linkedin
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai editorial

Año XXX Nº 316 Junio 2024 0,01 Euros

El mayorista blinda su papel en la ciberseguridad

La ciberseguridad sigue presentando importantes oportunidades de negocio

El mayorista blinda su importante papel en el mercado de la ciberseguridad

No deja de crecer el mercado de la ciberseguridad. Un mercado, complejo, en el que las amenazas siguen ganando enteros de peligrosidad y eficacia, al mismo tiempo que las empresas siguen tratando de armar una estructura de protección, con una filosofía proactiva, para repelerlas. En el ecosistema tecnológico encargado de ayudarlas en esta tarea, los mayoristas mantienen, incólume, su importante papel, desplegando un soporte que alcanza tanto a los fabricantes como al panel de distribuidores e integradores. Un papel en el que deben hacer frente a retos tan importantes como la falta de talento, la gestión de la complejidad de la tecnología, el soporte en áreas como la formación, la financiación o la consultoría, o el desempeño en apartados de crecimiento como los servicios gestionados o la oferta de sus propias plataformas. Mayoristas como Arrow, Exclusive Networks, Ingram Micro, TD Synnex, V-Valley y Westcon; que los afrontan con la vista puesta en la rentabilidad y el crecimiento.

Marilés de Pedro

Panorama de mercado

La seguridad sigue siendo un segmento "bendecido" por la oportunidad. Según la consultora IDC el mercado de la seguridad en España está mostrando este ejercicio un crecimiento respecto al año pasado del 9,2 % y la previsión es que alcance los 2.130 millones de euros. Para 2026 podría superar la barrera de los 2.995 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito (9,9 %).

Para Carmen Muñoz, directora general de Exclusive Networks en España y Portugal, la inversión en ciberseguridad es una prioridad para las compañías. "Observamos los mayores crecimientos en torno a la protección de la nube. Cada vez hay más volúmenes de datos que gestionar y hay que minimizar las vulnerabilidades y las posibilidades de ataque en las infraestructuras que se alojan en estos entornos", señala. Junto a ello, la privacidad de los datos, la gestión de identidades y la protección de los entornos industriales completan, a su juicio, las mayores áreas de inversión.

Ángel García, director del área de Seguridad en Arrow, corrobora que en los presupuestos de TI una parte muy importante se dedica a la inversión en ciberseguridad, lo que permite que el crecimiento vaya a continuar. El directivo se refiere a la inteligencia artificial que recuerda que es un alma de doble filo. "Por un lado, permite que las técnicas de los fabricantes avancen para mejorar tanto la detección como la remediación; pero también sirve a los *hackers*, permitiéndoles armar unos ataques mucho más sofisticados y difíciles de mitigar". En la lista de áreas con mayor inversión, corrobora la oportunidad en torno a la nube y a la protección de los entornos industriales; a lo que añade las tecnologías de Confianza Cero. "Controlar el acceso, sea quien sea, dentro o fuera de la red, es una importante área de inversión".

Nota Martín Trullás, director del área de Advanced Solutions en Ingram Micro, a pesar de las excelentes oportunidades, una cierta fatiga en el mercado. "A pesar de los buenos crecimientos de los que disfrutamos, los proyectos vinculados con la Administración pública están sufriendo una cierta ralentización", señala. Sin embargo, prevé un cambio de tendencia en la segunda parte del año; pasadas ya todas las citas electorales que ha vivido España. "De cualquier manera la ciberseguridad sigue siendo un motor de crecimiento para el negocio de los mayoristas".

David Gasca, *sales & marketing manager cybersecurity* en V-Valley, recuerda la creciente consolidación que sigue produciéndose en el sector, tanto en el segmento de los fabricantes como en el de los mayoristas. "Los fabricantes, además, cuidan mucho más sus políticas de distribución: muchos han reducido su canal mayorista, analizando, de manera más pormenorizada, con qué compañías trabajan". A su juicio, aunque los crecimientos son buenos, "va a costar, cada vez más, mantener estos ritmos".

