facebook

twitter

newsbook.es

» La revista del distribuidor informático

Newsbook

Tai editorial

Año XXVII Nº 283 Junio 2021 0,01 Euros

La seguridad sigue siendo una senda rentable para el canal

La seguridad sigue tirando, con soltura, del negocio de los mayoristas

El canal sigue recorriendo el largo, rentable y ambicioso camino de la seguridad

No hay senda fácil. Pero sí segura. E incluso muy rentable. Transitado desde hace décadas por el canal, el camino de la seguridad guarda numerosos recovecos, en forma de mercados jugosos, oportunidades novedosas y tecnologías disruptivas. Una senda jalonada también de retos y de obstáculos que rodear. El recorrido en 2020, allanado por urgencias vinculadas con la protección del teletrabajo, llenó las mochilas de los distribuidores de buenos crecimientos. Ahora, en el tramo de 2021, toca consolidar negocios y afrontar retos tan importantes como la protección en el entorno de la nube o subirse al carro de los servicios gestionados. Nuevas paradas en las que ya están parados mayoristas como Arrow, Exclusive Networks, Ingram Micro, Ireo, Tech Data y V-Valley.

Marilés de Pedro

Negocio al alza

El negocio de la ciberseguridad ha sido uno de los negocios que mejor se ha comportado en los últimos meses en España. El pasado 2020 creció un 8 % y, según IDC, este año, crecerá un 8,1 %, sobrepasando los 1.324 millones de euros.

La inversión en 2020 estuvo centrada en la primera parte del año en el segmento de la empresa privada. Los mayoristas con foco en el área de la mediana y la gran cuenta experimentaron un enorme crecimiento, con proyectos para proteger los despliegues masivos para habilitar el trabajo en remoto. Una inversión que en el último trimestre del pasado

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

"La promoción de soluciones que aúnen a los fabricantes especializados en el mercado de la seguridad con los servicios de los hiperescalares es esencial"

año alcanzó también a la Administración Pública, que empezó a retomar su actividad.

En la primera parte de este 2021, explica David Gasca, coordinador de la unidad de seguridad empresarial en V-Valley, que la empresa privada sigue tirando del mercado de la seguridad. "Están llevando a cabo un proceso de consolidación de las soluciones que adquirieron el pasado año". La necesidad de asegurar la continuidad de negocio condujo a una compra, "en ocasiones, sin control; y ahora, se observa, por ejemplo, una mayor inversión en torno a soluciones de gestión de identidades para controlar y para orquestar".

A juicio de Alberto Pérez, director de desarrollo de negocio de Exclusive Networks Iberia, lo que ha acontecido en España en materia de seguridad en el último año ha sido un proceso natural. "La situación actual ha catalizado el mercado de la seguridad", señala. "Hemos pasado de los *firewalls* y antivirus, en muchos casos básicos, a una inversión de mayor valor", explica. Una inversión, todavía insuficiente, pero que conduce al mercado desde la seguridad a la ciberseguridad. "Estábamos centrados en la protección física y de las comunicaciones, con soluciones alrededor de la infraestructura de seguridad, y ahora estamos dando un salto, doloroso y complejo, hacia la ciberseguridad, donde es fundamental la explotación de los datos, donde juegan un gran papel los analistas, capaces de analizarlos para obtener mejores respuestas ante los incidentes e incluso desplegar estrategias de prevención". Una inversión que, como recuerda, no se hará de golpe, "sino que será progresiva".

"Los distribuidores aún no han aprovechado la enorme oportunidad que ofrece blindar el entorno de la nube"

Álex Benito, *IBM & Next Gen senior manager* de Tech Data, corrobora el crecimiento en áreas como la gestión del acceso de las identidades. "Cada vez hay una mayor demanda en la protección de los accesos a las organizaciones incluyendo, por supuesto, la nube, el acceso VPN o la protección de los dispositivos de los usuarios".

