facebook

twitter

newsbook.es

>> La revista del distribuidor informático

Newsbook

Año XXIV Nº 248 Abril 2018 0,01 Euros

La llave de la seguridad, en manos del mayorista

El negocio del canal mayorista crece por encima del ascenso del mercado en España

La seguridad sigue cotizando al alza en el canal

La seguridad sigue siendo un valor seguro en la bolsa en la que cotiza el negocio del canal mayorista. No cesan las amenazas, ni desciende su complejidad, y el panorama, donde lo digital es ya tiranía, está convirtiendo la seguridad en materia troncal de la estrategia de las empresas. El canal sigue a pie de obra del negocio. Un canal que, con el tiempo, ha visto cómo su papel iba mutando: su participación en el desarrollo de los servicios gestionados y el peso, creciente, que han ido cogiendo los fabricantes en el mercado. Junto a integradores y distribuidores permanece el canal mayorista que mantiene incólume su gusto por la seguridad. Arrow, Aryan Comunicaciones, Exclusive Networks, Ingram Micro, Tech Data, V-Valley y Westcon son sus miembros.

Ofrecer como referencia el crecimiento del 7 % en el mercado de la seguridad en España en 2017, que los fabricantes han dado por bueno, no es baremo suficiente para el canal mayorista. Los principales actores que conforman este escalón de la cadena aseguran que su crecimiento ha sido mayor. La variedad de los ataques, algunos de ellos con una enorme carga mediática, ha asegurado la inversión en torno a las tecnologías de protección. También la mejora de la situación económica (según datos del FMI, España creció un 3,1 % en 2107) ha repercutido en la bonanza general del segmento TI y, en particular, en el apartado de la seguridad.

Carmen Muñoz, directora general de Exclusive Networks en España y Portugal, entra en el detalle, asegurando que en el

caso del mayorista, han existido un número elevado de proyectos de refresco tecnológico de las infraestructuras de las compañías y se han reactivado áreas tan tradicionales como el *endpoint*, "con crecimientos muy vinculados con los ataques que se produjeron el año pasado y con el *ransomware*".

No cesan tampoco de crecer las áreas más tradicionales, como puede ser la protección del perímetro; pero junto a ellas cobran cada vez más relevancia la seguridad vinculada con la nube y los servicios gestionados desde ella. "La protección de las aplicaciones y de todo lo que tiene que ver con soluciones de SIEM, para detectar y predecir, de manera activa, los ataques y amenazas en las redes de las empresas, también han crecido", apunta Iñaki López, *country manager* de Arrow en España y Portugal.

Carmen Muñoz,
directora general de **Exclusive Networks** en España y Portugal

"Debemos convertir la adopción de las nuevas tecnologías en una oportunidad de negocio real"

La protección del dato ha sido objetivo prioritario. Alberto Gómez, *director enterprise security division* en V-Valley, asegura que hay una clara tendencia hacia la protección de la información. Conceptos como IRM *(Information Rights Management)* para controlar y proteger los archivos que se descargan desde listas o bibliotecas; o el siempre tradicional DLP *(Data Loss Prevention)* para asegurarse de que los empleados gestionan de manera adecuada los datos críticos, están de plena vigencia. "Las empresas ya tienen claras las medidas de seguridad en el perímetro y en el acceso a las aplicaciones; por lo que este año donde va a haber más oportunidades es en torno a la protección y el cifrado de información". También incide en la seguridad de la red. "El concepto NAC *(Network Access Control)*, que lleva sonando desde hace años, cobra cada vez más importancia. Saber qué pasa en la red y el acceso seguro a la misma desde el dispositivo es clave".

Por su vocación exclusiva en la pyme, Juan José Roncero, director comercial de la división de seguridad IP en Aryan Comunicaciones, reconoce que todavía hay mucho que hacer en el mercado de la pyme. "El mercado en este apartado está todavía por hacer". Roncero explica que este apartado crece, sobre todo en el área de la seguridad perimetral, y que muchas pymes han actualizado las soluciones de seguridad con las que contaban, lo que les ha permitido responder mejor a las nuevas amenazas. "Estamos orientando a nuestros distribuidores a desarrollar los servicios", explica. De cara a este año Roncero recuerda que va a ser clave el GDPR. "También la protección de las redes *wifi*, así como las soluciones MDM *(Mobile Device Management)* y la protección de aplicaciones móviles".

No podía faltar el término más en boga: la transformación digital. "Cuando una empresa se embarca en un proyecto digital, la seguridad debe estar muy bien cubierta. Incluye el manejo de las redes sociales, una mayor visibilidad para la empresa y contiene elementos de analítica y *machine learning* que incluye a la seguridad", explica Martín Trullas, director del área new *generation technologies* de Tech Data, que también índice en la fórmula de la seguridad como un servicio. "Cada vez hay más SOC que ofrecen este tipo de protección".

