“Nuestro modelo de defensa inteligente colaborativa es nativo de la transformación digital”

>Por **José de la Peña Muñoz**
>Fotografía: **Jesús A. de Lucas**

Daniel Solís Agea

CEO y Fundador de Blueliv

En 2009, tras una intensa carrera profesional en Unitronics, S21sec y KPMG, un joven ingeniero de telecomunicaciones, Daniel Solís, decidió jugarse el futuro a una carta, y fundó la compañía Blueliv, convirtiéndose en uno de los pocos y genuinos "emprendedores" españoles en ciberseguridad. Siete años después, con alguna cana más y una compañía con clientes en quince países, no ha perdido un ápice de su entusiasmo y creatividad.

– ¿Se considera usted un emprendedor?

– Corría el año 2009, y algunos expertos nos habíamos dado cuenta de que los sistemas tecnológicos de gestión de riesgos de inseguridad digital y de control de fraude electrónico, con ser necesarios, no eran suficientes para poder prevenir, prever razonablemente y poder tomar medidas de defensa casi en tiempo real. La debilidad principal era la falta de información de fuentes externas, y la dificultad para analizar y explotar toda la información. No había ciclo de inteligencia ni estaba metabolizado el concepto de colaboración.

Con esos mimbres, me lié la manta a la cabeza y decidí crear Blueliv. Fue muy duro, porque iniciamos la actividad en plena crisis económica. Con mucho esfuerzo logramos crear el germen de lo que hoy es Cyber Threat Intelligence Platform, algunas empresas nos contrataron y obtuvimos financiación externa. Siempre agradeceré la confianza que depositaron en nosotros algunos clientes que apostaron por nuestro modelo de ciberseguridad.

– Muchos expertos relacionaron desde ese momento a Blueliv con la vigilancia digital.

– Nosotros trabajamos, desde el principio, en la defensa inteligente colaborativa. El concepto de vigilancia digital es erróneo y supone confundir la parte con el todo.

– ¿Cuántas personas forman hoy el equipo de Blueliv?

– Somos sesenta y cinco personas, de las cuales cincuenta son ingenieros.

– ¿Y en cuántos países operan?

– Nuestros mercados principales son EE.UU., España y Norte de Europa, además de Francia, Alemania e Italia. También operamos en Reino Unido, Canadá, Chile, México,… En total, quince países.

– ¿En qué sectores operan sus clientes?

– Principalmente en banca y los seguros, aunque los de distribución y energía empiezan a demandar soluciones acordes con las particularidades de sus sectores.

– Siempre va en primer lugar el sector financiero.

– Lo primero en lo que se afanaron los delincuentes fue en robar dinero a entidades y clientes. Sin embargo, aunque el robo masivo de dinero causa gran revuelo, lo cierto es que en la "Dark Web" se trafica con todo tipo de datos de cosas, de personas físicas y jurídicas, y con una diversidad de finalidades pasmosa: extorsión, chantaje, espionaje industrial, sabotaje, modificación del valor de las cosas, terrorismo… En fin, las amenazas intencionadas son cada vez más agresivas, más constantes y se lanzan en momentos muy bien estudiados. Los malos están cada vez mejor informados. Y, en paralelo, se continúan haciendo los ataques de siempre aprovechando vulnerabilidades documentadas, ya en el software y las comunicaciones, ya imprevisiones y vacíos en los procesos organizativos internos y en los procesos de externalización, mezclados con ingeniería social.

– La función de inteligencia no de negocio en las empresas ha estado vinculada históricamente a las áreas de seguridad clásicas. ¿Qué aporta su compañía a dichas áreas?

– No hay distintos tipos de inteligencia; lo que sí tenemos es distintas formas de contextualizar la información. Las áreas de seguridad corporativa tienen experiencia en la investigación, conocen a los proveedores tradicionales de datos, y dominan el arte de la gestión de las redes de personas. Pero se encontraban con la barrera digital, porque para saber lo que se estaba guisando en el ciberespacio, tenían poco más que Google.

Blueliv proporciona desde hace años a todas las funciones de seguridad herramientas para saltar al universo digital y saber qué están haciendo los malos. En la compañía no entramos en el debate de si es mejor la nueva cocina o la tradicional. Lo que nos gusta es la buena cocina.