El segmento que más sufrió el pasado año fue la pyme. Chuck Cohen, director general de Ireo, cuyo corazón de negocio está centrado en el entorno de los *partners* medianos y pequeños, recuerda que el pasado año se resintieron mucho con la crisis. "Este año, sin embargo, estamos viendo un fuerte crecimiento, de doble dígito". Cohen explica que están observando un mayor interés en las soluciones de *antiransomware* y en la protección de datos para los entornos de teletrabajo. Sin embargo, todavía queda mucho recorrido. "Sigue habiendo una inmensa mayoría de las empresas que es totalmente vulnerable a los ataques de *ransomware* y a los robos de datos y de identidad", reconoce.

Como asegura Martín Trullás, director del área de Advanced Solutions de Ingram Micro, las pymes tuvieron que aprender a marchas forzadas, adecuando en tiempo récord sus modelos de trabajo a los entornos híbridos. "Es una enorme oportunidad el desarrollo de este mercado, a través del canal, en el que deberá tener un peso muy importante el área de los servicios gestionados".

Se trata de empresas a las que las cuesta ver la inversión en seguridad. Iñaki López, director general de Arrow en España y Portugal, insiste en que son los distribuidores los que tienen que hacer ver a las

Panorama de amenazas

No fueron ataques diferentes, ni utilizaron técnicas distintas, pero fueron más masivos, usaron nuevos ganchos vinculados con la covid-19 y se aprovecharon de la vulnerabilidad de seguridad que desencadenó la adopción masiva del teletrabajo, las conexiones permanentes a Internet o el consumo desorbitado de las plataformas digitales. Ese fue el panorama que se pintó durante 2020 en el terreno de las amenazas y que ha continuado, sin bajar la virulencia, a lo largo de este 2021.

Un panorama en el que los ataques de *ransomware* siguen ubicados en el número uno. Según Fortinet, el *ransomware* se multiplicó por siete en el segundo semestre de 2020. Check Point, por su parte, calcula que en el mundo se produce, cada 10 segundos, un ataque de estas características a una empresa. Señala el fabricante que en el tercer trimestre del pasado año, se incrementaron también los ataques dirigidos contra sistemas de acceso remoto como RDP y VPN.

Calculan los proveedores que en el entorno del *ransomware* va cobrando más peso, como práctica delictiva más frecuente, el de doble extorsión, un ciberataque que implica la amenaza de liberar datos robados de la empresa y que ha llegado a provocar casi la mitad de los incidentes de este tipo de ciberataques. Además, los ataques han cobrado una dimensión "dirigida": se realizan contra una víctima elegida con el objetivo de extorsionar. Una víctima, generalmente, de alto perfil, como empresas, organismos públicos estatales y municipales, y organizaciones sanitarias. Estos ataques son mucho más sofisticados (compromiso de red, reconocimiento y persistencia, o movimiento lateral) e implican un pago mucho mayor. Casi un tercio (32 %) de las víctimas de *ransomware* en España pagaron el rescate para recuperar el acceso a sus datos el año pasado, según un estudio global realizado por la empresa de ciberseguridad Kaspersky entre 15.000 consumidores en todo el mundo.

"No hay semana que no nos despertemos con una noticia de un ataque: infraestructuras críticas, sanidad, bancos, etc.", recuerda Iñaki López. Unos ataques que, recuerda, tienen mucha más repercusión que hace unos años. "La entrada en vigor de la GDPR, hace ahora tres años, ha obligado a las empresas a comunicar los ataques de los que son víctimas", recuerda. Por otro lado, el impacto económico que tienen los ataques, alguno de ellos con elevadas cuantías, en ocasiones, de millones de dólares, conduce a que "crezca su número y los grupos de *hackers* que se dedican a ello".

pymes la obligatoriedad de contar con eficaces sistemas de protección. "No están libres de los ataques", recuerda. "Deben acometer la transformación, necesaria para mantener su competitividad, lo que incluye una estrategia de seguridad".

Protección en torno al puesto de trabajo

La protección en torno al puesto de trabajo está siendo, sin duda, la "estrella" en el mercado de la seguridad desde hace un año. "Las amenazas alrededor del puesto de trabajo se han visto incrementadas por la explosión de teletrabajo, lo que obliga a reforzar y a adaptar políticas y procesos en este entorno", recuerda Álex Benito.