En definitiva, el crecimiento tiene que ver, como apunta Alberto Pascual, máximo responsable del negocio de valor de Ingram Micro, con que la cultura de seguridad se va implantando. "Las amenazas cibernéticas son ahora *trending topic*", arranca. "Hay una gran sensibilidad frente a los ciberataques; lo que hace que la ciberdefensa también esté creciendo". Corrobora el tema de los servicios que, a su juicio, es el área que más está creciendo. "Las pymes tienen muy difícil el acceso a determinadas soluciones y, sobre todo, a la metodología que permite su actualización continua. Muchas de ellas se decantan por soluciones mixtas, con un cortafuegos implantado, y externalizando el resto de servicios".

¿Crece o se reduce la brecha entre seguridad y ataques?

La creciente complejidad de las amenazas hace que mute también la tecnología encargada de detectarlas y detenerlas. Alejandro Soto, *sales manager* de Westcon Security, asegura que lo que marca el crecimiento de la seguridad es precisamente el rápido avance del *malware*. "En ocasiones, no alcanzamos su ritmo", asegura. Los vectores de ataque se

El "retorno" al puesto de trabajo

Tras "denostar", durante años, la protección del puesto de trabajo, las nuevas fórmulas que han adoptado los ciberdelincuentes, la popularización del *ransomware* y el hecho de que la mayoría de las APT se dirigen, fundamentalmente, a este entorno, ha provocado que las marcas hayan vuelto sus ojos y pongan un mayor énfasis en su protección.

"El gran reto es lograr que las compañías quieran invertir en una solución de *endpoint* de nueva generación sin que el factor precio sea el determinante", asegura Carmen Muñoz. Se trata de concienciarlas de que la inversión no se centra en el antivirus tradicional sino en soluciones de nueva generación. "Incluso las compañías que estaban centradas en el perímetro han evolucionado para contar con la solución completa, lo que ha reactivado el mercado".

Este despertar ha provocado que estas soluciones, incluso, sean bautizadas por Gartner: *new generation antivirus* (NGAV). "Comienzan a contar con un posicionamiento concreto porque aportan una mayor protección y, sobre todo, un menor consumo del *endpoint*", apunta Iñaki López.

El canal, lógicamente, no es ajeno. Alberto Gómez reconoce que incluso los integradores más tradicionales, que huían de los proyectos relacionados con el puesto de trabajo, están entrando en este entorno. "Forman parte de los proyectos globales de seguridad que abarcan desde el perímetro del *firewall* hasta el *endpoint*". Una oportunidad en la que los servicios ocupan un lugar predominante.

Como sucede con otros ámbitos, el atractivo negocio va a provocar muchos movimientos en forma de compras o alianzas. Martín Trullas recuerda que hay compañías tradicionales del mercado de la seguridad que están comprando empresas con soluciones de nueva generación en este apartado. Incluso hay fabricantes que solo están centrados en el endpoint. "Hay que decidir, por tanto, por quién se apuesta y por quién no".

Iñaki López,
director general de **Arrow** en España y Portugal

"Que el cliente pague un servicio en función de la demanda es la mejor opción. Esto marcará el futuro de la seguridad"

multiplican y, por tanto, los proyectos de seguridad encargados de detenerlos son mucho más complejos con un carácter multitecnología. A su juicio, la brecha entre la seguridad y los ataques ha crecido. "Se requiere más inteligencia, un conocimiento cada vez más amplio de las tecnologías y un diseño adecuado de las soluciones de seguridad, para alcanzar a los malos, que van a un ritmo más rápido", recomienda. No olvida el componente humano. "La inversión en talento técnico y tecnológico es prioritaria".

Un elemento en el coincide con Alberto Pascual. "La brecha sigue haciéndose mayor por la escasez de profesionales especializados en seguridad. Hay empresas que están tratando de resolverlo atrayendo al lado "bueno" a los *hackers*", corrobora. El responsable de Ingram Micro asegura que según un estudio sobre los CISO de grandes empresas en Reino Unido sus sueldos rondan el millón de euros al año, lo que deja claro tanto la escasez de la oferta como el valor que tiene uno bueno.

También Iñaki López reconoce que la brecha es mayor y apela a una de las técnicas más en boga para apuntalar que la situación no tiene visos de mejorar: la rápida monetización del *malware* y de los ataques gracias al uso de las cibermonedas. Junto a esta, Martín Trullas añade la industrialización de los ciberataques y la tendencia, cada vez más en boga, de la "oferta" del *malware* como servicio, al que se dedican compañías de maleantes especializados en su desarrollo. "Ya no solo afecta al dinero sino también a la imagen y a la reputación de las com-

ARROW

arrowecs.es

Leading **Security Solutions** distributor

Cybersecurity is essential in today's environment of hackers, malware, viruses, spyware and more.

Establishing a complete, *end-to-end* cyber security framework is critical to ensuring a **comprehensive, efficient, compliant and secure enterprise**.

