ESPAÑA Y LA CIBERSEGURIDAD: HORA DE REMANGARSE

LUIS FERNÁNDEZ DELGADO
Revista SIC

Quién esto escribe ha estado involucrado en lo que hoy genéricamente se denomina Ciberseguridad desde hace ya la friolera de 27 años, fecha en que la revista de la que desde entonces tengo el honor de ser su editor, se asomó al panorama español para abordar, informar y formar a los concernidos en una especialidad cuyo corpus iría generando de forma imparable sucesivas especialidades para acabar erigiéndose en pilar nuclear de la sociedad digital que estamos intentando construir hoy. Por entonces, recién estrenada la década final del siglo pasado, esta exótica temática estaba en sus albores; sus más precoces protagonistas asomaban la cabeza con cantos a la necesaria disponibilidad de los armatostes computacionales alojados en CPDs bajo su custodia y gestión mientras que los hallazgos criptográficos en fértiles escenarios académicos y universitarios presagiaban una era dorada para la disciplina.

INTRODUCCIÓN

Casi tres décadas después la ciberseguridad se ha imbricado en el ADN de la sociedad, siendo cómplice de su destino, para lo bueno y lo malo, y en lo que concierne a nuestro país, cabe preguntarse en estas primeras bocanadas del nuevo siglo qué papel están en disposición de jugar los diversos actores públicos y privados en este ámbito, y qué cabe esperar de las fuerzas contrarias que, valiéndose de una dimensión perennemente inestable, legalmente desestructurada y alegal en muchos frentes, como es el entramado de Internet, se sirven de él para exprimir y saquear el fértil valle del ciberespacio.

Con este panorama en mente, en las siguientes páginas se ofrece un repaso al contexto internacional y su devenir en el desarrollo del mercado español, se hacen breves referencias a tiempos pretéritos conducentes al hoy, al tiempo que se toma el pulso a la situación actual del sector, favorablemente condicionada por la pujante coyuntura internacional del mercado y la imparable inmersión de la sociedad en una transformación frágil necesitada de custodia y acompañamiento por parte de unas empresas que, en el caso de las de ciberseguridad en España, protagonizan un esperanzador futuro si bien no pocas de ellas aún precisan de un mayor apoyo, afianzamiento y consolidación.

CONTEXTO

En estos primeros compases del siglo XXI, España, como el resto de países de su entorno que gozan de la per-

FIGURA 1
GASTO EN SEGURIDAD A NIVEL MUNDIAL POR SEGMENTO 2017-2019

GASTO EN CIBERSEGURIDAD A NIVEL MUNDIAL POR SEGMENTO 2017-2019*

SEGMENTO DE MERCADO	2017	2018	2019
Seguridad de Aplicaciones	2.434	2.742	3.003
Seguridad en la Nube	185	304	459
Seguridad de Datos	2.563	3.063	3.524
Gestión de Identidades y Accesos (IAM)	8.823	9.768	10.578
Protección de Infraestructuras	12.583	14.106	15.337
Gestión Integral del Riesgo	3.949	4.347	4.712
Equipos de Seguridad de Red	10.911	12.427	13.321
Otros Software de Seguridad de la Información	1.832	2.079	2.285
Servicios de Seguridad	52.315	58.920	64.237
Software de Seguridad de Consumo	5.948	6.395	6.661
Total	101.544	114.152	124.116

* En millones de dólares americanos

Fuente: Gartner

tinente soltura digital, se halla inmersa en un proceso de imparable, y cabe prever que, también, inexorable transformación. Luego de superar una lesiva crisis que durante casi una década minó su próspero latir y descuadernó buena parte de sus estructuras industriales y laborales, parece estar volviendo a velocidad de crucero a la senda de la recuperación y la prosperidad.

Con todo, estos últimos dos lustros han puesto patas arriba los clásicos pilares que convencionalmente han venido sustentando a la sociedad de nuestro entorno. No quiere ello decir que han desaparecido, pero sí que han visto como se les sumaba un compañero de viaje que ha alborotado su tranquilo discurrir. Como es lógico deducir, me refiero a la eclosión de una internet masiva, causante última en su poliédrico uso de una digitalización inevitable del latir de la sociedad. Así, junto a un boyantísimo turismo (quizá irrealmente próspero en lo cuantitativo por haber parasitado tanto destinatario refractario de otros destinos demasiado inestables) y a los suculentos beneficios de las exportaciones derivados de la valiente héjira del empresariado español en su salida a los mercados exteriores, España se encuentra hoy en la tesitura de llegar, o no, tarde al futuro. Un futuro que será, o no será, en razón a cómo de digitalizable consiga revestirse en las próximas décadas; ello, naturalmente, sin descuidar sus fuerzas tractoras tradicionales, que hasta ahora han venido propiciando su dinámica y holgada prosperidad.

Lo cierto es que, junto a la notable –aunque reducida– pléyade de primorosas macroempresas de bandera españolas (financieras, textiles, energéticas, infraestructuras, de distribución…) tan resultonas ellas en los rankings internacionales, coexisten también unos escasos centenares de compañías de rango medio junto a algo más de tres millones de microempresas y pequeñas empresas. Y, conviene señalar, que este último colectivo constituye la auténtica columna vertebral de nuestro país. Un colectivo, que, no cabe olvidar, sabe hacer con soltura lo que ha hecho toda la vida, no así en cambio eso de auparse al devenir digital, que puede hacérsele muy cuesta arriba por su de natural resistencia a los cambios.

