NEGOCIO | **OPORTUNIDADES**

Las ‘start up’ que combaten el ataque de los ‘hackers’

La pandemia ha provocado una **digitalización acelerada** en el tejido productivo español. Los cambios han hecho que los activos digitales se conviertan en los más valiosos y vulnerables para todas las empresas.

Jesús de las Casas. Madrid

¿Qué haría si mañana, sin previo aviso, no pudiese acceder a toda la información de su negocio? Parece una pesadilla, pero es una realidad que padecen cientos de empresas cada día en España. 2021 fue escenario de importantes ciberataques que pusieron en jaque a organismos públicos como el Servicio Público de Empleo Estatal (SEPE) y también a compañías de todos los tamaños, y es que hace tiempo que las pequeñas y medianas empresas dejaron de pasar desapercibidas para los *hackers*.

Aunque el Instituto Nacional de Ciberseguridad (Incibe) aún no ha revelado la cifra de ataques registrados en 2021, este tipo de incidentes no dejan de crecer. Sólo en España se produjo una media de 40.000 ciberataques diarios durante el último año, un dato que refleja un incremento del 125% respecto a 2020, según estimaciones de Datos101. La implantación acelerada del teletrabajo ha abierto una puerta a los ciberdelincuentes y ha situado en la diana a todas aquellas organizaciones cuyos empleados trabajan mayoritariamente desde casa.

Dreamstime

Este escenario ha provocado que la ciberseguridad cobre más importancia que nunca, ante la necesidad de prever y dar respuesta a amenazas cada vez más numerosas y complejas. Las *start up* no han sido ajenas a este fenómeno: el ecosistema español se ha situado en los últimos años como un actor relevante en este ámbito y ha dado a luz compañías que han crecido hasta protagonizar operaciones muy destacadas a escala mundial. Estos emprendedores vienen a revolucionar el sector, con soluciones que cuentan con una gran escalabilidad y un valor incalculable para sus clientes.

Lejos de detener a los ciberdelincuentes, la pandemia generó un caldo de cultivo idóneo para su actividad debido al incremento de las personas y dispositivos conectados en remoto, además de la adopción masiva de la nube. El grado de exposición de las compañías ha aumentado en paralelo a la incertidumbre global. Más de la mitad de las grandes empresas no son capaces de detener de manera eficaz los ciberataques, según un informe de Accenture, que resalta que el número de incidentes en España creció el año pasado un 236% respecto de 2020.

No sólo se dispararon las amenazas, sino que además su efectividad fue mayor que nunca, con un crecimiento del 32% en la cifra de ciberataques efectivos en comparación con el año anterior. El repunte fue especialmente significativo en el caso del *ransomware*, que se consolida como uno de los principales riesgos para las empresas. Ante estas perspectivas, el gasto en ciberseguridad no deja de crecer: el 82% de las compañías ha elevado su inversión en el último año, una tendencia que queda patente tanto en el plano internacional como en España. Es la consolidación de un sector que va camino de convertirse en un gigante global.

Gigantes con sello español

Hace ya quince años que **AlienVault** nació en Madrid. Por aquel entonces, nadie esperaba que una ‘start up’ española de ciberseguridad pudiese llegar a convertirse en un referente mundial de este segmento. Sin embargo, y tras una década de vida, esta empresa fue adquirida en 2018 por el gigante estadounidense AT&T por una cantidad cercana a los 500 millones de euros. Algunos años atrás, en 2012 Google había visitado España para hacerse con la ‘start up’ malagueña VirusTotal, que ofrecía una herramienta sencilla y práctica para detectar virus en archivos y páginas web. A diferencia de la mayoría de las compras de la compañía de Mountain View, el equipo de **VirusTotal** mantuvo su autonomía y aún sigue trabajando desde Málaga, ahora bajo el paraguas corporativo de Chronicle –la firma especializada en ciberseguridad de su matriz Alphabet–. Son los dos casos pioneros que pusieron de manifiesto que las ‘start up’ españolas no tienen nada que envidiar a sus competidores internacionales.

La aparición de estas empresas, cuyas tecnologías de desarrollo propio son capaces de rivalizar con las de potencias como EEUU e Israel, ha puesto a España en el mapa del sector como un referente en todo el mundo.

En los últimos años, la lista de compañías que se han hecho un nombre en el mundo de la ciberseguridad no deja de crecer. Una de ellas ha llegado a ser unicornio: es la tecnológica **Devo**, que pone el foco en la seguridad y análisis de datos en la nube, que lo consiguió tras anunciar en octubre de 2021 una ronda de financiación Serie E de unos 215 millones de euros (250 millones de dólares). La ‘start up’ fundada por Pedro Castillo es de origen español pero tiene su sede en Estados Unidos.

Devo es el primer unicornio de ciberseguridad de origen español.

Además, **Revelock**, pionera en el mercado español de la prevención del fraude online, fue adquirida en agosto por Feedzai, un unicornio portugués que también se centra en este ámbito. A finales de 2020, las tecnológicas españolas **4iQ** (liderada por el cofundador de AlienVault Julio Casal) y Alto Analytics se fusionaron para crear la gran empresa de ciberseguridad **Constella Intelligence.**

David Barroso, fundador y CEO de CounterCraft, junto a Dan Brett, fundador y director estratégico de la 'start up'.