Ángel García
director del área de Seguridad en **Arrow**

"Entrar en la rueda de servicios gestionados le permite al *partner* disfrutar de un crecimiento paulatino, a largo plazo"

María Isabel Arias, directora de ciberseguridad de Westcon, ratifica el buen momento que vive la ciberseguridad y las oportunidades que pueden abrir las nuevas normativas que van a entrar en vigor, como es el caso de NIS2 o DORA. "Tanto las empresas privadas como los organismos públicos están analizando qué necesitan para cumplir con ellas, lo que demuestra que la ciberseguridad forma parte de su negocio", señala. A su juicio, el alcance de ambas legislaciones exige un proyecto adaptado a cada empresa. "Va a ser un traje a medida ya que cada organización tiene que ver qué necesita y qué soluciones se adaptan mejor a su caso. Se trata de una enorme oportunidad para los *partners*. Y también para los mayoristas en nuestra labor de concienciar y de ayudar a que el distribuidor dé más valor y más servicios", explica. Por último, Arias recuerda la necesidad de que "la ciberseguridad sea cada vez más proactiva. Sin lugar a dudas, es uno de los factores que asegura su crecimiento", continúa.

Santiago Méndez, director del área de Advanced Solutions en TD Synnex, corrobora la enorme oportunidad que se abre con estas normativas. Aunque ha notado, tras un buen primer trimestre, cierta ralentización en el segundo. "Seguimos generando oportunidades, pero el

Carmen Muñoz
directora general de **Exclusive Networks**

> "Hoy, más que nunca, tienen sentido figuras como las nuestras, en aspectos, por ejemplo, como la concienciación o la formación"

proceso de maduración de los proyectos se está alargando. Quizás esté relacionado con la inversión de la Administración pública; pero también con los modelos y las normativas regulatorias que empiezan a tener cierta fatiga, como es el caso de la GDPR, por ejemplo. Otras, sin embargo, están tirando mucho más, como las relacionadas con los medios de pago y, sobre todo, con DORA y NIS2".

Repaso a las amenazas

Según el CERT del INCIBE en 2023 se registró un incremento del 24 % de los incidentes respecto a 2022. Entre las amenazas, el *ransomware* sigue marcando tendencia con un crecimiento el pasado año del 128 %. En España se calcula que las "ganancias" superaron los 1.100 millones de dólares el pasado año. Junto a esta amenaza, siguen cobrando peso los ciberataques patrocinados por el estado, el *hacktivismo* y el uso de la IA por parte de los *hackers*.

Otra de las tendencias al alza es el *phishing* a CIO y CEO; un modelo que forma parte de las estrategias "a futuro" que desarrollan los *hackers*. "Se trata de captar, en un primer momento, los datos sensibles y, posteriormente, cuando cuenten con la suficiente capacidad de cómputo, son capaces de acceder, con una enorme facilidad, disponiendo de una base instalada de ataques", explica Santiago Méndez.

Para María Isabel Arias este complejo mapa de amenazas se torna, una vez más, en una enorme oportunidad para fabricantes, mayoristas y distribuidores. "Estamos viendo muchas novedades por parte de los fabricantes para prevenir o resolver las amenazas; lo que abre enormes oportunidades al canal de distribución para desplegar sus servicios".

Recuerda Martín Trullás el creciente poderío que tienen las organizaciones criminales dedicadas a la propagación de las amenazas. "Hay grupos de ciberdelincuentes cuyo PIB es mayor que el que tienen muchos países. Cuentan con un enorme potencial económico y con suficientes recursos para innovar y desplegar las mejores técnicas para atacar". Trullás reconoce que el uso que hacen de la tecnología les permite ir por delante de los fabricantes.

"Nadie está a salvo", recuerda Ángel García. "Aunque, a mayor magnitud de la empresa, mayor posibilidad de sufrir ataques y mayores puntos de ataque; lo que señala una mayor recompensa para los *hackers*". El directivo de Arrow recuerda que el eslabón débil es la concienciación del usuario. "Hay muchas puertas de entrada en la infraestructura de las empresas que permiten el ataque. Y esto no va a acabar ya que la sofisticación de las amenazas va a seguir creciendo", explica. Es el caso, por ejemplo, de la evolución que ha experimentado el *ransomware*: antes estos ataques cifraban la información y los *hackers* cobraban por descifrarla; ahora cobran por no hacer públicos los datos. "Va cambiando la manera en la que los ciberdelincuentes consiguen el dinero".