Five Years Out

algosec · allot · aruba · Carbon Black. · Check Point · f5

FireEye · FORTINET · gemalto · GEMINI · HUAWEI · IBM Business Partner

Infoblox · ixia · MICRO FOCUS · NETSCOUT · Pulse Secure · radware

splunk> · swivelsecure · Symantec · TREND MICRO

ARROW ECS • Avenida de Europa, 21 Parque Empresarial La Moraleja • 28108 Alcobendas, Madrid
Tel. + 34 91 746 02 20 • marketing.ecs.es@arrow.com

Alberto Pascual,
director del negocio de valor de **Ingram Micro**

"Las amenazas cibernéticas son *trending topic*"

pañías: hacia ahí apuntan los ciberdelincuentes". El directivo de Tech Data alerta de otra práctica al alza: los ataques dirigidos contra los procesadores integrados en los servidores, que ha colocado en la diana del cibercrimen a los proveedores de servicios *cloud* que ofrecen servicio a un ramillete amplio de compañías. "La escalabilidad del daño es brutal", añade. "Se trata de dañar la imagen del mayor número de empresas a través del ataque a grandes centros de datos".

En la lista de recomendaciones para acortar la brecha, destaca la configuración de la solución, que debe estar muy por encima de la venta de un determinado producto o una marca concreta. "Cada vez cobra más sentido el concepto de seguridad conectada", recuerda Alberto Gómez. "Cuando se diseña un proyecto de seguridad todos los elementos de la red deben hablar entre sí y las soluciones de los distintos fabricantes que integran el proyecto deben entenderse; de lo contrario los proyectos ganan en complejidad y son muy difíciles de administrar".

Se prioriza, por tanto, automatizar la ciberseguridad. "Las marcas están condenadas a entenderse", insiste Alejandro Soto que, sin embargo, recuerda la paradoja que exhibe este entendimiento. "Uno de los pilares fundamentales de la ciberseguridad es la segmentación (cuánto más segmentado esté el entorno, más complicado resulta que los ciberataques tengan éxito); sin embargo el desarrollo de estándares que permiten la integración y la comunicación entre los diferentes elementos está yendo en contra de esta segmentación".

Carmen Muñoz no tiene claro qué tamaño tiene la brecha. "Los ataques siguen creciendo y cada vez son más complejos pero también hay cada vez más soluciones en el mercado", analiza. La directiva de Exclusive Networks asegura que el área de la se-

Ante una oferta fragmentada, ¿el mayorista armoniza?

La seguridad sigue siendo uno de los apartados con un panorama más fragmentado: multitud de opciones, de soluciones y de fabricantes, con una estrategia global o con soluciones específicas, conforman un caldo de cultivo que el mayorista debe cocinar de manera adecuada. "Debemos convertir la adopción de las nuevas tecnologías en una oportunidad de negocio real", resume Carmen Muñoz, que recuerda que el primer paso del integrador es definir dónde debe dirigir su inversión: en qué soluciones y en qué marcas. "Nuestro papel es clave, tanto para contribuir a su formación como para ayudarle a desarrollar el proyecto". A su juicio, la seguridad se está convirtiendo en un factor clave en la estrategia de negocio de las compañías. "Ya forma parte de sus decisiones de negocio; independientemente del tamaño de la empresa".

La combinación de la oferta y la integración que ofrece al canal, hace a cada mayorista único. "Se trata de interpretar la seguridad y brindársela al canal, a través de soluciones combinadas de diferentes marcas, que se apliquen a las necesidades concretas de sus clientes", explica Iñaki López. "Tenemos, además, un papel como formadores, con herramientas para transformar los productos de las marcas en soluciones y ayudar al canal a venderlo como un servicio".

El servicio. Clave siempre. Y más en el mercado de la pyme. Alberto Pascual asegura que la pyme se está inclinando por los servicios de seguridad gestionada. Muchas de ellas, además, están en pleno proceso de internacionalización, lo que exige coberturas 24x7, en cualquier parte del mundo. "Todo esto requiere un enorme coste para el integrador. Muchos de ellos son capaces de construir soluciones a medida, pero el coste en mantenerlas actualizadas es enorme. Y contar con un SOC propio es inasumible". La labor del mayorista se torna clave: facilitar el suministro de estos servicios, incluso con marca blanca, como es el caso de Ingram Micro.

EXCLUSIVE NETWORKS

EXCLUSIVE CAPITAL

paloalto NETWORKS

CYBERENTING

100% FREE
CHARGES FREE
100% FREE

AHORA TÚ TAMBIÉN PUEDES TENER UN FIREWALL DE ÚLTIMA GENERACIÓN.

Ante la evolución constante de las amenazas no tienen mucho sentido comprar tecnología cuyo ciclo de vida contable no se alinea con su ciclo de vida útil.

¡Utiliza pero no compres!

Exclusive Capital te ofrece el *best of breed* de la ciberseguridad en modo renting desde 70€/mes.

APP-ID | VISIBILIDAD Y CONTROL | PREVENCIÓN DE AMENAZAS | PROTECCIÓN CONTRA MALWARE | FILTRADO DE URL

ACTUALIZATE CON LA MEJOR TECNOLOGÍA SIN COSTES ADICIONES Y APROVECHA NUESTROS **BUNDLES PROMOCIONALES** DESDE: **70€/MES**

TENEMOS DISPONIBLES PARA TI 6 CONFIGURACIONES:
PA-220, PA-820 E PA-850 EN STANDALONE Y HA

BUNDLE INCLUYE:

- Hardware: PA-220, PA-820 o PA-850
- Suscripciones Threat Prevention + URL filtering + WildFire + Premium Support
- Suscripciones y suporte para 3 años

Las compañías deberían adquirir lo que se aprecie y alquilar lo que se deprecie.