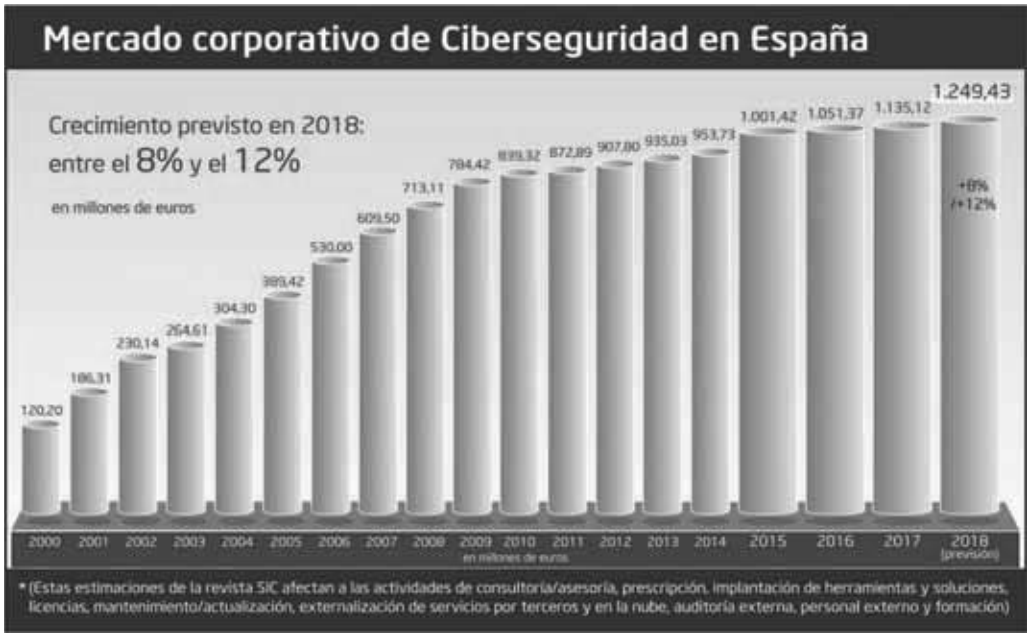
En esta tesitura, sin duda disruptiva por el alboroto de una sociedad digital desajustada en sus primeros albores de construcción, resulta que por narices hay que subirse al carro de la modernización e incorporar los 'nuevos modos' de una transformación que, paradójicamente, se ve abocada a tomar un sendero abrupto, bacheado y, lo que es peor, pésimamente señalizado, para abrirse paso hacia el futuro.

Así, junto a la cautela de embarcarse en un mar huérfano de buenas cartas de navegación, soplan además otros vientos de inquietantes augurios, cuales son los causados por la desconfianza social ante los embates de un océano digital plagado de filibusteros ansiosos por hacerse con botines de toda índole, por mercar abusivamente con la privacidad de sus bienintencionados y legos navegantes, por evidenciar severas lagunas legales e incluso para desestabilizar estados. Es en este contexto donde la ciberseguridad y sus actores adquieren un protagonismo crítico en su necesaria contribución a dotar de los mimbres necesarios para poder construir un entramado solvente en el que extender al ciberespacio el normal deambular de la sociedad.

LLEGAR PARA QUEDARSE

Como ya se mencionó en las primeras líneas de este artículo, lo que hoy se entiende por ciberseguridad tiene ya un apreciable recorrido a sus espaldas; en concreto y de manera masivamente creciente, ha venido dando forma a su polifacética actividad en la última treintena de años.

FIGURA 2
MERCADO CORPORATIVO DE CIBERSEGURIDAD EN ESPAÑA



Fuente: SIC

Este hecho no es únicamente aplicable a los países embrionarios de la computación, sino que, además, sus efectos también aterrizaron a no mucho tardar en destinos como el nuestro, una España que ya desde finales de los setenta del siglo pasado comenzaba a proveerse de sus primeros ordenadores y cuyos madrugadores especialistas académicos y en criptografía, iniciaban sus fructíferas trayectorias.

EL MERCADO DE LA CIBERSEGURIDAD EN ESPAÑA

Según previsiones de Gartner, firma analista internacional mayormente centrada en el mundo de la tecnología y la computación, el gasto mundial en productos y servicios de seguridad de la información, supondrá en este 2018 un total de 114.000 millones de dólares, suponiendo un incremento porcentual del 12,4% respecto del año anterior, y previendo igualmente que para 2019 el aumento sea del 8,7%, alcanzándose los 124.000 millones de dólares.

De igual modo, según datos recabados por la Comisión Europea, el sector de la ciberseguridad viene registrando crecimientos superiores al 13% anual.

Estas cifras y porcentajes son claros indicadores de una más que saludable actividad del sector. El halagüeño panorama no es nuevo; desde hace ya dos décadas se vienen registrando elevados crecimientos, incluso de holgados dos dígitos de modo sostenido en el grueso del periodo, aun a pesar de sortear una crisis generalizada (aunque de impacto sectorial desigual).

El diagnóstico es perfectamente extrapolable al mercado español. Desde inicios de siglo nuestro mercado corporativo empresarial también ha demandado protección en modo creciente y los actores suministradores de dicha ciberseguridad han venido atendiendo esta necesidad con notables resultados. Así, y según el estudio que desde SIC venimos efectuando al colectivo de referencia que opera en España, a comienzos de 2000 el mercado suponía una facturación de 120,20 millones de euros, en tanto que para este 2018 se ha multiplicado por diez, previéndose alcanzar los 1.249,43 millones de € a finales de año, con un crecimiento promediado del orden del 12%, derivado de las actividades de auditoría/consultoría, prescripción, implantación de herramientas y soluciones, licencias, mantenimiento/actualización/suscripción, externalización de servicios por terceros y en la nube, auditoría externa, personal externo y formación. A ello debe sumarse el potente empujón adicional, mayormente en servicios de consultoría, derivado de una atropellada adaptación a última hora al Reglamento General de Protección de Datos (RGPD).