Una explosión que ha conducido a una mayor notoriedad de las soluciones de gestión de accesos con privilegios (PAM), en la que todos coinciden. "Aunque no al nivel que esperábamos", puntualiza Cohen. "Es cierto que hemos multiplicado por dos las ventas en esta área, pero sigue siendo la gran asignatura, ya que el despliegue de estas soluciones está muy por debajo de lo que debería ser", razona. Muchos empleados siguen accediendo desde su casa a los sistemas de sus empresas, y en muchos casos siguen haciendo uso de una VPN, sin "utilizar, en muchos casos, soluciones de autenticación multifactor".

Corrobora Alberto Pérez que las empresas siguen sin "trabajar" como debieran la identidad de los usuarios. "La autenticación multifactor debería ser una protección básica cuando los empleados acceden a información confidencial a través de sus aplicaciones corporativas". Para proteger al usuario, asegura, hay mil capas. "Las soluciones VPN no entrarían dentro de la seguridad sino como una aplicación para permitir la conectividad".

> "La seguridad es responsabilidad de las empresas, no de los proveedores de nube pública"

Alberto Pérez,
responsable de desarrollo de negocio de **Exclusive Networks Iberia**

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/ecs/es

ARROW

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

> "Las empresas suben sus aplicativos a la nube, a cualquier proveedor, y piensan que están protegidos. Y no es así"

El responsable de desarrollo de negocio de Exclusive recuerda que hay soluciones muy básicas de gestión de PAM, adaptadas a una pyme, que pueden ser ofrecidas de manera sencilla por los *partners* que, además, pueden mostrar a estas empresas unas buenas prácticas básicas. "No hay mucha cultura de ciberseguridad en la pyme. Ahora bien, todo llegará. Toda mi empatía con estas empresas, que bastantes frentes tienen que cubrir tecnológicamente como para llegar a este nivel de ciberseguridad".

David Gasca apela al concepto, complementario, del Zero Trust. "Una vez que pasó el *boom* de las VPN, que fue clave el pasado año y en el que vendimos "todo", empezamos a poner foco en Zero Trust: con independencia de si el usuario tiene sus credenciales, confianza cero, lo que obliga a la verificación con soluciones PAM", insiste. A su juicio, el año pasado se generó la demanda y "ahora los *partners* están desarrollando negocio en torno a este concepto".

El siguiente paso lo marca el SASE, un concepto que apela a una arquitectura de red que combina capacidades de VPN y SD-WAN con funciones de seguridad para los entornos de la nube (agentes de seguridad de acceso a la nube, cortafuegos, Zero Trust, etc.). "Los fabricantes ya están apelando a esta nueva nomenclatura que identifica la protección del acceso al puesto de trabajo desde el perímetro hasta la nube", recuerda Martín Trullás. "No solo crece la protección avanzada del puesto de trabajo con soluciones que integran *antiransomware*, *antiexploit*, *antiphishing*, etc.; sino también hay una mayor preocupación por la protección de la red, con soluciones SD-WAN". También se ha producido un salto cualitativo en la adopción de soluciones EDR *(Endpoint Detection and Response)*, para analizar el comportamiento del usuario, y su integración con los elementos de seguridad de red (XDR, MDR), que añaden capacidades de *machine learning* y de inteligencia artificial. "Este tipo de soluciones ha experimentado un enorme crecimiento", recuerda Iñaki López. En este 2021, también ha seguido creciendo los entornos vinculados con la virtualización del puesto de trabajo. "En estos entornos, donde se han ido acoplando, con el tiempo, muchos servicios, la seguridad se ha convertido en un elemento clave", razona.

El crecimiento del comercio electrónico también ha impulsado la protección de las aplicaciones que lo permiten con redes CDN o soluciones WAF (cortafuegos para aplicaciones web). "Ha habido un cambio enorme en los hábitos de los compradores que se han decantado por la compra *online*", explica David Gasca. Incluso las pymes, que también están abriendo su negocio hacia esta vía. "Hay muchas oportunidades de negocio en torno a la seguridad en este entorno".

