NEGOCIO | **INNOVACIÓN**

‘Start up’ que protegen de los ‘hackers’ el teletrabajo

La **ciberseguridad** es uno de los pocos sectores que salen reforzados de la pandemia del Covid-19. El trabajo a distancia obliga a las compañías a proteger mejor sus equipos, una labor para la que cuentan con los emprendedores.

Alejandro Galisteo. Madrid

El pasado 1 de junio, la Universidad de California en San Francisco (UCSF, por sus siglas en inglés) tuvo que desembolsar 1,14 millones de dólares para defender la fórmula de la futura vacuna contra el Covid-19. Netwalker, una banda de *hackers*, extorsionó a los rectores de la escuela norteamericana. Sin embargo, no hace falta irse tan lejos ni a instituciones de tanto prestigio para ser objetivo de un cibercrimen, sobre todo ahora, cuando las empresas tienen al grueso de su plantilla en casa. Y parece que el modelo de teletrabajo ha llegado para quedarse, con lo que eso supone para los piratas informáticos: una puerta abierta a los sistemas de las compañías.

El Centro de Operaciones de Seguridad (SOC) de Grupo Oesía informó que, durante el confinamiento, las alarmas de ciberseguridad se triplicaron. Y es algo que se venía advirtiendo, ya que el primer trimestre de 2020, previo a la pandemia, el número de ciberataques aumentó un 40% a nivel mundial, según datos de IBM. “El aumento exponencial de personas y dispositivos conectados en remoto, así como la adopción de *cloud* de manera masiva, hizo crecer el grado de exposición de las empresas. Esto no quiere decir que seamos más inseguros, lo que sí tenemos es más superficie de exposición y la misma debe ser protegida. Esta protección se gestiona en varios ejes: prevención, detección y respuesta, por lo que el sector no ha parado de crecer”, explica Pedro Pablo, consejero delegado de ElevenPaths, la división de ciberseguridad de Telefónica.

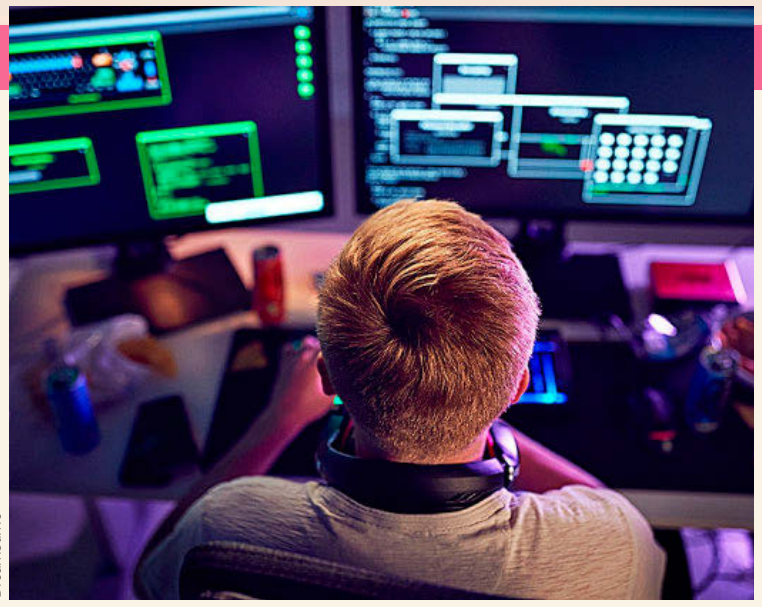
Dreamstime

Los números no hacen más que dar la razón a Pablo. En el *webinar Retos y soluciones para la ciberseguridad de la tecnología operacional*, los expertos de IDC Research Spain anunciaron que en 2020 el mercado de la ciberseguridad generará en España un volumen de negocio de 1.381 millones de euros, lo que supondría un crecimiento del 6% con respecto al año2019.