Estos saludables guarismos vienen refrendados también por el Instituto Nacional de Ciberseguridad (INCIBE), quien en sus estimaciones no difiere en demasía de los de SIC y calcula que en España la actividad supone unos 1.200 millones de euros.

Ejemplos de éxitos de alcance internacional

El buen hacer de nuestras primeras compañías, reducido en número pero no en la calidad de desempeño, se viene constatando con creciente notoriedad. Así y a modo de ejemplo, cabe reseñar dos noticias que dan buena cuenta de lo afirmado.

De un lado, es de destacar la trayectoria del Grupo Telefónica –y por derivada su unidad específica Eleven-Paths–, que a principios de siglo empezó a conformar la línea de Ciberseguridad, y ya dispone hoy día de 16 CSIRTs ubicados en sus diversas filiales erradicadas por el mundo, con cobertura de sol a sol. En 2017 facturó más de 428 millones de euros gracias a las partidas específicas de protección incluidas en sus servicios mega-externalización globales, a sus servicios propios desde la red –por ejemplo, de limpieza de tráfico o escudo antidenegación de servicio– y por servicios de ciberseguridad gestionada y de integración. A día de hoy la multinacional española acredita el liderazgo en el sector, disponiendo de más de 2.000 especialistas en el mundo y mismamente en el SOC de Madrid cuenta con 400 profesionales.

De la misma manera, y ya con la vista focalizada en demarcaciones e impacto europeos, procede celebrar el proyecto ganado por la multinacional tecnológica GMV, anunciado también en septiembre pasado, por el que resultó adjudicataria de un gran contrato con la Agencia Espacial Europea (ESA) para el mantenimiento y evolución del Segmento de Control en Tierra de Galileo (*Galileo Ground Control Segment* o GCS), el sistema global de navegación por satélite europeo, auténtico buque insignia de la creciente actividad espacial de la Unión Europea. El contrato marco suscrito por GMV con la ESA tiene una envolvente presupuestaria de 250M€ e incluye la contratación en firme de la primera Orden de Trabajo por un importe en torno a los 150M€. Se trata sin duda del mayor contrato firmado por GMV en su historia, además de ser el mayor contrato firmado por la industria espacial española. Según lo previsto, GMV liderará en el proyecto un equipo en el que el 60% del trabajo lo realizarán empresas españolas, y dará empleo directo a unas 200 personas.

En la actualidad, GMV, nacida hace casi 35 años y con más de 1.800 empleados y sedes en diez países, es el primer proveedor independiente del mundo de Sistemas de Control en Tierra para operadores de satélites comerciales de telecomunicaciones y líder europeo en el Segmento de Tierra de Sistemas de Navegación (EGNOS y Galileo); el principal proveedor de sistemas de mando y control C4I del Ejército de Tierra español; el primer proveedor en España de sistemas telemáticos para el transporte público. Y, además, en el sector TIC se ha constituido desde finales del siglo pasado en referente como proveedor de soluciones y servicios avanzados de Ciberseguridad en redes IP, aplicaciones de movilidad y aplicaciones TICs para las Administraciones Públicas y el desarrollo de la e-Administración. Precisamente, la parcela de la protección es algo crítico en el proyecto satelital, por lo que la necesidad de *expertise* en este área es determinante. Se calcula que esta parcela podría rondar la treintena de millones de euros y una demanda de especialistas que excede la cincuentena.

COMPOSICIÓN DEL MERCADO ESPAÑOL OFERENTE

A día de hoy y en España, grosso modo, el mercado de la ciberseguridad empresarial lo protagonizan algo más de 100 compañías, las cuales ya exclusivamente o con foco intenso, atienden los diversos frentes demandados.

Genéricamente, el ecosistema lo conforman tres actores oferentes: los mayoristas, los consultores/integradores y los fabricantes, quienes entre todos interactúan –no siempre fluidamente– para en último término dirigirse al usuario final (las empresas y entidades demandantes) y proporcionarles la ciberseguridad solicitada. A este trípode sustentador del mercado ha venido a sumarse un actor de creciente protagonismo: el proveedor de servicios, destinado inexorablemente a acaparar buena parte de la clientela y del pastel.

Los mayoristas

El colectivo de los mayoristas aglutina la distribución de las tecnologías punteras y de última generación, en su mayoría procedentes de los dos mercados suministradores con más peso: Estados Unidos e Israel; en tercer lugar se sitúan las soluciones y herramientas gestadas en la Unión Europea, y por último, las desarrolladas en España por un reducido pero solvente grupo de compañías.

Estas empresas distribuidoras, cuyos principales actores son las multinacionales Exclusive Networks, Arrow ECS, Westcon y GTI Netxwave, se reparten el mercado junto con mayoristas locales tales como Ajoomal, Lidera o Ingecom, entre otros, conformando un tejido que representa cerca del 80% del total. El restante 20% interactúa ya directamente ya a través de acuerdos específicos con empresas prescriptoras e integradoras.

Las empresas mayoristas, pese a su notable vitalidad, sufren en la actualidad ciertos cuestionamientos por sus dificultades en conferir mayor valor a sus actividades (con la sombra de la aún incomprendida y atragantada computación en la nube sobre sus cabezas) más allá de la obvia representatividad tecnológica y de sus capacidades de provisión de financiación. Con todo, a día de hoy son indiscutibles actores de intermediación y canalizan muy saludablemente un plantel estelar de marcas de la ciberseguridad ((más de 50), entre las que cabe mencionar a las referencias top como Check Point, McAfee, Symantec, Fortinet, Palo Alto Networks o Kaspersky Lab.