> Uno de los grandes retos a los que tiene que enfrentarse el segmento tecnológico es la escasez de talento. Se calcula que en España hay 140.000 vacantes que no están cubiertas

Carmen Muñoz corrobra que todas las empresas están expuestas. "Ya no es una cuestión de tamaño. Los ataques empiezan a estar tan automatizados que la escalabilidad es mucho mayor. Los atacantes pueden poner el punto de mira en todos los sectores y en todos los tamaños de compañía".

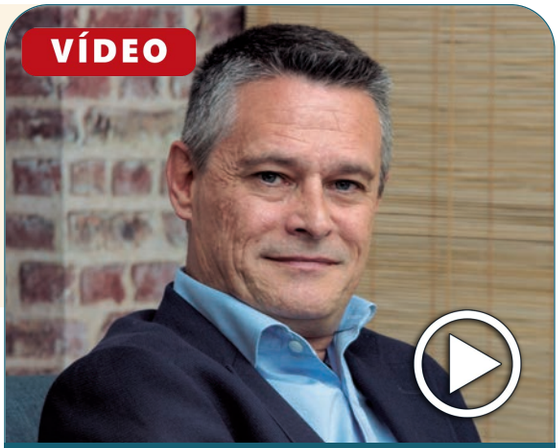
Habilite las medidas de Seguridad, en cualquier lugar

Proteja los intereses y las posibilidades de su negocio sin limitar a empleados, clientes o proveedores.

arrow.com/globalecs/es

ARROW

"La ciberseguridad sigue siendo un motor de crecimiento para el negocio de los mayoristas"



Martín Trullás
director del área de Advanced Solutions en **Ingram Micro**

La directora de Exclusive Networks asegura que hay una mayor concienciación. "La exigencia, como así lo recogen las regulaciones, de hacer públicos los ataques que tienen éxito en la empresa, ha conducido a elevar la concienciación", analiza. Una idea que corrobora María Isabel Arias que recuerda que estas normativas también exigen que las empresas cuenten con todos los medios necesarios para evitar estos ataques. "Y si éstos se producen, disponer de una capacidad de reacción rápida para que ocasionen los menos daños posibles".

Santiago Méndez, aunque sí que observa una mayor concienciación, duda si esta ha provocado una mayor reacción. "Hay muchas compañías que solo reaccionan cuando son atacadas. La concienciación debería conducir a que las empresas contaran con una mayor partida presupuestaria para la ciberseguridad".

Valor "imprescindible" del mayorista

En un mercado cada vez más complejo, en el que la ciberseguridad debe hacer frente a un panorama con un mayor número de amenazas, y en el que hay un número enorme de fabricantes que cuentan con soluciones para poder armar una adecuada defensa, el papel del mayorista se ha consolidado. Carmen Muñoz asegura que "hoy, más que nunca, tienen sentido figuras como las nuestras, en aspectos, por ejemplo, como la concienciación". La directiva insiste en que la ciberseguridad tiene que ser parte de las estrategias de negocio de las compañías. "Como mayoristas tenemos la obligación de ir con este mensaje al mercado y, ante su enorme y creciente complejidad, ayudar al canal a implementarlo en sus clientes". Un canal en el que hay un problema de especialización y de recursos. "Cualquier fabricante que cuente con una estrategia de canal necesita que sus *partners* estén formados. Nuestra figura es una extensión del fabricante: tenemos que tener claro cuáles son sus prioridades y complementarlos en las áreas donde sea necesario". Muñoz recuerda que, aunque las marcas cuenten con estrategias globales, hay una "realidad" local que les ha permitido, en algunos casos, contar con algunas particularidades. "Seguimos contando con la confianza de algunos de ellos, por ejemplo, que han abierto su distribución en otros países a más mayoristas y que, en nuestro caso, seguimos manteniendo una exclusividad. Han confiado en que sigamos siendo una extensión de sus equipos en el mercado local por nuestra capacidad de desarrollar el canal y de llegar a segmentos de mercado donde ellos no llegan".

Los mayoristas siempre han sido poderosas canteras de profesionales para los fabricantes y el ecosistema de integradores y distribuidores

David Gasca recuerda que, para el fabricante, el mayorista es un socio con una labor que va mucho más allá de la comercialización de sus soluciones. Incluso los grandes fabricantes, con una presencia muy sólida en España que incluye una amplia plantilla, despliegan alianzas con mucho contenido. "Hay fabricantes, por ejemplo, que disfrutan de una gran presencia en el mercado *enterprise* y en los ISP, pero que requieren de nuestra ayuda para desarrollar el mercado de los proveedores de servicios gestionados (MSP) o el segmento medio. Y, al contrario: hay proveedores con mucho foco en los segmentos de entrada o en la mediana empresa, que nos piden soporte para acceder a los clientes corporativos".