La protección se vertebra en tres ejes: prevención, detención y respuesta

En estos últimos meses esa mayor exposición que experimentan las empresas y las personas al llevar casi toda su vida en modo remoto amplía aún más este mercado y despierta interés en nuevos jugadores e inversores, lo que explica el auge de un sector en el que las *start up* españolas juegan un papel muy importante.

La principal diferencia entre el emprendedor y la multinacional tiene que ver con ritmo que marcan los *hackers*. “Esto implica una agilidad que es más difícil de ejecutar en grandes empresas de software. También es un tema de *mindset* y cultura de empresa. Las grandes compañías no disponen de los mecanismos y la forma de trabajar que exige este sector tan cambiante y experimental donde la agilidad es clave” concluye Marc Torres, profesor de Esade.


Dreamstime

CLAVES DEL SECTOR

- **Teletrabajo.** En España, en 2020 se pasó de un 5% de personas trabajando desde su casa al **36%** de la actualidad.
- **Empresas.** Se estima que el **39%** de las empresas españolas sufrió un ataque de ciberseguridad en 2019, unos números que parece van a quedarse muy pobres en 2020.
- **Coste.** El coste medio de cada ciberataque a una pyme es, según el estudio de Google ‘Panorama actual de la ciberseguridad’ en España, de **35.000 euros**, y el 60 % cierra seis meses después de haber sufrido uno.
- **Porqué ‘start up’.** Los emprendedores tienen una agilidad y conocimiento técnico y específico de algunos segmentos del mercado de difícil acceso para grandes compañías. Pero es un sector donde más que la supremacía de grandes o pequeños, la **colaboración** es más relevante que en cualquier otro ámbito. Los clientes más exigentes, como pueden ser los bancos o los gobiernos, demandan especialización, innovación, estar en la frontera del conocimiento, pero también robustez, confianza y capacidad de cubrir todos los aspectos de la seguridad.
- **Tipos de empresa.** Las soluciones más demandadas pasan por la **protección** del dato, las comunicaciones seguras, eliminación instantánea de contenido ilegal y software de redes privadas en remoto.

David Barroso, fundador de Countercraft.

Contrainteligencia digital

En pleno confinamiento, los responsables de **Countercraft** anunciaron una ronda de financiación cerrada con éxito en mitad de julio. Habían levantado 4,5 millones de euros. "El hecho de haber cerrado la ronda en unas circunstancias tan difíciles, que nos han obligado a quedarnos en casa y recurrir a la tecnología para llevar a cabo todas las reuniones necesarias, ha sido todo un reto y nos enorgullece haberlo superado", explica David Barroso, fundador y consejero delegado de una compañía que nació en San Sebastián, pero que tiene vocación internacional. De hecho sus competidores se encuentran entre Israel y Estados Unidos. La tecnología de Countercraft ofrece inteligencia propia para, en vez de levantar muros para mantener al enemigo fuera, crear una trampa por la que se vaya a colar el adversario para llegar a un entorno ficticio y controlado por la empresa. La 'start up', que colabora entre otros con PwC y Minsat, de Indra, manipula al atacante recurriendo a la contrainteligencia: le hace creer que está robando información mientras le permite estudiar y conocer mejor sus técnicas, sus objetivos y sus intenciones. "Por ejemplo, puede darse el caso de una empresa que se dedica a fabricar aviones necesite poner a salvo los planos del último modelo que ha desarrollado. En este caso se generarían planos falsos, aparentemente desprotegidos, y se atraería al atacante mediante algún tipo de cebo, que en realidad es un activo. De esta manera, cuando cayera en la trampa, el atacante pasaría a ser investigado", concluye Barroso.