Los consultores e integradores

Nuestro sector, el de la ciberseguridad, presenta algunos rasgos distintivos frente al resto de compañías prestatarias de servicios de consultoría e integración dedicados a atender los temas genéricos asociados a la implantación y/o la gestión de las Tecnologías de la Información y las Comunicaciones –coloquialmente llamadas TIC– y es que precisan un personal tan extremadamente especializado y su ciclo de comercialización, venta y, si procede, de ulterior gestión, es tan notablemente complejo y no cortoplacista –característica esta aplicable a la gran mayoría de otros productos, herramientas y soluciones que inundan el mercado– que históricamente solo un reducido número de empresas han apostado por conformar una plena dedicación al asunto –juga-

dores puros– o, al menos, a 'armar' unidades especializadas con profundo foco en la ciberseguridad.

Así, resulta habitual constatar que las más importantes compañías de integración manifiesten una acusada miopía mercantil en esta materia, adoleciendo de la experiencia y el personal necesarios para lanzarse a competir con garantías en el mercado haciendo gala de una resultona apuesta en sus catálogos al incluir la seguridad TIC. Este anormal comportamiento ha provocado por contra el sólido posicionamiento de una docena larga de compañías de solvente 'savoir faire', que han aprovechado la carencias de sus 'mayores' –abocadas a subcontratar cuando no queda más remedio– para hacerse acreedoras de la máxima confianza incluso en clientes de gran tamaño –multinacionales españolas incluidas– que en otras circunstancias no se hubieran decantado por estos 'especialistas' de nicho.

En lo respecta a la consultoría y prescripción, el panorama no difiere del hallado en otros países de nuestro entorno. Los grandes jugadores transnacionales logran obtener también en España una muy significativa cuota de mercado: las denominadas *big four* clásicas de la auditoría y la consultoría (Deloitte, EY, KPMG y PwC), así como Accenture y otras empresas de ese perfil, disponen de unidades de riesgos y ciberseguridad compuestas por centenares de especialistas, para dar respuesta a una demanda que, hoy día, es casi imposible de atender debido a la alarmante escasez de expertos derivada de adosar de forma inexorable la ciberseguridad a cuanto proceso de transformación digital y de Industria 4.O es puesto en marcha, y, al tiempo, para dar respuesta a la mayor demanda de privacidad (DPOs incluidos) y al cumplimiento regulatorio (*compliance*), azuzados por el torrente legislativo y normativo concernidos: RGPD, Directivas NIS e EiDOS, etc.

Dentro de este último segmento, en lo relativo a la privacidad y los datos personales, las compañías de consultoría, abogacía digital y formación han experimentado una febril actividad para atender los plazos derivados del RGPD en sus clientes. Como cabía prever, y entroncando con el habitual carácter mediterráneo de no actuar hasta última hora, la avalancha de peticiones ha desbordado la capacidad de atender esta necesidad y aún hoy el grueso del empresariado español continúa con los deberes sin hacer. Según manifiestan algunas de las principales compañías centradas en prestar estos servicios, dicen haber experimentado crecimientos de entre un 15% y un 20% adicionales en sus unidades específicas.

Los proveedores de servicios

Como enfáticamente han venido alertando Gartner y otras firmas analistas especializadas en TIC (Forrester, Ponemon, Frost & Sullivan, IDC…), la imparable proliferación y crecimiento de los denominados Proveedores de Servicios de Ciberseguridad (MSSPs), viene dadas por algunos factores claramente determinantes de su creciente adopción y pujanza:

- Menores presupuestos y personal especializado.
- Adopción de complejas tecnologías de ciberseguridad y herramientas analíticas para prevenir, identificar y responder a ataques avanzados.
- Incremento en la adopción de servicios basados en la nube.
- Evolución de los informes de control y cumplimiento de regulaciones.

Teniendo en cuenta el hecho de que la mayoría de las empresas ya no puede defender a solas y con garantías sus infraestructuras y su información por razones de eficiencia y rentabilidad, y de que la externalización de la ciberseguridad se ha convertido en un elemento común, se está viviendo una intensa proliferación de la oferta que ha causado la aparición de numerosos proveedores de servicio, los cuales se han sumado a esta tendencia, detectándola como la más provechosa y, en parte, como el único camino para seguir evolucionando en un mercado que cada día se ha de enfrentar a nuevos retos.

Pero no todos han cruzado las –cada vez más– amplias puertas que llevan a la condición de MSSP del mismo modo. Las capacidades, el 'expertise', la situación geográfica e incluso la naturaleza de los servicios que prestan les diferencian, puesto que no es lo mismo una operadora con presencia internacional y propietaria de infraestructura de red, que un integrador que haya aunado las tecnologías de algunos fabricantes para ofrecer servicios a su cartera de clientes, o una de las 'cuatro grandes' clásicas o de nuevo cuño (Amazon, Google…).

El mercado de MSSPs en España

En este escenario y actividad concretos, satisface recordar que nuestro país ha sido pionero en la provisión de algunos servicios específicos de ciberseguridad gestionada desde Centros de Operaciones de Ciberseguridad (*Security Operations Center-SOC*), un mercado que se inició hace más de década y media de la mano de compañías como la española GMV Soluciones Globales Internet, SIA, S21Sec (hoy en manos del grupo portugués Sonae y fusionada con Nextel S.A.) y algo posteriormente Ecija y Telefónica. A ellos se fueron sumando actores como Accenture, IBM, Iecisa o Atos, que jugaban en el terreno más general de la externalización total o parcial de la función de TIC y que, por tanto, prestaban a tenor de esta circunstancia atención a la ciberseguridad en el marco de sus contratos.

Casi simultáneamente aparecieron otros proveedores con SOC como Innotec System (Grupo Entelgy), las antaño competitivas Unitronics y Oesía, algunos integradores clásicos de tecnologías que ofrecían gestión de dispositivos de red, ciertos fabricantes con línea de servicios, como Symantec, y algún significado mayorista cuya iniciativa para pymes no prosperó.