La exclusividad sigue existiendo en el canal. En la oferta de V-Valley, como sucedía con Exclusive Networks, cuentan

Lidera cloud

Powered by V-Valley

TU PLATAFORMA MSSP AUTOMÁTICA Y DESATENDIDA

La plataforma de gestión de servicios de suscripción MSSP, que ofrece la posibilidad de provisionar servicios de ciberseguridad de fabricantes mundialmente reconocidos, de manera automática y desatendida.

ÚNETE A LAS VENTAJAS DE LIDERA CLOUD

- Modelo de suscripción
- Pago por uso
- Mayor margen por volumen
- API de provisión
- Atención comercial
- Proceso de onboarding
- Servicio integral de soporte
- Beneficios económicos

En V-Valley | Lidera trabajamos con los líderes del sector

A10 Networks · Acronis · AREXDATA · ARMIS · BACKBOX · BlackBerry · CA Technologies (A Broadcom Company) · CHECK POINT · CLOUDFLARE · CYBERARK · Cyber Guru · elastic · ENTRUST · iberlayer · invicti · ivanti · kaspersky · Lidera cloud (V-Valley) · NETWITNESS · Omada · opentext Cybersecurity · REDCARBON · RED SIFT · SailPoint · securonix · SONICWALL · sumo logic · Trellix · TREND MICRO · WatchGuard · XM Cyber

¿Quieres saber cómo integrar nuestras soluciones para acelerar tu negocio?
¡Contacta con nuestros especialistas!

www.v-valley.com

Santiago Méndez
director de Advanced Solutions de **TD Synnex** Iberia

"La concienciación debería conducir a que las empresas contaran con una mayor partida presupuestaria para la ciberseguridad"

con proveedores de los que son el único mayorista en España. "El mayorista es la extensión del equipo del fabricante en aquellas áreas a las que no llega", corrobora Gasca.

Martín Trullás recuerda el papel de asesoramiento y "filtro" en la configuración del catálogo del *partner*. Recuerda que hay segmentos, como es el caso de los entornos de infraestructura, en los que el abanico de marcas es mucho más reducido. No sucede así con la ciberseguridad "La oferta es enorme; hay muchos fabricantes con tecnologías similares", explica. Un *partner* que no está familiarizado con el mundo de la ciberseguridad y que observa la oportunidad, necesita un mayorista especializado que le asesore en la configuración de la oferta y le indique qué fabricantes le encajarían mejor en su estrategia de negocio con sus clientes. "Hay que entender al *partner* y cómo le puedes ayudar en su estrategia de ciberseguridad. Además de ayudarle a conformar su oferta, hay que desplegar, junto a él, los primeros pilotos y pruebas de concepto, así como la necesaria generación de demanda e, incluso, los servicios relacionados con la posventa".

No se olvida el despliegue de las plataformas y los *marketplaces*. "Al ritmo que nos ha marcado el mercado, ya contamos con capacidades de despliegue de servicios gestionados, que también podemos poner en manos del canal. Incluso la posibilidad de que pueda trabajar con los hiperescalares", relata el responsable del área de Advanced Solutions de Ingram Micro. "No somos prescindibles".

Santiago Méndez apela al papel orquestador del mayorista. "Hay que tener una aproximación inteligente a la oferta; no se trata de coleccionar marcas". En un mercado de la ciberseguridad absolutamente desfragmentado, con más de 160 fabricantes, algunos muy especializados, es clave que el mayorista configure una oferta en la que exista coherencia, haya la mayor sinergia posible y esté adaptada al ecosistema de *partners* con el que trabaja de manera más natural. "Hay que crear un ecosistema y disponer de suficiente capacidad

INGRAM MICRO®

Jueves, 10 de octubre

SIMPOSIUM 24

Redefiniendo la distribución

Fira Barcelona

Fira Barcelona Gran Vía

MÁS INFO: es.ingrammicro.eu/simposium

#IngramMicroSimposium

10-10-2024

para cubrir las necesidades que el fabricante requiere". Méndez recuerda la estrategia de plataformas que están siguiendo los mayoristas y que también requiere coherencia en la selección de marcas.