> "Sigue habiendo una inmensa mayoría de las empresas que es totalmente vulnerable a los ataques de *ransomware* y a los robos de datos y de identidad"

Chuck Cohen,
director general de **Ireo**

vinzeo

V-Valley
the Value of esprinet

GTI Software & Networking

Ciberseguridad Corporativa

McAfee
IPS · CASB · EPP · Mobile · ATP · Sec Content · EDR · SIEM · DLP

Microsoft
CASB · EPP · IAM · IRM

Check Point SOFTWARE TECHNOLOGIES LTD.
NGFW · IPS · DDoS · Este/Oeste · vSec · CASB · EPP · Mobile · ATP · VPN · Encryption · Sec Content

A10
DDoS · ADC · SSLi

PulseSecure
IdP · Mobile · ADC · VPN · NAC · SDP

BROADCOM connecting everything
Management IT · IAM · SSO · Intelligent Automation

CounterCraft
Honey Pot · Deception · Threat Hunting

kaspersky
EPP · Mobile · ATP · EDR · Sec Content · Encryption

SONICWALL
NGFW · IPS · vSec · ATP · EDR · Sec Content · VPN · WIFI

CLOUDFLARE
DDoS · DNS SEC · CDN · WAF

ENTRUST
HSM · Secure PKI · Digital Sign · IAM · MFA

BACKBOX
Intelligent Automation

solarwinds
Management IT

aruba a Hewlett Packard Enterprise company
VPN · UEBA · WIFI

cybereason
EPP · EDR · Threat Hunting

NETWORK SECURITY · ENDPOINT SECURITY · SECURITY MANAGEMENT
CLOUD SECURITY · IDENTITY SECURITY · INFORMATION SECURITY
DIGITAL SIGN & PKI · CONTENT SECURITY · INFRASTRUCTURE SECURITY

www.v-valley.es seguridad@v-valley.com
BARCELONA · BILBAO · MADRID · LISBOA · SEVILLA · ZARAGOZA

La asignatura pendiente: la protección en la nube

La seguridad en el entorno de la nube sigue siendo un reto. Y, a la vez, una oportunidad. Según el fabricante Proofpoint, en el último año, los atacantes se han dirigido al 95 % de las organizaciones con la intención de comprometer cuentas en la *cloud*. El 52 % de las empresas ha sufrido, al menos, una vulneración de este tipo en 2020 y entre estas compañías afectadas, más del 30 % ha registrado otras acciones después de que los ciberdelincuentes accedieran a las cuentas, como manipulación de archivos, reenvío de correos electrónicos y actividad OAuth.

Datos que dejan claro el enorme camino que queda por recorrer a la seguridad en este entorno. Y, por ende, al canal. Alberto Pérez cree que los distribuidores aún no han aprovechado la enorme oportunidad que ofrece blindar este entorno. "Bastante han tenido las empresas con subir las cargas a la nube", pinta en el panorama de los clientes finales. "Sigue habiendo una falta de cultura brutal", razona. A su juicio, las empresas creen que, en los entornos de nube pública, la seguridad es responsabilidad del proveedor en el que las cargas están alojadas (AWS, Google, Microsoft Azure, etc.). "Las herramientas más avanzadas para proteger estos entornos son propiedad de los fabricantes específicos de seguridad, tanto de los tradicionales como algunos, más jóvenes, que están lanzando soluciones muy novedosas y ambiciosas para esos entornos", recuerda. "La seguridad es responsabilidad de las empresas, no de los proveedores de nube pública", insiste.

El reto no es sencillo. "Los entornos en la nube evolucionan a una gran velocidad: cada día surge una solución o una arquitectura nueva", reconoce el directivo de Exclusive Networks. "Las empresas ya contaban con sus entornos virtuales protegidos, por ejemplo; y, de repente, cobran relevancia los contenedores, y deben volver a aprender".