Ya desde hace tiempo desembarcaron en este mercado actores relevantes, desde la clásica referencia nacional en servicios tecnológicos Indra-Minsait, la *big four* Deloitte –que cuenta con ciberSOC y academia relacionada, y ha exportado con gran éxito mundial desde España su idea de prestación generada aquí–, HP Enterprise, DXC Technology y BT –con Centros de Operaciones de Seguridad en nuestro país integrados en sus redes mundiales de SOCs–, hasta compañías como la española S2 Grupo –pionera en la ciberseguridad orientada a los entornos industriales, aunque atienda también a otros ámbitos más generales–, Mnemo –que ya se está abriendo camino en este segmento en el mercado ibérico–, Aiuken –un proveedor muy especializado que va ganando mercado, con especial énfasis en Oriente Medio e Iberoamérica (como curiosidad es la única empresa de ciberseguridad española entre las 1000 con mayor crecimiento según Financial Times/Statista–, Prosegur Ciberseguridad –que dispone de SOC y capitaliza información diferencial derivada de la actividad central de su empresa madre–, y Necsia -que supo traerse para Barcelona hace ahora dos años la sede de Proficio de cara a su cobertura de los mercados europeos-. A ellos hay que sumar otros actores clásicos de la externalización generalista como T-Systems o Fujitsu, que evidencian en estos últimos tiempos una mayor apuesta expansiva por la captación más allá de sus habituales clientes por servicios estándar TIC.

Ya en este mismo año, un integrador de alcance mundial como es Capgemini ha decidido instalar en Asturias su SOC con cobertura especializada de amenazas relacionadas con procesos industriales y la nube, y desde Valencia Sothis, integrador a punto de cumplir una década en consultoría tecnológica, anuncia su decidida apuesta por esta actividad, habiendo obtenido recientemente el ingreso en CSIRT.es

También otras empresas están sopesando dar el paso y desembarcar al fin en este mercado. Entre estos posibles *new players* no resulta difícil imaginar la llegada o el movimiento de ficha de operadores competidores, decididos a importar los exitosos y jugosos 'savoir faire' de sus nodrizas británicas, francesas y norteamericanas en estas materias. Con todo no será tarea sencilla posicionarse tras una miopía mercantil de lustros para con el mercado español.

Sin duda, las bazas de sus estrategias pasan por ofrecer los obligados servicios básicos a su clientela cautiva, pero realmente deberán hacer hincapié en otros muy exclusivos y completamente sectorizados, a la espera de que el crecimiento en el uso de la nube y cambios en la legislación pueda ampliar el caladero de clientes. Así, tal parece ser el caso de Orange, que en la edición de 2018 de Securmática anunció su intención de comercializar a través de su SOC 3.0 servicios avanzados de protección a sus redes y usuarios, proteger sus infraestructuras y defenderse de ataques y fraude interno.

Mientras tanto, los proveedores de proveedores de MSSPs (con foco muy específico, como la correlación avanzada, la vigilancia digital, la identidad como servicio e incluso fabricantes de productos de seguridad para red y nube…), estudian el impacto en sus negocios de ir directamente o no a proveer servicios al usuario final sirviéndose de sus propias infraestructuras, usualmente operativas desde la nube.

Principales servicios que ofrecen los MSSPs

El innegable aumento de la demanda de este tipo de externalización, con previsiones de crecimientos anuales en torno al 20% en algunos segmentos, no solo ha conllevado un incremento en el número de proveedores, sino también en su tipología, desde aquellos que prestan desde Centros de Operaciones de Ciberseguridad únicamente servicios generales básicos o parciales, a los que, una ver cubiertos estos servicios básicos por el mercado, se centran en los de nuevo cuño, definidos por la correlación avanzada, el análisis de inteligencia y la prospectiva como piezas clave (aquí entran el *big data* –macrodatos–, el *machine learning* –aprendizaje automatizado–…–, o los que lo aplican a ámbitos específicos, como los entornos industriales, las infraestructuras críticas, la sanidad-e, las ciudad inteligentes, la movilidad de vehículos o la lucha contra el fraude en sus diversas manifestaciones. Naturalmente, todo lo derivado a escenarios de nube demanda una atención significativa y cuyo crecimiento es ostensible e imparable, pese a las lógicas reticencias por mantener el control, supervisión y confidencialidad en la 'cloud' de sus activos de información.

A modo de resumen, desde los más básicos a los más sofisticados, en las siguientes líneas se mencionan los principales servicios incluidos en los catálogos de prestación de servicios de los MSSPs:

- Anti-malware en el puesto de trabajo
- Gestión de cortafuegos, cortafuegos multifunción (UTM), de nueva generación y WAF
- Gestión de sistemas de protección/detección de intrusiones (IDS)
- Filtrado de correo-e
- Anti DoS y DDoS
- Gestión de *logs*, monitorización y archivado
- SIEM
- Monitorización de aplicaciones web
- *Gateways* (mensajes y tráfico web)
- Inteligencia y engaño ante amenazas
- Detección y remediación de APTs
- DLP e IRM
- CASB
- Forensía digital

- *Pentesting*
- Servicios de Identidad y acceso como servicio
- DPO como servicio
- CISO como servicio
- Oficina de ciberseguridad
- Consultoría de cumplimiento, riesgo y gobierno
- Monitorización y detección de amenazas en entornos industriales
- Control, visibilidad y propiedad de datos en la nube

Soluciones y herramientas made in Spain

Históricamente, en España han emergido algunas compañías que con gran esfuerzo, voluntad y no siempre éxito, han probado fortuna desarrollando soluciones de ciberseguridad. La tipología es variadísima. Por nombrar algunas, desde las ya mentadas primeras soluciones antivirus de Anyware y Panda, pasando por los cifradores de Penta 3 y Realsec, los SIEMs Bitácora (gestado por Bankinter en conjunción con Telefonica y S21sec) y los evolucionados de AlientVault, ICA y Logtrust/Devo, protección de correo (Spamina), PKI (Safelayer), firma electrónica (Vintegris), aislamiento controlado (Randed), Contrainteligencia y Engaño (Countercraft), inteligencia modular y vigilancia digital (Blueliv), gestión de incidentes y amenazas (S2 Grupo, ITS) y un extenso etcétera.