Una configuración de la oferta en la que incluso es coherente decir que no. "Hay algunos fabricantes que desean desplegar una política de distribución y que, sin embargo, una vez analizada su cartera de soluciones, observamos que no encajan en el mercado español", recuerda David Gasca. "Aplicamos el criterio de ser realistas de lo que se puede abarcar. Aunque somos muy versátiles y podemos desempeñar, prácticamente, cualquier rol, hay que analizar qué demanda cada fabricante". En ocasiones, continúa, la estrategia del mayorista no permite el desarrollo conjunto del negocio. "Hay que ser honesto y observar los recursos de los que se dispone en un momento determinado. En algún caso hemos tenido que denegar la distribución de un fabricante y, sin embargo, más tarde, en el momento adecuado, sí que lo hemos incorporado".

Ángel García apela a la capacidad de flexibilidad como uno de sus valores más importantes. "Somos capaces de comprender la necesidad de cada uno de los fabricantes que tenemos dentro del *portfolio* y adaptarnos a ella: desde el desarrollo de segmentos de mercado a los que no pueden acceder hasta labores de formación, pasando por el soporte en el despliegue de servicios gestionados". Labores a las que suma la capacidad de financiación a medida, la suscripción como servicio o el pago mensual. "El mayorista puede dar todos esos servicios; no así muchos fabricantes, que cuentan con una menor capacidad de flexibilidad".

> Según IDC, los segmentos que mayor crecimiento tendrán este año en el mercado de la ciberseguridad son los relativos a los servicios gestionados

García recuerda que en los últimos años muchos fabricantes han reducido el número de mayoristas con los que trabajan. La explicación la encuentra en el cada vez mayor nivel de exigencia. "El desarrollo del negocio del fabricante exige equipos dedicados cada vez más grandes", explica. Es una alianza en la que ambas partes ganan: el mayorista, que disfruta de una política de distribución en la que hay menos compañías, puede desplegar un mayor foco e invertir más en su desarrollo; y el fabricante disfruta de mayoristas con mejores recursos, más especializados y capaces de hacer

María Isabel Arias
directora de ciberseguridad de **Westcon**

> "El cumplimiento de las nuevas normativas, como NIS2 o DORA, abre una enorme oportunidad al canal"

POC, acciones de preventa y pilotos con su ecosistema.

En la configuración de la oferta del mayorista, Carmen Muñoz insiste en que no se trata de firmar con un mayorista por su volumen o por ganar cuota de mercado. "Cada vez es más complicado porque los fabricantes se están consolidando y tienen cada vez una oferta más amplia. El mayorista debe exhibir una coherencia tecnológica en la firma de los fabricantes con los que trabaja para mantener un nivel de especialización y de recursos necesarios para cumplir con sus expectativas".

Por último, el papel evangelizador. María Isabel Arias apela a las capacidades de los mayoristas de ayudar al canal a conocer las nuevas tecnologías que van apareciendo en el mercado, absolutamente innovador, de la ciberseguridad. Una labor que, incluso, alcanza a los fabricantes, que tienen la visión "limitada" de su oferta, "a los que se puede complementar con un conocimiento de otras tecnologías".

Gestión y retención del talento

Uno de los grandes retos a los que tiene que enfrentarse el segmento tecnológico es la escasez de talento. Se calcula que en España hay 140.000 vacantes que no están cubiertas, lo que dificulta el diseño y el despliegue de adecuadas estrategias de ciberseguridad en los organismos públicos y las empresas privadas. "Falta talento", explica María Isabel

Zero Trust: primera línea de defensa contra el acceso no autorizado y la fuga de información

Con el auge del trabajo remoto y el incremento de las amenazas, la confianza cero ha pasado a ser un modelo integral de seguridad basado en la segmentación de redes, la autenticación continua y el principio de mínimos privilegios.

Garantizar el acceso a los recursos desde cualquier lugar y una experiencia de usuario óptima es clave. Pero dado que las cargas de trabajo y las identidades pueden residir en cualquier punto de Internet, eliminar la confianza implícita es del todo prioritario.

En este contexto la protección de datos sensibles y frente a amenazas internas, el cumplimiento normativo o la mejora de la visibilidad de la actividad y de la adaptabilidad a diferentes entornos, Zero Trust despega con fuerza, especialmente en sectores altamente regulados como los de finanzas y salud.