Ventajas renting tecnológico:

- Elimina los riesgos de obsolescencia tecnológica
- Mejora tú tesorería y el ROI
- Ahorra tiempo, procesos y costes de gestión asociados a la adquisición, contratación y mantenimiento de los equipos.

OFICINAS CENTRALES MADRID
C/ Arturo Soria 336, Plnata 8
28033 Madrid
Tel: +34 902 10 88 72 | Fax: +34 917 662 634

DELEGACIÓN CATALUÑA
Avda. Diagonal, 177, Planta 5
08018 Barcelona
Tel: +34 93 547 72 21

guridad es uno de los mercados que exhibe una mayor innovación. "Una muestra de ello es que cada vez nacen nuevas compañías con soluciones muy específicas para necesidades concretas". Recuerda que la seguridad al 100 % no existe y apela, para tratar de reducir la distancia, en la exigencia de monitorizar de manera constante los sistemas de seguridad. "Una auditoría proactiva nos permite comprobar si están actualizados y preparados para las amenazas. La clave está en la respuesta integrada y coordinada de todos los elementos de seguridad".

Es Juan José Roncero el más optimista de la mesa en este asunto. "La tecnología de prevención ha avanzado lo bastante para reducir esa brecha casi al mínimo", opina. Sin embargo, reconoce que en España no abundan las empresas que hayan hecho la inversión adecuada en soluciones profesionales que realmente incorporen las últimas tecnologías. "Nunca había existido tanta tecnología centrada en la seguridad como ahora, con una filosofía proactiva y una enorme capacidad para prevenir".

Una lista interminable de amenazas

La lista de amenazas no ha descendido en el último año. Tras un 2017 marcado por el enorme impacto mediático de WannaCry, convenientemente arropado por un ramillete de amenazas en el que aparecieron diversos ataques de denegación de servicio, robos de datos, fugas de información o *malware* de distinto pelaje, el panorama este año no pinta mejor. Alejandro Soto recuerda que ya en 2018 se han producido dos ataques de denegación de servicio mucho más grandes que el que se produjo el pasado año, que fue el mayor de la historia. "Están haciendo uso de los múltiples dispositivos conectados que no cuentan con ninguna medida de seguridad; una tendencia que se incrementará en los próximos meses". Unos ataques de denegación de servicio que duplicaron su virulencia el pasado año. Según un informe, el 33 % de las organizaciones tuvieron que enfrentarse a este tipo de ataques, en comparación con el 17 % que se vieron afectadas en 2016.

El *ransomware* seguirá siendo una de las principales preocupaciones. Según la consultora CyberSecurity Ventures, los daños causados por esta amenaza alcanzaron en 2017 los 5.000 millones de dólares, cinco veces más que en 2016. Una cantidad que estiman que superará los 11.500 millones de dólares en 2019.

Alejandro Soto,
sales manager de **Westcon Security**

"El auténtico guerrero del mercado de la seguridad es el integrador; que es el que está en el cliente"

Un peligro mucho menos mediático es la fuga de información. Alberto Gómez insiste en los enormes riesgos que supone. "Es relativamente sencillo que un empleado sustraiga información crítica de una compañía", recuerda. "Las empresas se están dando cuenta de que los datos sensibles y confidenciales están al alcance de cualquier empleado; por lo que habría que prestar mucha más atención e incidir en la necesidad de proteger y cifrar los documentos porque hay soluciones, sencillas de implementar, que previenen estas fugas".

Y no solo su protección sino también su gestión. "Los datos son el negocio que todos tenemos encima de la mesa", recuerda Martín Trullas. "Son claves las soluciones que no solo permiten su seguridad, sino que también aseguren su buen gobierno y su gestión correcta, separando lo qué es importante de lo que no lo es". A su juicio, aún estamos lejos de desplegar soluciones de analítica de datos donde la seguridad sea importante y "tratar los datos desde el punto de vista de la seguridad, no para generar más negocio".

No se olvida la formación, básica para concienciar al eslabón más débil de la cadena: el usuario. "Es clave", recuerda Carmen Muñoz. "Además de su educación, es necesario implementar mecanismos de control para evitar que la información salga de las empresas. Muchas veces se trata de fugas no premeditadas, provocadas por descuido o por desconocimiento de los usuarios", explica.

Ahora bien, tras todas las amenazas del año pasado, los integrantes de la mesa coinciden en que lo que sí se ha producido es una mayor concienciación de las empresas en temas de protección de datos y de educar a los usuarios. "Ha sido la gran lección", resume Carmen Muñoz.