Entrenando la ansiedad de un ataque

Solamente en Europa, se estima que en 2022 habrá más de 350.000 puestos relacionados con la ciberseguridad que quedarán vacantes. Una demanda de perfiles que no existen y que trata de cubrir **iHackLabs**. "Nuestro objetivo es ayudar a las organizaciones a resolver este problema facilitándoles soluciones que les permitan identificar el talento potencial para trabajar en ciberseguridad y seleccionarlo, formar y entrenar a candidatos y especialistas, y realizar ejercicios de estrés (similares a los que realizan periódicamente los pilotos de aviones comerciales) para que los alumnos se enfrenten a ciberataques similares a los que se producen diariamente en Internet", explica Miguel Rego, consejero delegado de iHackLabs. El emprendedor, que antes de marcar el rumbo de esta 'start up' había dirigido el Instituto Nacional de Ciberseguridad de España, señala como uno de sus proyectos más destacados el que tiene con la Junta Interamericana de Defensa. "Este organismo, con base en Washington DC, tiene como objetivo ayudar a la mejora en las capacidades de ciberdefensa en el continente americano. Nuestra colaboración con la JID está centrada en el diseño de contenidos formativos y en el desarrollo de talleres de trabajo y entrenamientos", asegura Rego. La compañía valora seguir creciendo más allá de España, donde llegó en 2018, dos años después de ser fundada en Reino Unido. Y los indicadores –que señalan que en los próximos diez años se demandarán cada vez más perfiles relacionados con la ciberseguridad– parecen avalar la idea.

Miguel Rego, consejero delegado de iHackLabs.

Píldoras para atajar el riesgo

Kymatio es una 'start up' de ciberseguridad que identifica, analiza, evalúa y proporciona todo lo necesario para tratar los riesgos internos de origen humano relativos a seguridad de la información. "Nuestro sistema intercala periódicamente con los empleados teniendo entrevistas virtuales con ellos, sesiones ágiles, de 5 o 10 minutos que se realizan a través de un chatbot", explica David Sánchez, director de operaciones de la compañía. En estas sesiones Kymatio realiza preguntas muy variadas, como por ejemplo el tipo de información que utilizas, que es parte de la determinación del impacto de un incidente en tu puesto, o cómo estás en cuanto a conocimientos de ciberseguridad básicos, y en general cuál es tu situación en la empresa. Con esta información, el sistema es capaz de ofrecer a cada empleado acciones periódicas de concienciación en ciberseguridad, píldoras de conocimiento o recomendaciones personalizadas de bienestar. Durante la pandemia del coronavirus, iniciaron conversaciones con clientes tan relevantes como Santander Vida y Generales o Telefónica. "A principios de junio incrementamos un 40% nuestra primera ronda de inversión para dar cabida a dos nuevos socios: BStartup, de Banco Sabadell, y el fondo JME Ventures. De esta manera ambos se suman a la ronda liderada por The Crowd Angel, que contaba con grandes apoyos como Wayra y destacados 'bussines angels' como Enrico Raggini", comenta Sánchez.

David Sánchez, director de operaciones de Kymatio.

Aliados con el cine contra la piratería

La idea de negocio de **Smart Protection** surge al descubrir la necesidad de transformación digital en la lucha contra la piratería de contenidos en Internet. "Se venía haciendo por medios legales tradicionales que no conseguían la efectividad necesaria ante la avalancha de copias falsas provocada por grupos organizados y altamente tecnificados", apunta Javier Perea, consejero delegado de una empresa que cautivó a clientes como Antonio Banderas, con su productora Green Moon Producciones, o Almodóvar con El Deseo. "En el caso de películas, series o libros, estos pueden protegerse de forma permanente o durante unos meses, coincidiendo con el lanzamiento de cada contenido. Por otro lado, los eventos deportivos en directo pueden protegerse partido a partido o por ligas completas. Las marcas y productos, sin embargo, se protegen de forma anual, ya que tienen un carácter más permanente y en ellos se aplican algoritmos de 'machine learning' que optimizan los resultados a medida que aumenta el periodo de protección", explica Perea. Lo que se inició con la protección de una primera película para Antonio Banderas ha evolucionado hasta convertirse en una empresa que no solo lucha contra la piratería digital sino que también protege a las marcas de falsificaciones en internet con el uso de la tecnología, y que cuenta hoy con unos cien empleados de 20 nacionalidades distintas y clientes hasta en 22 países.

Javier Perea, consejero delegado de Smart Protection.