Aunque el 63% de las organizaciones en el mundo han implementado total o parcialmente una estrategia de confianza cero, según Gartner, muchas empresas aún no conocen las mejores prácticas para desplegar un modelo de confianza cero efectivo. En este terreno, caben mejoras necesarias orientadas a aumentar la comprensión y las habilidades relacionadas con Zero Trust, simplificar su implementación, asegurar la integración de soluciones y desarrollar unas políticas de acceso y seguridad claras y coherentes.

Pero es de rigor señalar que el modelo Zero Trust no debe reducirse únicamente a la gestión de identidades y accesos; debe abarcar todas las superficies de riesgo corporativas en términos de identidad, infraestructura, producto, procesos y cadena de suministro.

Distintas ofertas, amplia seguridad

Exclusive Networks marca una clara diferencia como distribuidor con un portfolio de soluciones enfocadas en Zero Trust entre las que destacan las ofrecidas por:

Palo Alto Networks ofrece soluciones que permiten desplegar de una estrategia Zero Trust, simplificando la gestión de los riesgos y reduciéndola a un solo caso de uso: la eliminación de toda confianza implícita. Independientemente de la situación, el usuario y su ubicación o el medio de acceso, la seguridad se convierte en un único caso de uso que conlleva comprobaciones sumamente rigurosas.

La protección SASE de Palo Alto Networks, conecta el acceso a las redes en la nube con los servicios de seguridad, incluyendo el acceso Zero Trust a la red, ZTNA 2.0. Con una combinación de controles de acceso detallados, según el criterio de privilegio, con la verificación continua de la confianza y una inspección de seguridad profunda e ininterrumpida, se consigue proteger todos los dispositivos, datos y aplicaciones y usuarios, estén donde estén desde una única solución unificada.

Netskope, por su parte, completa el recorrido de la confianza cero a través de las cuatro etapas de transformación de la red, las aplicaciones y los datos con su plataforma Security Service Edge (SSE), preparada para SASE. Su motor de confianza cero analiza las transacciones del negocio con un acceso adaptable basado en la identidad, el contexto de la nube, la confianza de las aplicaciones y los usuarios, y el perfil de los dispositivos, la protección contra amenazas y datos. Todas sus soluciones se basan en este motor central con una consola, un agente y un modelo de políticas para perfeccionar su posición de seguridad con análisis continuado. Adicionalmente, y gracias a Cloud Exchange simplifica la integración de la pila de seguridad mientras que con, NewEdge, la red privada más grande e hiperconectada, ofrece una experiencia superior de usuario y aplicación.

Fortinet ofrece un conjunto completo de capacidades de seguridad y red que van más allá de los elementos básicos de SASE, y entre las que destaca su ZTNA universal. Como parte de (FortiOS), su sistema operativo, ZTNA de Fortinet actúa como punto de aplicación, y el agente ZTNA en FortiClient proporciona la postura del dispositivo y SSO, todo compatible con FortiAuthenticator para la identidad del usuario. La solución implementa una red de puntos de control, orquestada por FortiClient EMS, que permite una arquitectura de baja latencia para poder aplicar inspecciones de seguridad adicionales a los controles ZTNA.

EXCLUSIVE NETWORKS
Exclusive Networks Iberia

Arias. Un problema que concede a los mayoristas un papel esencial en sus labores de formación. La responsable de ciberseguridad de Westcon recuerda que, además, cuentan con acuerdos con universidades. "Somos capaces de ofrecer formaciones técnicas y comerciales al canal. Necesitamos que cada vez más lleguen más conocimientos de ciberseguridad al mercado".

También cuenta TD Synnex con acuerdos con universidades para tratar de generar talento para el sector. Santiago Méndez reconoce que es complicado ya que los recién titulados no cuentan, lógicamente, con toda la formación requerida. "Hay que invertir en formar a esos jóvenes, gestionando la posibilidad de que, una vez formados, puedan moverse a otras compañías", recuerda. Es muy importante retener el talento y reducir la rotación de la plantilla. "Hay que diseñar proyectos atractivos, dar mucha visibilidad a las personas, identificar los talentos importantes y retenerlos; y, por supuesto, no solo con buenos salarios".