QUÉ CIBERSEGURIDADES SE DEMANDAN (PRIVACIDAD INCLUIDA)

En otro reciente estudio de Gartner, en total sintonía con lo percibido en nuestro mercado, se reveló que los tres 'drivers' que espolearían el gasto en ciberseguridad vendrían dados por la existencia de mayores riesgos en la sociedad digital, por las nuevas necesidades del negocio y por los propios cambios en la industria, que junto al aspecto clave de la privacidad, se constituyen así en los principales dinamizadores del mercado. De hecho, la firma analista estima que el segmento de la privacidad y los datos personales –asunto este que a decir de SIC es inseparable y se enmarca en el más global de la ciberseguridad– representará al menos el 10% de la demanda de servicios de seguridad en 2019 y causará un severo impacto en una gran variedad de segmentos, como son los de gestión de la identidad y los accesos (*identity and access management*, IAM), el Gobierno y la Administración de la Identidad (*identity governance and administration, IGA*) y la prevención de pérdida y/o sustracción de datos (*data loss prevention, DLP*).

Por otro lado, en lo referente a la suscripción o gestión de servicios, se estima que supondrán al menos el 50% de la entrega de software de seguridad para 2020 y que la propia Seguridad como Servicio (*Security as a Service, SaaS*) se está imponiendo a los tradicionales despliegues en sede tecnológica corporativa (*on-premise*), con especial decantación a los despliegues híbridos. Igualmente, un elevado porcentaje de los respondientes a la encuesta de seguridad de Gartner manifestó su intención de desplegar, de aquí a dos años y en modo híbrido, tecnologías y soluciones específicas como pueden ser los sistemas gestores de eventos y de seguridad de la información (*security information and event management, SIEM*).

EL USUARIO SE LO HACE

Siquiera brevemente, es necesario hacer también mención especial a un colectivo de compañías usuarias de gran porte y muy consumidoras de ciberseguridad que, por su especial casuística, no puede ver satisfechas sus demandas de protección con lo que el mercado les ofrece y optan por proveerse ellos mismos además de la necesaria protección dotándose de recursos tecnológicos y humanos para tales fines.

Así sucede con algunas de nuestras multinacionales financieras y energéticas, las cuales reúnen en sus filas ingentes retahílas de especialistas para gestionar la ciberseguridad de sus activos transnacionales en instalaciones de propósito específico. Así, por ejemplo, ocurre con lo que será el nuevo centro SOC mundial del Grupo Santander, prevista su inauguración a finales de este año en su ciudad financiera ubicada en Madrid. Aglutinará nada menos que a varios centenares de especialistas y este hecho ha desestabilizado el mercado laboral español pues los atractivos puestos abiertos y jugosos salarios ofrecidos para su puesta en funcionamiento están provocando una alarmante escasez de talento para atender otras necesidades del mercado y del sector.

Prosiguiendo con estas decisiones que abocan al 'home made', la filial BBVA Next Technologies, empresa experta en ingeniería que impulsará la transformación tecnológica del banco matriz, arrancó el pasado junio. Cuenta para ello con expertos avanzados en análisis masivo y macrodatos, inteligencia artificial, cadena de bloques y, como no podía ser de otra manera, ciberseguridad, tecnologías y especialidades todas que ofrecen un gran potencial de disrupción. En lo concerniente al ámbito de la ciberseguridad, cuentan con el solvente equipo i4s (proveniente de la antigua Information 4 Security) por el que se ofrecerá la prestación de servicios profesionales de seguridad avanzada incluyendo soluciones de infraestructura y aplicaciones, desarrollo de soluciones software seguras y soluciones de ciberseguridad tanto para el Grupo BBVA como para empresas líderes.

A BUSCARSE LA VIDA Y ACELERAR

Nadie duda que los colosos oferentes en tecnologías y soluciones de ciberseguridad en el ámbito occidental son Estados Unidos e Israel. Ambas potencias acaparan el grueso del mercado, llevándose la parte del león y dejando únicamente migajas al resto, Europa incluida.

Aunque sea triste comentarlo, nuestra flamante unión continental ha venido mostrando en este asunto una atolondrada actitud no muy diferente a la de otros te-

mas neurálgicos que fisuran un proyecto europeo que no acaba de *'biencuajar'*, plagado de enfrentamientos entre sus integrantes y con serios temores de que esta falta de unidad impida conformar jugadores tecnológicos capaces de erigirse en una 'nueva esperanza' para competir de tú a tú frente a la 'galáctica' dominante.

Con todo, hace escasamente unos semanas el presidente francés Macron abogó por un mayor énfasis de nuestra soberanía y propugnó que la UE espabilara y asumiera, ante la tesitura actual, que su seguridad -en todos sus órdenes entendida- no dependiera de Estados Unidos. Este ideario suena bien y tal vez aboque a los atomizados actores europeos a redoblar los esfuerzos de entendimiento y eficiencia entre ellos y, por derivada, a recibir un más intenso apoyo y promoción de su tecnología frente a los acaparadores del mercado. Naturalmente, esto también aplica a la ciberseguridad.

Desenfoques aparte, nuestro mercado en sí anda agitadísimo en estos últimos tiempos. Un inusitado aluvión de compañías está protagonizando operaciones de compra, fusión y adquisición, además de que los fondos de inversión trasiegan desaforadamente con *startups* de nuevo, y no tan nuevo, cuño. Y como esta vez dicho trasiego sí concierne a actores españoles, es de justicia reseñarlo aquí.