– ¿Qué ofrece Blueliv?

– Lo que nosotros facilitamos a nuestros clientes es la visibilidad de Internet y el análisis de las amenazas de su interés –en base a nuestra clasificación de las mismas por módulos–. A partir de aquí los apoyamos para que puedan ir creando su propia ciberinteligencia. Ellos tienen habilidades y necesidades que nosotros podemos desconocer.

– Hay otras compañías que prestan servicios similares.

– En la actualidad; pero no hace siete años. Nosotros fuimos visionarios. Y ya sabe lo que se dice: que quien golpea el primero, golpea dos veces. Además, la tecnología que aportan otras compañías es limitada y poco escalable o en algunos casos no existe, lo que resulta en que todo se hace de forma manual, insuficiente para procesar volúmenes ingentes de información y correlar datos.

– También se dice eso de que a los pioneros se los comen los indios.

– No siempre. Llevamos siete años en esto y no hemos escatimado esfuerzos. En los mercados domésticos detectamos una sobreoferta de productos generalistas orientados a la inteligencia en ciberseguridad. Y es que en este sector se copia una barbaridad. Eso sí, muchos no lo hace bien y el ánimo que les mueve es francamente cortoplacista. En suma: que están en esto sólo por el dinero. Nosotros, no.

En Blueliv procuramos no perder nuestro foco, aquello en lo que somos buenos. Si bien es cierto que en el mercado de EE.UU. sí identificamos algunos competidores, hecho que no nos asusta. Aunque "pioneros" -como decía usted-, hemos sobrevivido a la aventura, estamos fuertes como empresa y nuestra tecnología es reconocida hoy por, entre otros analistas, Gartner.

– ¿Van directamente a usuario final o mediante intermediario?

– Trabajamos de las dos maneras. Normalmente, operamos directamente con clientes muy grandes, que tienen suficientes capacidades; en aquellas organizaciones que no las tienen, y cuya operación de la ciberseguridad está externalizada, las relaciones son con el externalizador.

Sucede que aunque nuestro foco originario es el de la prevención, las circunstancias nos están llevando a trabajar el remedio, porque con el paso del tiempo,

"Blueliv facilita al usuario corporativo la visibilidad de Internet y el análisis de las amenazas de su interés. A partir de aquí lo apoya para que pueda ir creando su propia ciberinteligencia".

nuestra información de inteligencia incorpora el valor necesario para esta otra parte de la ciberseguridad.

– **Internamente en el usuario, ¿quiénes son sus clientes?**

– Tradicionalmente hemos ido al CISO; pero desde hace algún tiempo tenemos demanda de los departamentos de prevención de fraude, de auditoría, de prospectiva de mercados, de seguridad corporativa… En todos los casos, nuestra Plataforma es la misma, lo que cambia es cómo la usa el cliente.

– **¿Han tenido casos en los que usando la tecnología de Blueliv alguna organización haya podido prever un ataque con antelación suficiente para poder actuar?**

– Sí; lamentablemente no puedo referenciar nombres de entidades, pero al poder detectar la actividad de captación de información de alguna *botnets*, hemos podido ayudar a frenar los efectos de algunos caballos de Troya bancarios, por ejemplo Dridex o Vawtrak. Cierto es que los delincuentes están al tanto de los avisos y toman sus medidas; pero si la información la proporcionas de modo rápido y continuado, aunque disponen de una industria bien engrasada y con los servicios de externalización y pago por uso a la última, no son infalibles.

Fíjese que en una ocasión nos llamó una gran agencia gubernamental de un país para indicarnos que tras liberar uno de nuestros informes habíamos estado a punto de dar al traste con una investigación suya en curso. Uno nunca sabe…

Sea como fuere, de lo que se trata es de facilitar información fiable, rápida, correlacionada y contextualizada para que se pueda saber por dónde puede venir el ataque. Y si ello no fuera posible, para saber en qué frentes está trabajando la delincuencia y como.