En la gestión del talento también es posible fomentar las carreras internas, permitiendo que los profesionales se muevan a otras áreas dentro de las compañías. Ángel García, que defiende el valor creciente de los ciclos formativos (FP), que permiten contar con profesionales en áreas como la preventa, explica que en Arrow cuentan con iniciativas "para identificar a profesionales con perfiles claves, estudiando sus necesidades e inquietudes".

Los mayoristas siempre han sido poderosas canteras de profesionales para los fabricantes y el ecosistema de integradores y distribuidores. Carmen Muñoz explica que es muy importante la capacidad de gestionar este talento. "Hay determinados perfiles que, por su desempeño profesional, siempre tienen su vista puesta en el fabricante. Hay que saber interiorizarlo, gestionarlo bien y maximizar los beneficios de disfrutar de sus capacidades durante el tiempo en el que trabaja en el mayorista".

Martín Trullás apela a la formación dual como una vía para solucionar la falta de talento. "Contrasta el hecho de la escasez de talento con los datos del paro en España", reflexiona. "No hay suficientes programas que permitan una formación dual que combine el estudio de una carrera tecnológica con las prácticas en una empresa", explica. En España este tipo de formación apenas supone el 4 o 5 % en relación a Europa, donde se mueven en porcentajes entre el 17 y el 20 %. Alemania, por ejemplo, alcanza el 85 %. "Hay que empezar a cambiar la forma en la que se educa a los futuros trabajadores", insiste. Y, después, no basta solo con un paquete económico. "Hay que desarrollar planes de retención, que cuenten con suficiente flexibilidad".

Un talento en el que no solo se cuenta con profesionales con perfiles tecnológicos. Arias explica la necesidad de incorporar a las plantillas personas con formación matemática, física o de administración y gestión empresarial. "La implantación, cada vez mayor, de la inteligencia artificial, por ejemplo, requiere de otras especialidades; tenemos, por tanto, que abrir el abanico a nuevas profesiones, ofreciéndoles formación y una visión más holística de lo que es la tecnología. Con ello contamos con más diversidad de talento y ayudamos a que diferentes áreas de conocimiento estén involucradas en la tecnología".

David Gasca
sales & marketing manager cybersecurity en **V-Valley**

"El mayorista es la extensión del equipo del fabricante en aquellas áreas a las que no llega"

Recuerda David Gasca que las nuevas generaciones tienen inquietudes distintas, vinculadas, por ejemplo, con la conciliación o con el compromiso con la ecología o la sostenibilidad. "Lo más importante para desplegar un plan de carrera es la actitud de la persona, más que sus capacidades y cualificaciones". Además de conocer "sus expectativas e inquietudes".

Para Carmen Muñoz se trata de un asunto en el que la educación y la concienciación en edades tempranas es clave. "Nuestros niños y jóvenes están mucho más familiarizados con la tecnología", recuerda. La sociedad debe acometer un cambio cultural. La labor del mayorista, especifica, alcanza la formación y el soporte a su ecosistema de socios, desarrollando una labor de divulgación, pero se necesita, insiste, "un cambio mucho más radical".

Servicios gestionados

Según IDC, los segmentos que mayor crecimiento tendrán este año en el mercado de la ciberseguridad son los relati-

Westcon

El distribuidor de TI que te ofrece las mejores marcas globales de Ciberseguridad y Redes e Infraestructura.

ANOMALI · ATTACKIQ · CERTES NETWORKS · CLAROTY · CROWDSTRIKE

efficient iP™ · Extreme networks · f5 · FIREMON · JUNIPER NETWORKS

MNEMO · NETSCOUT · NOKIA · okta · ōrdr

paloalto NETWORKS · RUCKUS COMMSCOPE · SKYBOX SECURITY · sumo logic · zscaler

Accede a más informaciones sobre nuestros fabricantes en nuestra página web:
https://www.westconcomstor.com/es/es/westcon.html o escanea ese código QR

vos a los servicios gestionados. Carmen Muñoz recuerda que está directamente relacionado con la crisis de talento. "La manera de ayudar a las empresas a invertir en ciberseguridad y a incorporarla como parte de su estrategia de negocio es contar con socios que ofrezcan servicios gestionados, lo que permite a las empresas disfrutar de unos niveles adecuados de seguridad sin una inversión excesiva y sin contar de manera interna con personas especializadas". Su peso, por el momento, no es muy grande pero es un área de crecimiento muy fuerte. "Hay compañías que están muy focalizadas en una estrategia de servicios, con un gran éxito. Son los que han visto la oportunidad y han invertido, dedicando recursos", continúa Carmen Muñoz. La inversión necesaria es una barrera; a lo que se une el nivel de especialización requerido. Ahí entra el soporte del mayorista. "Todas las compañías que inviertan en su propuesta de servicios gestionados van a tener niveles de crecimiento por encima del resto".