Martín Trullás reconoce que hay mucho desconocimiento de las cargas alojadas en la nube. "Existe mucho descontrol", alerta. E incide en la falsa sensación de seguridad que tienen

Movilidad, ese eterno camino por descubrir

Los dispositivos móviles siguen estando en el punto de mira. A raíz de la pandemia y del teletrabajo, miles de dispositivos se unieron a las redes corporativas. Unos dispositivos móviles que, si no están debidamente protegidos, son una posible brecha de seguridad para que los ciberdelincuentes se aprovechen de ella, lo que ha aumentado la preocupación de las empresas por el BYOD. Según calcula Check Point el pasado año un 46 % de las empresas tuvieron, al menos, un empleado que descargó una aplicación móvil maliciosa y casi todas las compañías experimentaron, al menos, un ataque de *malware* móvil.

La gran pregunta es si esta brecha ha elevado, por fin, la protección y la gestión de los dispositivos, uno de los ámbitos en los que ha existido menos inversión. "Al terminal se le ha dado por imposible, sobre todo en las grandes empresas", explica Alberto Pérez. El software para gestionar los dispositivos móviles (MDM), a su juicio, no limita prácticamente nada, lo que ha conducido a las empresas hacia el uso de las tecnologías UEBA *(User and Entity Behavior Analytics)*, basadas en la detección del comportamiento de los usuarios.

Reconoce que Exclusive destinó inversiones al desarrollo de MDM e incluso los principales proveedores de seguridad cuentan con soluciones para la protección de los dispositivos pero, con el tiempo, "se ha ido diluyendo". Se ha demostrado, insiste, en que aunque haya brechas en los terminales "estas son mucho menos serias que las que se abren en torno a la identidad o al dato. Por ello, resulta más efectivo llevar a cabo una política efectiva de gestión de identidades".

En una línea parecida se expresa David Gasca que reconoce que las soluciones para proteger los dispositivos móviles se utilizan muy poco. "Hay proyectos pequeños y medianos pero la gran empresa pocas veces se embarca en la problemática de la gestión de los dispositivos, optando por políticas de Zero Trust y de aplicaciones PAM que protegen al usuario, independientemente del dispositivo. Con estas herramientas la empresa diseña una estrategia de gestión de accesos y de identidades, con una visibilidad completa del comportamiento de los usuarios", relata. "Es una manera más sensata de abordar un proyecto".

Para Chuck Cohen, debe haber un cambio, enorme, en la manera en la que las grandes empresas observan los dispositivos móviles. "No está muy claro cómo deben gestionar los dispositivos que no son corporativos. Es muy difícil proteger un dispositivo que no puedes controlar. Y muchas están mirando para otro lado".

Más optimista se muestra Álex Benito que recuerda que Tech Data sigue apostando por el desarrollo de soluciones MDM para gestionar y tener acceso seguro a través de los móviles, cuyo mercado no ha dejado de crecer en los últimos años. "Estoy convencido de que va a haber un desarrollo más importante en este apartado".

Martín Trullás introduce en este juego a las operadoras, que parece que han observado en este entorno un campo de oportunidad. "Pueden venderlo como un servicio, aunando la protección del entorno colaborativo de trabajo y el ámbito personal".

INGRAM MICRO
Advanced Solutions

IngramMicro | Financial Solutions

Advanced Solutions

Advanced Solutions, la División de Valor de Ingram Micro para integradores especializados en tecnologías de Datacenter. Servidores, almacenamiento, ciberseguridad, networking, virtualización y software empresarial.

- HPE DIVISION
- CISCO DIVISION
- SERVERS & STORAGE
- VIRTUALIZATION & MOBILITY
- NETWORKING & SECURITY
- POWER & COOLING

Life Is On APC by Schneider Electric
aruba a Hewlett Packard Enterprise company
Barracuda
cisco Partner Distribution Partner
cisco Meraki
citrix
DATACORE
EATON Powering Business Worldwide
flexxible IT Leading a revolution in digital transformation
FUJITSU
Hewlett Packard Enterprise
McAfee
Praim Transforming Enterprise Computing
PURE STORAGE
riello ups
RSA
SONICWALL
SOPHOS
VERTIV

Para más información: 902 902 750 - www.ingrammicro.es - comercial@ingrammicro.es