RGPD, la oportunidad que ya está aquí

En el horizonte, el próximo 25 de mayo. Una fecha en la que sí o sí las empresas deben tener lista una hoja de ruta para cumplir con el Reglamento General de Protección de Datos (RGPD). De acuerdo con los informes de las consultoras y de los acto-

Ingram Micro: acelerando el negocio de la ciberseguridad

2017: 123.064 incidentes de seguridad gestionados. 116.642 afectaron a empresas y ciudadanos, 885 a operadores estratégicos y 5.537 correspondieron al ámbito académico de la RedIRIS. 18.111 vulnerabilidades nuevas.

Las cifras anteriores, sin duda relevantes, son sólo la punta del iceberg de la Ciberseguridad en España. Corresponden únicamente a la gestión realizada por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Energía, Turismo y Agenda Digital.

"El subsector de la ciberseguridad representa ya más de 600 millones de euros de facturación en España"

Una amenaza, sobre la que existe cada vez una mayor sensibilización, una creciente percepción del riesgo, pero que supone también una gran oportunidad de negocio. El subsector de la ciberseguridad representa ya más de 600 millones de euros de facturación en España.

Sin embargo, tanto la capacitación de las compañías IT, como la disponibilidad de talento especializado, siguen siendo tremendamente escasos. Y el abanico de soluciones disponibles sigue estando muy atomizado. Esta atomización, unida a la rápida evolución de las ciberamenazas, hacen difícil a las empresas implementar soluciones efectivas y sostenibles.

La mayor parte del tejido empresarial, territorio pyme, opta por cortafuegos, auditorías de red y externalizan los servicios de seguridad, como principales recursos para proteger sus negocios. Sus tradicionales proveedores IT, que ahora deben proporcionar también respuestas en entornos OT, deben evolucionar al ritmo que lo hacen los nuevos retos. En su formación y apoyo encuentra el mayorista de valor su razón de ser.

En Ingram Micro, hemos puesto al servicio de nuestro canal una estrategia PPDR (Pronosticar, Prevenir, Detectar y Responder). Les ayudamos para ello a integrar en una solución completa las diferentes piezas/marcas que componen nuestro *portfolio* especializado en ciberseguridad.

Proporcionamos también respuestas convergentes con el mundo de la seguridad física y el IoT.

Además de servicios de consultoría y formación, facilitamos servicios SOC marca blanca para nuestros *partners*, habilitándoles los recursos necesarios para la monitorización, correlación, detección o gestión de dispositivos, que permitan la alerta temprana y la respuesta ante amenazas.

"Hemos puesto al servicio de nuestro canal una estrategia PPDR (Pronosticar, Prevenir, Detectar y Responder)"

Desde esta tribuna, invitamos al lector a solicitar un análisis de vulnerabilidades y una asesoría en ciberseguridad, que le permita profundizar en estas capacidades de Ingram Micro. Contacten para ello con **antonio.anchustegui@ingrammicro.com**. Se sorprenderán.

Alberto Pascual
Executive director Ingram Micro Madrid

IoT, ¿el desastre que se avecina?

El Internet de las cosas es mucho más que una tendencia de "moda". Los analistas de la industria estiman que en el año 2020 habrá más de 30 billones de dispositivos conectados y este mercado del IoT superará los 1.700 millones de dólares. El mercado español de Internet de las cosas representó en 2015 el 9 % de todo el mercado del IoT de Europa Occidental y la previsión apunta a que supere los 16.400 millones de euros en 2018, según datos de IDC.

El despliegue del IoT representa una convergencia entre el entorno TI y el OT (que señala las operaciones). "Dos entornos que hasta el momento no se hablaban", recuerda Alberto Pascual. "Y que lo están empezando a hacer gracias a las empresas proveedoras de soluciones tecnológicas", continúa. Los mayoristas, a su juicio, entran perfectamente en la ecuación. "Somos los mayores integradores de las soluciones que permiten el desarrollo del IoT". Ahora bien, a su juicio, el IoT explotará a partir de 2020. "Hasta que no se despliegue el 5G no se populizará". Optimista, cree que con la popularización llegará también la protección de los dispositivos IoT.

La seguridad se torna en el elemento fundamental en esta convergencia. "Los dos entornos deben entenderse", insiste Alejandro Soto. "Ha habido múltiples ataques en las áreas industriales que requieren una protección adecuada basada, precisamente, en herramientas TI". No es sencillo ya que los entornos industriales cuentan con protocolos de comunicación diversos; sin embargo, los fabricantes de TI están lanzando soluciones adaptadas a estos entornos. "Estamos ayudando a que el canal se centre en el desarrollo de estos proyectos en los que las latencias, por ejemplo, son claves ya que cualquier parón es crítico". Soto explica que es fundamental contar con profesionales certificados en los diferentes entornos, que presentan particularidades claras. "Sus protocolos son distintos; por tanto, las soluciones que acercan las herramientas de TI al mundo industrial también deben serlo".

También Trullas pone el acento en la seguridad, que parece ser, por el momento, la gran olvidada en los proyectos en torno al IoT que combinan analítica, *cloud* y servicios. "Es la oportunidad que se avecina", asegura. Se trata de crear *bundles* que resuelvan la problemática de diferentes segmentos de mercado (*retail*, *smart cities*, industria, etc.).

