezca la situación.

El directivo también recuerda que, al igual que los ataques evolucionan, la formación en ciberseguridad debe ir renovándose para que los empleados estén siempre preparados para las nuevas amenazas. Porque, como declara, "la formación y la responsabilidad son la primera barrera de seguridad".

Adiós al perímetro tradicional

La llegada del teletrabajo ha dejado numerosos desafíos en el sector de la seguridad. Algunos de estos nuevos retos son la desaparición del perímetro tradicional y la descentralización de los usuarios y los datos. Las pymes deben garantizar estos activos a través de la formación, por supuesto, pero también "teniendo actualizada su política de ciberseguridad, ya sea a través de un *partner* tecnológico, que les explique los pasos a seguir, o por el propio responsable de tecnología de la empresa".

Una vez actualizado el plan de seguridad hay que ser capaz de aplicarlo al entorno de trabajo que tenga la empresa. "Las pymes tienen que extender su política de seguridad a todos los trabajadores y dispositivos", afirma.

Pero, como reconoce García Sancho, el sector de la seguridad seguirá enfrentándose a nuevos desafíos de manera continua. "Los retos que le quedan por delante al sector son infinitos, ya que la seguridad debe evolucionar al ritmo que evolucione la tecnología", subraya. Para el directivo la formación, la tecnología y la protección del dato tienen que estar en continuo desarrollo dentro de las empresas.

"La tecnología evoluciona y con ella las brechas de seguridad y, por supuesto, los ciberdelincuentes. Si las organizaciones no se quieren quedar obsoletas deben evolucionar al mismo ritmo", comenta.

"La formación es la primera barrera de seguridad"

HYPER Edge, el pequeño-gran centro de datos

Coincidiendo con su primer aniversario en el mercado de Iberia, Syneto acaba de presentar HYPER Edge. Una plataforma diseñada para la gestión de datos en entornos *edge* que resuelve los problemas de espacio, coste y consumo de energía. Se trata de una solución versátil, silenciosa, fácil de instalar y con un diseño elegante y compacto.

HYPER Edge es el *data center* más pequeño de la compañía, que ha conseguido llevar todo el poder de un gran centro de datos a una solución del tamaño de tres *smartphones*. Además, esta nueva herramienta ofrece la máxima eficiencia del espacio y reduce el consumo energético.

La plataforma también dispone de un innovador sistema de refrigeración y una CPU con procesador Intel Core i7 de hasta 4,7 GHz capaz de acelerar aplicaciones críticas para el negocio.

HYPER Edge está basado en SynetoOS, el sistema operativo propio de la compañía y que está diseñado específicamente para equipos hiperconvergentes. De esta manera, la nueva solución proporciona una interfaz simple y unificada, una gestión rápida y sencilla a través de un solo click, protección de datos con hasta 1.440 copias de seguridad por día e inmunidad al *ransomware*. La nueva solución, que se une a la familia HYPER Series, también ofrece una recuperación ante desastres en solo 15 minutos tras el incidente, así como acceso a los datos en menos de un milisegundo. Además, su instalación es rápida y sencilla.

La tecnología, formación y protección del dato tienen que estar en continua evolución

Planes y objetivos

El lanzamiento de HYPER Edge está dentro de los planes que Syneto tiene para este último tramo del año. Asimismo, el fabricante tiene como objetivo duplicar su canal cualificado. Actualmente cuenta con 22 *partners* estratégicos activos y certificados en España, en el próximo trimestre. Para alcanzarlo Syneto cuenta con su programa de canal, Channel Challenge. "Estamos convencidos que de aquí a final de año lograremos cumplir con nuestros objetivos de crecimiento en el número de *partners* y volumen de negocio", asegura García Sancho. Por el momento la compañía tiene más de 2.700 clientes en Europa.

Además, tal y como explica el directivo, Syneto ofrece a los *partners* una financiación al 0 %, así como asesoramiento para que los clientes puedan acceder a todo tipo de ayudas públicas como, por ejemplo, los Fondos NextGenEU o cualquier otra ayuda que puedan tener disponible a través de los organismos públicos.

Syneto Iberia acaba de ampliar su equipo con las incorporaciones de Reinaldo Baldino como *Channel Marketing Specialist* y Pablo Ballestero en el *Business Development* en España. Ambos se suman a Matteo Restelli, *Country Manager;* Eduardo García Sancho, *Sales & Channel Manager*; y Ander Cabarcos, *Technical & Presales Manager*.

Syneto ofrece protección y recuperación ante un incidente de manera rápida y eficaz

Para Syneto contar con una estrategia de seguridad tiene que eliminar la incertidumbre de las pymes y garantizar la vuelta al trabajo de forma rápida y eficaz. Un objetivo que las soluciones de ciberseguridad que emplean las grandes empresas ya ofrecen, pero ¿y en el caso de las pymes?

El fabricante quiere, tal y como reconoce Eduardo García Sancho, *Sales & Channel Manager* de Syneto España, en este vídeo acercar esas soluciones a las pequeñas y medianas empresas. "Ofrecemos a las pymes la oportunidad de estar preparadas para que cuando el desastre ocurra no pierdan sus datos y puedan volver al nivel de producción previo al ataque", asegura.

Eduardo García Sancho, *Sales & Channel Manager* de Syneto España