> "Cada vez hay una mayor demanda en la protección de los accesos a las organizaciones incluyendo, por supuesto, la nube, el acceso VPN o la protección de los dispositivos de los usuarios"

Álex Benito,
IBM & Next Gen senior manager de **Tech Data**

las empresas. "Suben sus aplicativos a la nube, a cualquier proveedor, y piensan que están protegidos. Y no es así". Un desconocimiento que se extiende al canal. "A los distribuidores tradicionales, que no han trabajado en este entorno, con un negocio centrado en la venta de infraestructura, les cuesta mucho entender el cambio de concepto y a quién le corresponde la responsabilidad de la seguridad". Junto a ellos, trabajan con un canal, que nacido en el *cloud*, lo tiene más claro.

David Gasca insiste en que "el consumo de cargas y de aplicaciones en la nube es mucho mayor que la inversión en seguridad que debería acompañarlo". Ejemplo claro es el consumo de Microsoft 365, desorbitado el año pasado, que no ha tenido su parangón en seguridad. "El número de planes Enterprise con Microsoft 365 que no tienen ningún tipo de protección es muy alto", asegura. Es un mercado pintado por cientos de empresas, que cuentan con miles de buzones. "La oportunidad en torno a su protección, con estrategias de venta cruzada de soluciones, es enorme para el canal, no solo con la seguridad sino también con los servicios que se pueden generar alrededor", insiste.

Más optimista se muestra Chuck Cohen en torno a la protección de Microsoft 365 ya que es una de las áreas que más está creciendo en Ireo. "La oferta de los fabricantes en este apartado no deja de crecer, con numerosas soluciones de *backup*, por ejemplo", recuerda. La mentalidad está cambiando y, aunque queda mucho camino por recorrer, Cohen asegura que hay proveedores de servicios, pequeños y medianos, que están aprovechando la oportunidad que se abre en este entorno. "Venden a través de la confianza que ofre-

Tech Data

Advanced Solutions

LA CIBERSEGURIDAD EN BANDEJA

Acercamos a nuestro canal las **soluciones que dan cobertura a los segmentos IT más vulnerables a ciberataques**. Conoce nuestro portfolio y el equipo que ponemos a tu disposición, y verás cómo podemos colaborar para **dar respuesta a las demandas de ciberseguridad de tus clientes.**

01. End Point

02. Identidad y acceso

03. Contenidos

04. Seguridad en la red

05. Seguridad automatizada y monitorización

06. End Point

Contacta con Tech Data: **Security_ES@techdata.com**

Carbon Black. · cisco · IBM · Lookout · MICRO FOCUS · radware · RSA

Secureworks · SONICWALL · STORMSHIELD · VERACODE · vmware · WALLIX

"Estamos observando una mayor inversión en torno a las soluciones de gestión de identidades"

David Gasca,
coordinador de la unidad de seguridad empresarial en **V-Valley**

cen a sus clientes, haciéndoles llegar este mensaje de necesidad de protección".

También Iñaki López cree que el canal, aunque sea parcialmente, está aprovechando esta oportunidad en torno a la nube. "Aunque quede mucho camino por recorrer en la protección de este entorno, sí que estamos desarrollando negocio". Incide en el papel del mayorista de ayudar al canal a concienciar a sus clientes de la necesidad de proteger los entornos con soluciones específicas de seguridad; más allá de la oferta del hiperescalar. "La promoción de soluciones que aúnen a los fabricantes de nicho con los servicios de los hiperescalares es esencial".

Antes de abordar la seguridad, Álex Benito reconoce la excelente trayectoria que presenta en Tech Data el negocio de la nube, que presentó el año pasado un crecimiento por encima del 30 %. "Ha sido, sigue siendo y será una enorme oportunidad de negocio para todo nuestro canal". Reconoce, sin embargo, que cosa distinta es el grado de seguridad que presentan las cargas y las aplicaciones en este entorno. "El canal se está formando a marchas forzadas", reconoce. El mayorista cuenta con una herramienta, Tech Data Cloud Practice Builder, para ayudar a identificar al socio en qué punto se encuentran en la adopción del *cloud* y el grado de seguridad que exhiben los servicios ubicados en este entorno. "Se trata de mostrarles las posibilidades de recorrido que tienen y, por supuesto, acompañarles en la consecución de sus objetivos".