– **¿Tienen ya una taxonomía evolutiva de la delincuencia?**

– Dicho de un modo fino, los delincuentes son muy listos y cada vez son mejores en lo suyo. Explotan todo tipo de negocios: contratación de ciberataques, tráfico de datos, compraventa de tarjetas de crédito, productos mixtos… Y pueden poner esto en valor en sí o para adosarlo en otras actividades que asustan más: contratación de sicarios, ajustes, secuestros… Hay bandas bien organizadas, implantadas en países en los que tienen impunidad, que dominan bien las posibilidades del ciberespacio, y que mueven grandes cantidades de dinero. Para mi una de las grandes amenazas que está latente hoy es la del tráfico de capitales utilizando criptomonedas como bitcoin.

Y, además, "contratan" a chavales con interés en hacer I+D+i, cuyos trabajos sirven para desplegar *botnets*, encontrar y explotar 0-Days,… Algunos de estos jóvenes trabajan para los buenos y para los malos a la vez. Los hay que trabajan para gobiernos. También los hay que solo trabajan para los buenos en operaciones que les parecen asumibles desde la perspectiva ética.

– **¿Cómo podemos hablar de colaboración en un mercado en el que se considera la información sobre amenazas como una ventaja competitiva, al menos en una cierta ventana de tiempo?**

– Tengo claro que hay que colaborar facilitando de modo desinteresado información. Hay algunas iniciativas entre fabricantes, pero no óptimas. Si se centraliza la información en un organismo público, ello puede despertar susceptibilidades en países y mercados; si se hace en una organización privada, algunos pensarán que esta podría utilizar los datos en su provecho; si se hacen silos sectoriales, volvemos al pasado…

Por otra parte, los delincuentes son maestros en saltarse la ley. Si encima estas dejan mucho que desear y no están armonizadas nacional e internacionalmente, la labor policial parte de una mala posición. Sin duda, aunque las leyes se afinen, hoy por hoy la única manera de hacer frente a la ciberdelincuencia con éxito es la colaboración económicamente desinteresada. Desde luego, las multas, no.

– **Comentaba usted antes que una de las amenazas que le parecen más preocupantes es la relacionada con el tráfico ilegal de capitales mediante criptomoneda. No será la única**.

– Creo que la ciberextorsión va a ir en aumento, ya a empresas, ya a gobiernos, sea perpetrada por hacktivistas o por gobiernos enemigos.

Para luchar contra esto hay que tener buena información, de modo rápido y lo más importante, contextualizada. Hay que tener medios humanos y materiales para analizar los datos y extraer conclusiones de valor en tiempo útil.

Por eso cuando veo los excesos verbales que en algunos ámbitos del sector de TIC y de seguridad TIC se está cometiendo con el big data, me enfado. Lo que se ofrece es empachar de datos al usuario, que le salgan los datos por las orejas. Clásico de una informática caduca y metida en sí misma. Necesitamos analizar los datos, no procesarlos. Y aquí van a jugar un papel determinante los analistas de datos, actualmente muy escasos. Y los que hemos tenido en España, ciertamente pioneros, en su mayoría se han marchado a otros mercados.

Nosotros detectamos la necesidad de incorporar a los equipos de análisis a profesionales de otras disciplinas, como por ejemplo documentalistas, que son esenciales para clasificar. Obviamente, tam-

"En breve incorporaremos un nuevo inversor en el capital de Blueliv, seguramente extranjero. Obviamente, hemos tenido varias ofertas de compra, aunque no las contemplamos como opción, de momento".

bién se van a necesitar otros expertos con conocimientos en investigación de conductas.

– ¿Por qué decidió dar entrada a inversores en Blueliv?

– Nuestro objetivo era ser globales. Y eso requiere obligadamente dar entrada a compañías que te puedan ayudar a abrir mercados, a mejorar la tecnología y a poner en relación tu tecnología con otras complementarias… En breve incorporaremos un nuevo inversor en el capital de Blueliv, seguramente extranjero. Obviamente, hemos tenido varias ofertas de compra, aunque no las contemplamos como opción, de momento.

– ¿En qué mejoras y nuevos frentes tecnológicos están trabajando?