Tradicionalmente, en nuestro país emprender nunca ha sido sencillo. Ni siquiera hoy, envolviéndose en la enseña tecnológica y bajo el moderno epíteto de 'startup', se sale fácilmente adelante. Con todo, pese a la escuálida sensibilidad histórica pública a este neurálgico indicador de apuesta por la competitividad y por lo propio frente a lo extranjero, parece que corren tiempos más favorables para los valientes que confían en su saber hacer y en su temerario desembarco en mercados de fuerte competencia dominados por un puñado de megacampeones de dilatado pedigrí.

Así, a nadie que transite por el sector se le escapa que el mercado de compañías españolas fabricantes y desarrolladoras de ciberseguridad es ciertamente modesto. En estas casi tres décadas de recorrido, únicamente ha emergido en nuestro país un reducido número de empresas en disposición de sobrevivir compitiendo decentemente y con garantías.

Érase que se era

Históricamente, la más madrugadora fue Anyware Seguridad Informática, cuyo atinado enfoque y cuota tentaron a Network Associates –hoy McAfee– que la engulló en 1998 por unos suculentos 10 millones de euros de entonces. Por aquellas también andaba Panda Software, quien rebautizada como Panda Security y tras no pocos avatares y sin sucumbir a la tentación –por el momento–, ha venido durando hasta hoy, momento en que exhibe una solvente y diferenciadora propuesta de protección, nube mediante.

Y justo en el año de despedida del siglo pasado también procede reseñar el nacimiento de Safelayer, ejemplar compañía fabricante de software de seguridad para PKI, firma-e y tecnologías concernidas de raíces universitarias que, a día de hoy, sigue mostrando una saludable vitalidad y apuesta por la innovación.

Ya desembarcados en el presente siglo, en sus primeros arranques no hubo muchos más hitos dignos de reseñar salvo el pelotazo protagonizado por la catalana PasswordBank, comprada por la todopoderosa Symantec por 21,4 millones de euros en 2013 para dotarse a sus soluciones de mejores características de entrada única (*single-sign on*) para comprobar la identidad de los usuarios, y el despegue de Blueliv, innovadora propuesta de inteligencia ante ciberamenazas fundada en 2009 y que aún en este pasado febrero recibió una nueva inyección –4 millones de euros– para proseguir su consistente expansión internacional.

Por su peculiaridad, también cabe mencionar lo sucedido a Epoche & Espri, una modesta empresa española de ensayos y evaluación con excelente soltura internacional, dedicada principalmente a las certificaciones Common Criteria (CC) –una metodología ampliamente reconocida para la evaluación de la seguridad de productos–, que fue adquirida en octubre de 2017 por el conglomerado empresarial alemán Dekra, la cual se hizo con el buen hacer, tras diez años de experiencia, en la evaluación y realización de ensayos conforme a estándares de seguridad reconocidos internacionalmente (tipo FIPS 140-2, ISO/IEC 19790, …).

Érase hoy

Este 2018 está siendo muy prolífico y favorable en operaciones que incumben a compañías de estos lares. Entre las relativas a captación de fondos, figura Countercraft con sus innovadores enfoques en contrainteligencia y que fue receptora a inicios de año de una nueva ronda de 2 millones de euros; otro tanto le sucedió a inicios de verano a Devo –nueva denominación de Logtrust–, que captó nada menos que 21,5 millones de euros para seguir proyectando su competitiva plataforma de recolección y analítica de datos.

Las operaciones más recientes

Por otro lado, AlienVault, de luengo recorrido con el *open source* por montera y con la indisimulada intención de atracar en EE.UU., acabó este verano en las fauces de la todopoderosa AT&T, operadora estadounidense que, según algunas fuentes, habría desembolsado cerca de 700 millones de euros por el proyecto iniciado en 2007 y se lanza ¡ahora! a la conformación de una unidad de servicios de ciberseguridad para ofrecerlos a su clientela.

Asimismo, otro movimiento estival que ha causado no poco revuelo en el mercado de nuestro país fue el anuncio de adquisición de Nextel S.A. por parte del brazo inversor tecnológico de Sonae, adicionándola a la ya adquirida en 2014, S21sec, con el propósito de conformar un potente y genuinamente puro campeón de la ciberseguridad –el mayor en la península– y la fir-

me ambición de codearse con sus grandes pares en Europa e Iberoamérica.

ACELERACIÓN PÚBLICA: MÁS VALE TARDE

En estas dos últimas décadas el apoyo público a la industria española da la ciberseguridad ha sido insignificante, por no decir inexistente en la mayor parte del tramo recorrido. Con honrosas pero mínimas excepciones (como el apoyo del CCN/CNI a determinadas tecnologías y soluciones por lógico interés de defensa nacional y de estado, mayormente vinculadas con la confidencialidad y en buena medida forzadas por la perentoria necesidad de tener que emplear herramientas acreditadas por los conocidos Criterios Comunes (Common Criteria) –por lo demás engorrosos e inasumiblemente caros para todas aquellas minipymes de ciberseguridad no sobradas de recursos en sus inicios–, poco más es de reseñar. Hasta hace bien poco.

Con todo, sí es de destacar la iniciativa Cybersecurity Ventures, un reciente esfuerzo por conformar un programa de aceleración internacional en ciberseguridad a instancias de INCIBE y la Junta de Castilla y León, a través del Instituto para la Competitividad Empresarial de Castilla y León y el Instituto Leonés de Desarrollo, Formación y Empleo, con el objetivo de incentivar el desarrollo de nuevas empresas de base tecnológica en el ámbito de la ciberseguridad, al tiempo que apoyar al talento emprendedor en la maduración de sus proyectos empresariales a través de la formación, mentorización y *networking* con inversores y talento emprendedor, contribuir al despliegue de la estrategia de Ciberseguridad en España vinculándola con los retos en la protección contemplados en el Programa y, por último, complementar la oferta de actividades promovidas por INCIBE como centro nacional de referencia en la materia.