Seguridad española en el Pentágono

Durante la Guerra Fría, los servicios de contraespionaje optaban por vigilar a los espías extranjeros en lugar de expulsarlos de sus países, para evitar así la llegada de nuevos agentes infiltrados. **CounterCraft**, una 'start up' fundada en San Sebastián en 2015, nació con la idea de utilizar técnicas de engaño y contrainteligencia digital para combatir los ciberataques. Es decir, permite que los 'hackers' accedan a datos y aplicaciones ficticias diseñadas como un cebo para investigar quiénes son, conocer sus motivaciones e incluso dirigir sus próximos pasos. La compañía ya tiene oficinas en Nueva York, Londres y Madrid, y ha conseguido un hito inédito para una 'start up' española: firmar un contrato de servicios con el Departamento de Defensa de Estados Unidos. Así, los sistemas de seguridad del Pentágono, en Arlington (Virginia, EEUU), incorporan desde el año pasado la tecnología de la compañía donostiarra que, de este modo, se ha aupado hasta la élite global de la ciberseguridad. "Que el Departamento de Defensa de Estados Unidos utilice tu producto para protegerse de las amenazas es como jugar en la Champions League", aseguraba David Barroso, consejero delegado y cofundador de CounterCraft.
La firma se ha asentado en el mercado estadounidense, que ya representa la mayor parte de sus ingresos y prepara una nueva ronda en tierras norteamericanas.

Así se detectan los riesgos

Los fundadores de **Kymatio** se conocieron cuando trabajaban en la ciberseguridad de empresas como BBVA, Liberbank y Mercedes-Benz. Allí se dieron cuenta de que numerosos incidentes se originaban de forma involuntaria por los propios trabajadores de las compañías. De este modo, la 'start up' pone el foco en identificar, evaluar y proporcionar todo lo necesario para tratar los riesgos internos de origen humano referentes a la seguridad de la información. A día de hoy, "asistimos a una constante avalancha de ciberataques, y alrededor del 90% se dirige a los empleados. Es imprescindible prepararlos frente a las amenazas y disponer de métricas sobre este grave riesgo", señalan desde la compañía. Su sistema entrena a cada profesional de manera personalizada según sus vulnerabilidades individuales, simula ataques de 'phishing', busca credenciales online expuestas en brechas de seguridad y utiliza esta información para trabajar el riesgo con los propios empleados. La empresa presta sus servicios a un amplio abanico de clientes, desde despachos de abogados hasta 'start up', grandes tecnológicas y bancos, además de contar con el apoyo de inversores como Wayra, JME Ventures y BStartup, de Banco Sabadell.

Fernando Mateus, fundador y CEO de Kymatio.

La sede principal de Ironchip se encuentra en Barakaldo (Bilbao).

La localización como garantía

José Fernando Gómez y Julen Martínez eran estudiantes de ingeniería cuando decidieron fundar **Ironchip**. Esta 'start up', que tiene su sede en Barakaldo (Vizcaya), parte de la premisa de que la ubicación es un factor clave en las operaciones de riesgo porque puede determinar el comportamiento de las personas. "Por eso decidimos crear una tecnología capaz de convertir la ubicación en un factor de seguridad confiable, ya que los métodos de localización actuales no lo son", afirma su CEO y cofundador, Julen Martínez. El directivo indica que su sistema de autenticación cuenta con características únicas de seguridad, ya que crea una huella digital asociada que limita el acceso dependiendo del lugar en que está el usuario. Sus soluciones se dirigen principalmente al sector de servicios esenciales. Como ejemplo, Martínez destaca el caso de ciertos 'hackers' que atacan los sistemas de red eléctrica de determinados países o ciudades. Estos ataques no podrían producirse si el acceso a estos sistemas se limitase a localizaciones concretas, en lugar de todo Internet.

En la piel de los 'hackers'

Hace más de una década que Daniel Solís se dio cuenta de que la ciberseguridad llegaría a ser una industria potente. Ese convencimiento le llevó a fundar **Blueliv**, una 'start up' barcelonesa centrada en el ámbito de la ciberinteligencia. La compañía trabaja en la detección de amenazas gracias a un amplio conocimiento del cibercrimen y la tecnología que subyace. "Proporcionamos información sobre amenazas externas, de modo que nuestros clientes pueden prevenir o reaccionar frente a ellas, reduciendo drásticamente sus riesgos y acelerando sus tiempos de respuesta", subraya Solís, CEO de la empresa. Blueliv nació con vocación internacional y creció en los primeros años gracias a la captación de grandes clientes del sector de la banca y los seguros fuera de España. Desde entonces la 'start up' ha logrado conquistar a más de 250 clientes en 40 países, hasta que el pasado verano fue adquirida por uno de los mayores grupos de ciberseguridad de Europa, la compañía de origen sueco Outpost24. No obstante, Solís comenta que Blueliv sigue operando de forma independiente como línea de negocio con presencia fiscal en España.

El equipo de Blueliv.

A la caza los 'piratas'

En los dos últimos años, la digitalización exprés de muchas empresas y el auge del ecommerce han disparado la venta de productos falsos en Internet. La 'start up' barcelonesa **Red Points**, que cuenta con oficinas en Nueva York y Salt Lake City, ha desarrollado un 'software' que utiliza la inteligencia artificial y facilita a las empresas la detección y eliminación automatizada de falsificaciones, piratería y distribución ilegal de contenidos online. Es un problema que cada año provoca pérdidas millonarias a empresas de todos los sectores. La empresa ha transformado "una industria tradicionalmente dirigida por abogados de propiedad intelectual y empresas enfocadas a servicios en una solución tecnológica escalable", explica su CEO Laura Urquizu. Desde que nació hace una década, Red Points se ha convertido en uno de los principales referentes internacionales en la lucha contra las falsificaciones y más de 550 marcas de todo el mundo utilizan su tecnología. Con el impulso de la pandemia a su actividad, la 'start up' preveía a finales de 2021 nuevas contrataciones para aumentar sus ventas un 50% en 2021 tras cerrar 2020 con una facturación de 15,5 millones de euros.

El equipo de Red Points.