– Principalmente en cuatro frentes: desarrollar nuestro modelo colaborativo, tanto interempresarial como intraempresarial; perfeccionar nuestras capacidades predictivas; dar a nuestra Plataforma la capacidad de crear nuevas aplicaciones en campos en los que nosotros no tenemos experiencia, pero sí nuestros *partners*; y en la explotación de la información de una forma global y colaborativa mediante fuentes externas e internas para su aplicación en la defensa preventiva del perímetro.

– ¿Qué opina de la organización de la Ciberseguridad Nacional y de la legislación comunitaria y española?

– Convendría unificar criterios, no hacer cien veces la misma cosa en todos los ámbitos. En lo que se refiere a la PIC y la Directiva NIS, y al RGPD, aunque yo no sea jurista creo estar en condiciones de afirmar que es necesario armonizar los distintos sabores de la ciberseguridad y de la privacidad.

También convendría saber si la ciberseguridad privada tendrá alguna vez en España algún estatus como sector, más allá de ser considerara una actividad compatible con la Seguridad Privada.

– ¿Qué opinión le merecen las iniciativas públicas que se están haciendo en España para fomentar el emprendimiento en ciberseguridad?

– Algunas las veo positivas, porque están creando ecosistema. El ministerio de Industria está desarrollando algunas acciones brillantes, aunque como crítica diré que siguen siendo muy burocráticas, y con ello se está primando –seguramente sin quererlo– a aquellos que tienen alguna experiencia empresarial previa. Pero confío en que cada vez se afinará más.

Donde no hemos avanzado es el modelo de colaboración entre gobierno, empresas y universidades/centros de investigación. Las previsiones hablan de que vamos a necesitar miles y miles de expertos en ciberseguridad con experiencia. Me temo que con el atractivo profesional que tiene España, se irán fuera.

Una cosa hay que tener en cuenta también: aunque necesitemos ingenieros en grandes cantidades, en la ciberseguridad nos vamos a ver obligados a incorporar perfiles de Humanidades. Ya le mencionaba antes la necesidad de documentalistas. ¿Quién puede clasificar la información mejor que ellos? También requeriremos los servicios de geógrafos, de sociólogos, de filósofos que den fundamento ético a lo que hacemos… No olvidemos que los expertos en ciberseguridad somos un arma en potencia. ¿Se imagina que algunos gobiernos quieran contratarnos?

Y hablo de ciberseguridad, aunque este asunto la trascienda, porque estamos inaugurando la era del dato. Aunque a los analistas de datos les debería servir, y mucho, la filosofía hacker.

– ¡Analistas de datos! ¿Conoce usted alguno?

– Desde luego hay pocos profesionales en condiciones de dar lo que realmente requiere ese perfil. A medida que el mundo se digitaliza y va tomando cuerpo la inteligencia artificial necesitaremos realizar análisis en clave de interpretación social para contextualizar la información. En realidad, no me gusta hablar del analista de datos, sino de los equipos de análisis de datos.

La sociedad que integre antes y mejor esta realidad en sus ciclos de enseñanza, de mercado y de I+D+i, tendrá notables ventajas.

– Supongo que antes de esto tendrán que cambiar algunas cosas y venir otras…

– Claro está: la IoT, la explosión del uso de drones, las ciudades inteligentes, las nuevas fórmulas de *scoring* de entidades de todo sector y en cualquier ámbito… Todo ello requiere analítica de datos y ciberseguridad colaborativa.

– ¿Comercian ustedes con 0-Days?

– Ni los buscamos ni los compramos ni los vendemos. Cuando hemos tenido conocimiento de alguna vulnerabilidad no documentada, la hemos reportado siguiendo las mejores prácticas. Hay grupos que han hecho y hacen dinero en este mercado. Yo creo que esta actividad favorece más al cibercrimen que a quienes respetamos la ley.

– Una última pregunta: ¿trabajaría usted hoy para las estructuras de ciberseguridad chinas o rusas?

– No. ■

"Tradicionalmente hemos ido al CISO; pero desde hace tiempo tenemos demanda de los departamentos de prevención de fraude, de auditoría, de prospectiva de mercados, de seguridad corporativa… En todos los casos, nuestra Plataforma es la misma, lo que cambia es cómo la usa el cliente".