En el caso de Arrow, la convergencia se refleja en la propia configuración de sus áreas de negocio: junto a las más reciente TI, el mayorista cuenta con un negocio vinculado con los componentes y semiconductores. "Se trata de acercarla al área TI y, junto a los desarrollos de nuestras marcas, poner en contacto a los socios que trabajan en cada uno de los dos apartados".

Alberto López,
director enterprise security division de **V-Valley**

"En 2018 va a haber muchas oportunidades en torno a la protección y el cifrado de información"

res involucrados en la misma, todavía hay un número considerable de empresas que no tiene una estrategia definida para adaptarse a esta norma. Los números varían: en España algunos datos aseguran que apenas el 10 % de las empresas ha iniciado procesos en esta línea mientras que otros baremos sitúan el porcentaje en el 25 %. En el caso de las grandes empresas, es siempre superior.

La ley ordena la salvaguarda y adecuada protección del dato y cada compañía debe definir una estrategia que debe incluir, de manera global, a la organización y a los empleados; regulando todos los procesos en los que se manejen los datos.

V-Valley... Next Generation Distributor

Tres apasionados de su trabajo que se embarcan en la aventura de la construcción del Next Generation Distributor saliendo de su zona de confort. Si todo el mundo sabe lo que hay que hacer, ¿por qué resulta tan difícil plasmarlo en la realidad?

Nos incorporamos a este proyecto con un objetivo claro dentro de nuestra nueva organización: crear el mayor distribuidor de seguridad del sur de Europa, con la agilidad de un local y la fortaleza de una multinacional. Actualmente el grupo Esprinet, donde se enmarca V-Valley, y dentro de ella la división de seguridad a la que nos hemos incorporado, es ya líder en esta región, con más de 3.000 millones de euros de facturación global. Y también aspira a serlo en el área de la seguridad en un periodo de tres años.

Este proyecto, que se torna en importante reto, es lo que nos ha hecho emprender esta aventura. Apoyándonos en los sólidos cimientos de grupo y en los buenos mimbres del área de seguridad que existían, debemos construir la unidad de negocio de seguridad, creando un *portfolio*, un equipo, una metodología de trabajo y, en definitiva, plasmar nuestra filosofía del negocio de la distribución de seguridad. "Conceptos como equipo, colaboración o sentido común, queremos que estén en el ADN de las personas que formamos esta unidad de negocio. Concebimos la ciberseguridad como algo colaborativo, global, que acabe con los silos y en la que las diferentes soluciones colaboren entre sí para ofrecer una respuesta más eficaz y eficiente. Debemos informar de forma adecuada a cada uno de los componentes de las organizaciones para que la posible solución y las acciones que se deben adoptar frente a las amenazas sean las mejores y en el menor tiempo posible.

Pretendemos que nuestros equipos sean un todo, una máquina bien engrasada que ofrezca respuestas adecuadas a las necesidades de los *partners* y fabricantes con los que trabajamos; para que, a su vez, puedan ofrecer las mejores soluciones a sus clientes", comenta Javier Ruiz, director de desarrollo de negocio de la unidad de seguridad.

"Nuestro éxito pasa por tener claro el rol que ocupamos dentro de la cadena, saber qué podemos aportar a cada uno de los elementos de la misma y tener claras sus necesidades. El equipo de seguridad debe interiorizar esta filosofía y convertirla en su "modus operandi" en el día a día. Esto puede sonar básico y elemental, pero creemos en esta idea de trabajo, basada en el sentido común, en "escuchar" las necesidades, en ofrecer las mejores soluciones a nuestro alcance y en "apoyar" su desarrollo", afirma Antonio Arroyo, director comercial de esta unidad.

"La palabra valor en la distribución ha perdido su esencia después de tantos años de su uso indiscriminado. Nuestro objetivo es recuperar su sentido en estos nuevos tiempos con el mejor equipo profesional", concluye Alberto López, *director enterprise security division* de V-Valley.

> V-Valley aspira a ser líder en el área de la seguridad en un periodo de tres años

Este es el reto. El camino lo conocemos. Ahora hay que comenzar a recorrer la senda marcada, el esfuerzo, el trabajo y la convicción en nuestras ideas deben facilitar la consecución de los objetivos.

Alberto López,
***Director enterprise security division* de V-Valley**

El canal no es ajeno, lógicamente, a esta norma. Los mayoristas, en mayor o menor medida, han puesto en marcha iniciativas para que los distribuidores conocieran la norma. Aunque hay empresas que ya han arrancado proyectos para ajustar sus estrategias a este reglamento, el porcentaje sigue siendo muy bajo, siendo incluso inferior el número de empresas que cuentan con un DPD (Delegado de Protección de Datos). Fabricantes y canal esperan que los proyectos, que requieren una implantación larga, fructifiquen y, sobre todo, aumente su número en el segundo semestre. "Hay mucha expectación pero aún no se ha traducido en el negocio de manera significativa", asegura Juan José Roncero que vislumbra una clara oportunidad para que los servicios sigan creciendo. "Es un aspecto que se puede externalizar. En el caso de Aryan, estamos pensando en incorporarlo a la oferta como un servicio para ofrecérselo a los distribuidores que se dirigen a las pymes que no tienen la posibilidad de contar con un experto".