El mercado de la seguridad camina hacia SASE, un concepto que apela a una arquitectura de red que combina capacidades de VPN y SD-WAN con funciones de seguridad para los entornos de la nube

Las plataformas con las que cuentan los mayoristas se tornan esenciales. Iñaki López insiste en que es muy importante contar con un *marketplace*, con una oferta potente, en el que se combinen los servicios de los hiperescalares como las soluciones de los diferentes fabricantes. "ArrowSphere permite a nuestros distribuidores diseñar, de forma más sencilla, la oferta que van a presentar a sus clientes". Caso similar sucede con Tech Data, con su StreamOne, que acaba de estrenar nueva versión; el *martketplace* de Ingram Micro o las más recientes del grupo Esprinet y de Exclusive Network.

Servicios gestionados...

Los servicios gestionados marcan, dicen todos los expertos, el futuro del mercado. Un modelo que identifica no solo la venta de soluciones bajo un modelo de pago por uso sino la capacidad del distribuidor de proporcionar sus servicios, arropando la solución. "Son los clientes de nuestros distribuidores los que les están pidiendo, cada vez más este modelo, basado en los servicios y con una fórmula financiera flexible en el que se trata de pasar del CAPEX al OPEX", recuerda Iñaki López. "El distribuidor puede enriquecerlo con sus propios servicios".

Se trata de un modelo de negocio muchísimo más rentable que el tradicional. "Los distribuidores que apuestan por este modelo tienen unos ingresos recurrentes", recuerda David Gasca. Ahora bien, puntualiza, vender una licencia en un modelo de pago por uso no es ser un proveedor de servicios gestionados. "En el mercado enterprise ya hay algunos *partners* que cuentan con su propio SOC (Centros de Operaciones de Seguridad). E incluso algunos, que no cuentan con estos centros, están empezando a invertir en modelo", explica. Incluso, los modelos de pago por uso que los propios fabricantes están desarrollando cada vez más

X·OD
exclusive networks.
on demand.

Redefiniendo la distribución tradicional

X-OD es la nueva plataforma

on demand

de Exclusive Networks

www.x-od.com

- Transición hacia el modelo as-a-service
- Personalización de servicios: inclusión del hardware y software
- Elección del tipo de suscripción (mensual, trimestral, anual)

Escríbenos a **marketing_iberia@exclusive-networks.com**

Escasez de talento

Según el estudio mundial anual de profesionales de ciberseguridad realizado por la Asociación de Seguridad de Sistemas de Información (ISSA) y la firma de análisis Enterprise Strategy Group (ESG), la falta de talento en ciberseguridad afecta a tres de cada cuatro empresas y es la causa principal del aumento de los incidentes de seguridad.

Un problema al que no es ajeno el segmento de la seguridad en España: hay muy buenos profesionales pero son escasos ante la enorme demanda. Los mayoristas suelen ser una excelente cantera. Iñaki López recuerda que también son muy vulnerables. "Tenemos un modelo muy sensible a la inversión, muy diferente al que tienen los fabricantes, que manejan modelos de compensación muy distintos".

David Gasca lo corrobora. "Se aglutina el talento en aquellas empresas que pueden pagarlo por sus modelos de compensación o por los mayores márgenes que manejan". Lógicamente son los fabricantes los que exhiben mayores capacidades. Sin embargo, poco a poco va creciendo la formación, con más profesionales especializados en este complejo mercado. "La brecha entre demanda y oferta disminuirá", prevé.

La formación, una vez más, se torna camino de perfección. Ante la falta de profesionales en este ámbito, los mayoristas tienen que intensificar la formación. "Además de los cursos específicos, contamos con herramientas de autoevaluación, como es el caso de Alys, que permite al distribuidor identificar su situación en el mercado de la seguridad, el punto que quieren alcanzar y cómo lo pueden llevar cabo; un punto en el que usan la herramienta de Practice Builder", explica Álex Benito.