Durante cuatro meses este programa de aceleración ofreció apoyo intensivo a las empresas finalistas (resultantes de una selección previa entre 74 candidatos presentados) El jurado de estos galardones –compuesto por representantes de fondos de inversión, grandes corporaciones e instituciones públicas–, falló en febrero pasado dando como ganadora de entre diez proyectos finalistas a la *startup* de reciente creación Smartfense, una plataforma en línea de capacitación y concienciación en seguridad de la información que, a través de contenidos atractivos permite generar comportamientos seguros en los usuarios de una organización. Obtuvo un premio de 34.000 euros. El segundo recayó en Dinoflux (consistente en 24.000 euros) en tanto que el tercero lo hizo en la iniciativa empresarial Kymatio (dotado con 20.000 euros).

Aunque en el bando privado tampoco es para echar cohetes, al menos algunas compañías, Telefónica por ejemplo, a través de sus fondos de inversión, ha inyectado nutrientes en *startups* de ilusionante recorrido como Blueliv, Countercraft, Devo y 4iQ. Más recientemente, a mediados de septiembre la firma de capital riesgo Adara Ventures inyectó 855.850 euros en HDiV Security, cuyos productos ayudan a desarrolladores y arquitectos de software a proteger aplicaciones web y APIs a través de la adopción de la filosofía de desarrollo DevSecOps, que incluye funcionalidades de protección (RASP) y detección (IAST).

El inhabitual caso de S2 Grupo

Como cierre al repaso de hechos asociados a la inversión en empresas españolas de ciberseguridad es muy de destacar que a comienzos del pasado septiembre se supo que la compañía pública SEPI Desarrollo Empresarial (SEPIDES) –empresa de la Sociedad Estatal de Participaciones Industriales– decidió aportar 3,5 millones de euros a la empresa valenciana S2 Grupo, ya mentada con anterioridad, con el objetivo de coadyuvar a impulsar su expansión internacional, iniciada hacía un tiempo aunque de forma tímida por mercados de la UE e Iberoamérica . Esta inusual y grata noticia para una de las compañías de referencia española rompe con el maleficio de la escuálida orfandad de este tipo de apoyo inversor por parte de las instituciones públicas en nuestro sector.

Abundando en ello, el Consejo asesor de S2 Grupo aprobó a finales de 2017, año en cuyo ejercicio facturó cerca de 12 millones de euros, su plantilla se situó en 230 expertos y creció un 12%, un ambicioso «plan estratégico 2018-2022» cuya finalidad es posicionarse como una de las principales compañías globales de ciberseguridad en los próximos cuatro años.

De cara al objetivo principal de su plan, la expansión internacional, la empresa tiene previsto, entre otras acciones, incrementar en los próximos años un 40% su plantilla actual incorporando un gran número de profesionales con un alto nivel de conocimiento y experiencia en el sector tecnológico, y también está prevista una fuerte inversión en el desarrollo de tecnología nacional de ciberseguridad, además de seguir invirtiendo fuertemente tanto en el desarrollo de nuevos productos como en el perfeccionamiento de los que ya posee.

Por su singularidad, conviene precisar que desde hace años, S2 grupo ha sido la empresa que, en cooperación con el Estado a través del Centro Criptológico Nacional (CCN), ha desarrollado herramientas que han sido claves para la defensa de las Administraciones Públicas y empresas estratégicas españolas (por ejemplo CARMEN, solución enfocada a identificar si una red de una organización ha sido «comprometida» por terceros por causas atribuidas a amenazas persistentes avanzadas (APT). Junto a este software, también desarrollaron conjuntamente GLORIA, una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos con el objetivo de perfeccionar la detección avanzada y minimización del impacto de cualquier tipo de acción por parte de ciberdelincuentes. Basada en los sistemas SIEM, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes que hay hasta el momento

Despedida, cierre y ... a remangarse

Con una nueva Estrategia Nacional de Ciberseguridad en ciernes, la Directiva NIS –del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea– y su vigente transposición a la legislación española asomando la patita y un RGPD causante de no pocos quebraderos de cabeza, tiene pinta de que a todos los concernidos con la ciberseguridad, sean españoles u operen en nuestro país, les aguardan momentos de alta intensidad. Ello implica que la totalidad de sus actores deben remangarse para salir con bien de este desafío.

Por otro parte, y como no podría ser de otra modo, en SIC nos congratulamos de las hazañas nada triviales de estos últimos tiempos, y muy especialmente las conseguidas en lo que va de año, por parte de las compañías españolas del sector y sus gestores, abocados a buscarse la vida en una jungla mercantil que no entiende de fronteras y cuya espesura digital paradójicamente también contribuyen a proteger.

Y aunque el apoyo público a nuestra industria aún sea sonrojantemente tímido en comparación al prestado a sus equiparables en naciones de nuestro entorno, cabe tener la esperanza de que el talento y la convicción de sus protagonistas acaben por persuadir a los dueños del dinero de que reenfoquen mejor sus esfuerzos inversores y lo destinen también a un segmento clave para la sociedad de nuestro porvenir cual es el de asentar la confianza digital a través de proyectos y compañías predispuestas a ello. Seguro que revierte.

BIBLIOGRAFÍA

Revista SIC
www.revistasic.com
Gartner
www.gartner.com
INCIBE
www.incibe.com
Estrategia Nacional de Ciberseguridad
www.dsn.gob.es/es/estrategias.../estrategias/estrategia-ciberseguridad-nacion
Directiva NIS
www.dsn.gob.es/es/actualidad/sala-prensa/publicacion-directiva-nis
RGPD
www.aepd.es/