La aplicación correcta del reglamento va mucho más allá de la seguridad. "Muchos fabricantes, con foco de negocio en muchas áreas, ya cuentan con soluciones para ayudar a su cumplimiento que van desde la gestión del dato hasta la protección y el cifrado del mismo", recuerda Iñaki López que, como Roncero, habla de la enorme oportunidad que se abre en el campo de los servicios. "Muchas empresas lo abordarán a través de empresas que ofrecen una seguridad gestionada y que posiblemente ofertarán un módulo o una ampliación de sus servicios para ayudar a cumplir con este reglamento".

Se trata de definir qué medidas de seguridad hay que implementar para cumplir con lo exigido en la ley. "Las empresas son responsables de los datos que alojan en sus sistemas. Y de su protección", insiste Alejandro Soto. "Sin embargo, el RGPD no entra en el detalle de cómo hacerlo", alerta.

Todos auguran un dinámico segundo semestre: tras su entrada en vigor el 25 de mayo, se abre un tiempo para observar su implantación. Y las posibles sanciones que se aplicarían en el caso de las infracciones. Sanciones que, reconocen, seguro que promoverán una mayor adecuación. Y un mayor negocio.

Los servicios progresan adecuadamente en el canal

La externalización camina a buen ritmo en el mercado de la seguridad. Según IDC el 80 % de la seguridad será gestionada en 3 años y los mayoristas están convencidos de que no es un porcentaje desorbitado. "Muy pocas empresas se pueden permitir el lujo de adquirirla bajo una fórmula *capex*", asegura el máximo responsable de Arrow. "Pagar un servicio en función de la demanda es la mejor opción", continúa. "Y el futuro", remata.

La pyme parece ser la usuaria perfecta de esta externalización. "Por el alto coste que supone, la mayoría de este tipo de empresas sólo tiene instalado un *firewall*; lo que les asegura la protección, pero no la detección y la respuesta ante los incidentes", explica Alberto Pascual. "Los servicios gestionados se van a popularizar en los próximos meses", asegura. "Las empresas son conscientes de sus vulnerabilidades y por ello van a apostar por este tipo de servicios".

La evolución del modelo de negocio de los fabricantes va a marcar el crecimiento de este tipo de servicios y la gran mayoría de las marcas cuenta ya con modelos de licenciamiento ligados al pago por uso. Carmen Muñoz, además de este servicio gestionado, apela a los servicios, con más recorrido en el canal, vinculados con la asesoría y la consultoría. "Los nuevos ataques o la implantación del RGPD son claves para que el canal siga dando este tipo de servicios".

Roncero está convencido de que los servicios gestionados deben caer en manos de los distribuidores. "La labor del mayorista es contar con las soluciones de los fabricantes bajo el formato del pago por uso. Una empresa, por pequeña que sea, puede disfrutar de un pequeño SOC a su medida con este tipo de soluciones. Nuestra labor es motivar al canal para que sea capaz de dar ese servicio. Es lo que les va a dar la rentabilidad".

Enarbolando el valor

La oportunidad es enorme; lo que no impide que el canal debe seguir adaptando su organización a un mercado en el que se producen cambios de manera continua, lo que exige una adaptación casi perpetua. Alberto Gómez apunta uno, importante: la presencia, cada vez mayor, de las huestes de los fabricantes en el mercado, lo que ha provocado que una gran parte de los proyectos que se desarrollan en el segmento más elevado vengan muy definidos por su presencia. "En este en-

Juan José Roncero,
director del negocio de seguridad de **Aryan Comunicaciones**

"Estamos orientando a nuestros distribuidores a desarrollar los servicios"

Tech Data®

Advanced Solutions

NEXT GENERATION TECHNOLOGIES

CLOUD

SMART IOT & ANALYTICS

FORMACIÓN Y SERVICIOS PROFESIONALES

SEGURIDAD

División especializada en soluciones con equipos dedicados, expertos en dar soporte técnico y de ventas, consultoría, formación y servicios profesionales de todos nuestros fabricantes.

aws · ADVANTECH · BlackBerry · cisco · IBM

Informatica · Information Builders · McAfee · Microsoft · radware Every second counts

RSA · SONICWALL · STORMSHIELD · VEEAM · vmware

www.Holatechdata.com www.techdata.es 91 414 83 00

torno, tanto nuestro rol como el del integrador, vienen muy marcados", reconoce. Los márgenes, cada vez más ajustados, y la imposibilidad de que el integrador disponga de personal formado en todas y cada una de las tecnologías, complican el panorama. "Muchos de ellos están buscando alianzas con integradores más pequeños y especializados que les permitan, en colaboración, ofrecer el servicio".

Carmen Muñoz asegura que no se da en todos los proyectos. "Hay clientes que están observando diferentes problemáticas y, antes de casarse con una tecnología o un fabricante concreto, demandan una labor de consultoría previa, capaz de detectar los problemas y determinar las soluciones adecuadas para subsanarlos. Sólo después llega el mensaje de una marca concreta; no antes".