También cree Ángel García que los servicios gestionados van a seguir creciendo. "Con su despliegue los *partners* consiguen una diferenciación en relación al resto. Ofreciendo un servicio, el *partner* da un valor añadido al cliente, consiguiendo una mayor rentabilidad en su negocio: mientras que el margen de producto va decayendo cada vez más, los servicios gestionados permiten aumentarlo".

Un despliegue que exige a las compañías una adaptación continua a las tendencias del mercado: nuevos ataques, nuevas tecnologías, el desarrollo de la inteligencia artificial, etc. "Entrar en la rueda de servicios gestionados le permite al *partner* disfrutar de un crecimiento paulatino, a largo plazo. No se trata de vender un proyecto: los servicios gestionados señalan un negocio recurrente y permiten al *partner* ir introduciendo cada vez, más piezas, lo que asegura un negocio rentable a largo plazo", explica el directivo de Arrow. El mayorista cuenta con su propia oferta de servicios gestionados, que pone en manos de su canal, para apoyarle en aquellas áreas en las que éste no llega, por falta de conocimiento o por escasez de profesionales.

Como bien recuerda Martín Trullás, se trata de una tendencia marcada por el cliente. "Las cuentas grandes tienen su propia estrategia de gestión y cuentan con personal especializado capaz de gestionar sus servicios. Sin embargo, en las medianas y las pequeñas, por la falta de talento, la enorme oferta del mercado y la creciente competitividad, no son capaces de gestionar su protección. Y, por ello, la opción de un MSP". Trullás también reivindica el papel del mayorista. "Somos muy importantes en el despliegue de los servicios gestionados. Contamos con políticas propias para proveer a los *partners* que no pueden hacerlo o para complementarles en sus propuestas".

Para David Gasca una gran parte del negocio que siempre se ha movido en el área de la seguridad ha sido gestionado. "Excepto los grandes proyectos, en los que se incluían las renovaciones, en el resto había una capa de servicios gestionados". El mayorista, corrobora, despliega su soporte en aquellas áreas en las que el *partner* no quiere o no puede llegar. "Cada vez damos más capas de servicios gestionados".

Una realidad que alcanza, lógicamente, al escalón de los fabricantes. Arias recuerda que las grandes marcas cuentan con áreas específicas de servicios profesionales y, también, de servicios gestionados. "Se trata de una tendencia de los clientes, que prefieren desplegar un modelo OPEX en lugar de CAPEX". Una fórmula que permite al mayorista "incrementar la fidelización gracias a la renovación, lógica, de los servicios".

Para Santiago Méndez es una oportunidad para todo el ecosistema de distribución. "El *partner* establece un modelo de relación mucho más estrecho con su cliente final, más cercano, satelital", insiste. "Tiene que estar cerca de su cliente, entendiendo su estrategia y sus necesidades". Una fórmula que se sitúa en un reto para el *partner*. "Mantener un servicio gestionado no es sencillo: el *partner* debe manejar la vertiginosa velocidad a la que evolucionan las tecnologías de ciberseguridad. Un reto en el que cuenta con el soporte del canal mayorista".

TD SYNNEX

La Ciberseguridad en bandeja

Facilitamos a nuestro canal soluciones que dan cobertura a todos los segmentos IT más vulnerables a ciberataques.

Seguridad integral

End Point
Identidad y acceso
Contenidos
Seguridad en la red
Seguridad automatizada y monitorización
Seguridad de aplicaciones

¡Destacamos la nueva incorporación de Palo Alto en nuestro catálogo de soluciones!

aruba Instant On
cisco Distributor
IBM Distributor
Lookout
MICRO FOCUS
NETWITNESS
paloalto NETWORKS
radware
RSA
SONICWALL
STORMSHIELD
VERACODE
vmware
WALLIX CYBERSECURITY SIMPLIFIED

Contacta con TD SYNNEX: Security_ES@tdsynnex.es