De cualquier manera, algunos observan que es posible recuperar el terreno perdido. "Los mayoristas pueden ayudar al distribuidor a ganar presencia porque el auténtico guerrero de esta historia es el integrador; que es el que está en el cliente", asegura Alejandro Soto. "El control último de las cuentas lo tienen los integradores y es el mayorista quien debe conectar al fabricante con el *partner* para que éste sea capaz de generarle más negocio. Somos los catalizadores".

Hay que seguir insistiendo en el valor. Ahora bien, el integrador debe evolucionar en su estrategia. "Muchos ya lo han hecho", asegura Iñaki López que está convencido de que, tras la implantación de los proyectos, el integrador se convierte en el máximo protagonista del seguimiento del mismo. "Son primordiales las actualizaciones, las pruebas tecnológicas, el soporte…".

El panorama es radicalmente diferente en el escalón de las medianas y pequeñas cuentas. Juan José Roncero defiende la fidelidad de los socios que se mueven en estos apartados que esperan una cosa del mayorista: "Que le ayudemos a trasladar, de manera mucho más rápida, la innovación tecnológica que exhiben las marcas a los clientes".

Martín Trullas se muestra completamente confiado en que en estos terrenos medianos es el canal el que marca el terreno. "Somos los mayoristas quienes ayudamos a los distribuidores a definir qué tecnología es la mejor para el cliente".

Martín Trullas,
director de la unidad de *new generation technologies* de **Tech Data**

"Aún estamos lejos de desplegar proyectos de analítica de datos donde la seguridad sea importante"

Westcon Comstor

Delivering Results Together

Nuestra extensa experiencia en soluciones de seguridad es un activo para el éxito de su negocio

Westcon Security proporciona el portfolio, las herramientas y el apoyo que necesita para salvaguardar la información y la reputación de sus clientes a través de nuestra extensa red global de socios, décadas de experiencia en canal y un modelo de distribución innovador que combina **Servicios Profesionales** y logística avanzada. Nuestro equipo de Seguridad ajusta las soluciones a su medida para incrementar la rentabilidad de sus proyectos.

Más información:

security.es@westcon.com

+34 91 419 61 00

es.westcon.com

Westcon-Comstor Spain

@WestconEspana

Perspectivas de futuro: la seguridad como servicio

Uno de los mejores ejemplos de transformación tecnológica son las aplicaciones para seguridad basadas en software o seguridad como servicio. Estas aplicaciones encajan perfectamente en un modelo de servicio gestionado basadas en software y aplicaciones, siendo el hardware secundario. Así, las pymes pueden asegurar su infraestructura informática y de comunicaciones con un menor desembolso al reducir la inversión en costoso hardware o reinvertirla en mejores y más completas aplicaciones de seguridad que cubran las necesidades que ahora mismo tienen desatendidas por falta de capacidad financiera.

Por tanto, el software como servicio en seguridad es una tendencia con futuro. Se impone por la flexibilidad y dinamismo que aporta frente al hardware. Las amenazas informáticas que afectan a la pyme cada vez son más complejas y dinámicas, por tanto, las aplicaciones que le protegen deberán evolucionar igual o más rápido.

En la medida en que este software es más complejo y cambiante por su evolución, es necesario un mayor conocimiento y dedicación para gestionarlo adecuadamente y es aquí donde la pyme no tiene capacidad para abordar este reto; por ello el canal tiene que asumir este papel en modo de servicios, como expertos en seguridad, y atender sus necesidades. Se observa claramente cómo el software de seguridad como servicio en modo de pago por uso es, sin duda, una tendencia en alza.

Al canal, respecto de la seguridad como servicio, todavía le queda camino por recorrer lo que hace de ésta una oportunidad de negocio por explotar. Se está dando una transformación de proveedores de infraestructura a proveedores de servicios globales, lo que provoca un fuerte desarrollo de servicios de seguridad gestionados cuyo principal recurso son aplicaciones en nube o virtualizadas. Aryan, desde su división de seguridad, proporciona soluciones donde el software y las aplicaciones son el motor de la solución, y el hardware propietario es prescindible en muchos casos o solo una opción puntual en entornos críticos. En prácticamente todos los fabricantes de nuestro *porfolio*, desde WatchGuard, Ctera, Bitdefender a Cososys y F-Secure, el acceso al software de seguridad basado en formato de pago por uso está presente de forma total o parcial, favoreciendo que el canal ayude a la pyme a protegerse de la compleja ciberdelincuencia actual, a cumplir con la nueva normativa actual en materia de protección de datos y, en definitiva, dejar en manos de personal experto y dedicado todo lo relacionado con la seguridad, manteniendo siempre las aplicaciones más innovadoras y actualizadas sin tener que hacer costosas y complejas inversiones. De esta forma posiblemente podamos conseguir que la pyme española deje de ser de las más atacadas y vulnerables en materia de seguridad debido, entre otros factores, a su actual deficiencia tecnológica en este campo.

> El software como servicio en seguridad es una tendencia con futuro. Se impone por la flexibilidad y dinamismo que aporta frente al hardware

Juan José Roncero
Director comercial de la división de seguridad IP en Aryan