Cohen, por ejemplo, señala a los profesionales que hacen *hacking* ético como uno de los perfiles más demandados. "Son muy pocos, no bastan para cubrir la demanda y resulta muy difícil retenerles". Para aliviar esta escasez, apela a una mayor oferta de los fabricantes en soluciones de *pentesting*, "totalmente automatizadas".

Alberto Pérez también apuesta por una mayor inversión en tecnologías más disruptivas y avanzadas, que se autogestiones. "La automatización tiene que ser elevada", insiste. "Si no podemos resolverlo a golpe de músculo porque hay escasez, habrá que hacerlo a golpe de cerebro". El director de desarrollo de negocio de Exclusive vuelve a insistir en el desarrollo de los perfiles MSP que permitirán industrializar los servicios y que permitirán que el cliente tenga varios proveedores. "El crecimiento tan desorbitado de la tecnología podrá gestionarse, de manera eficiente y correcta, gracias a la industrialización y la automatización".

Para Martín Trullás la escasez de talentos en el campo de la seguridad es una situación análoga a la que se produjo, hace años, en el segmento de la virtualización. "Cuando esta tecnología apareció, hace lustros, había muy pocos especialistas y eran caros. También los mayoristas nos convertimos en pieza clave para formar a los distribuidores y proporcionar los servicios". Tras un tiempo, la virtualización se convirtió en un servicio homogéneo, lo que alivió la necesidad de un conocimiento especializado. "Con la ciberseguridad sucederá algo similar". También con el papel del canal mayorista que, desde los centros de excelencia, como es el caso de Ingram Micro, tratan de salvar esta escasez, proporcionando el apoyo que necesitan los distribuidores. "Nos convertimos en un integrador de integradores para proporcionar esos servicios especializados". insiste.

permite el acceso a este modelo a *partners* medianos o pequeños. "Poco a poco crece el número de compañías que se han dado cuenta de que, sin hacer una enorme inversión, pueden empezar a desarrollarlo".

El mercado MSP en España es todavía muy inmaduro comparado con otros países. "Tenemos que evolucionar", reconoce Cohen. "Y mucho". Desvela el director general de Ireo que, en España, por ejemplo, apenas se encuentran plataformas PSA *(Profesional Services Automation)* que permiten unificar diferentes herramientas y facturar a las empresas con un perfil de proveedor de servicio.

Martín Trullás observa una gran brecha entre el servicio que ofrecen los grandes integradores, con sus SOC, a las grandes empresas; y el servicio que se ofrece a la pymes, con *partners* que no están capacitados para ofrecer esta fórmula. "Aún falta mucha adopción en el canal", reconoce. "Los mayoristas somos pieza clave en este proceso". En el caso de Ingram Micro sus centros de excelencia sirven de respaldo para ofrecer a toda la capa de integradores de Europa la posibilidad de dar a sus clientes servicios de gestión, de implementación remota y auditorías.

La formación es materia obligada. Álex Benito reconoce que muchos distribuidores están preparándose y formándose para ser capaces de desplegar estos servicios. "Una gran parte del canal está convencido de que tiene que desarrollar los servicios gestionados como una clara vía para exhibir una diferenciación en todo lo que tiene que ver con el *cloud*".

Alberto Pérez apela a la especialización como el camino para desarrollar un perfil MSP que permitirá a los distribuidores desplegar un catálogo de servicio, absolutamente profesionalizado, con SLA definidos y precios competitivos. "Industrializa un modelo, que replica de manera recurrente, y en el que la inversión está adecuadamente repartida entre muchos clientes". Un modelo que debe huir del "servicio a la carta". "A muchos distribuidores les da miedo reconocer: hasta ahí no llego", explica. Hay muchos proyectos en los que el integrador pierde dinero porque el coste de los servicios se dispara y no son capaces de cubrir lo que necesita el cliente. "Esto se evita con una especialización y una oferta de servicios, controlada e industrializada, en la que demuestre su conocimiento".

TRABAJAMOS PARA TI

Nuestro éxito se basa en la confianza
y cercanía con el canal

Soluciones

SEGURIDAD

Soluciones avanzadas que permiten proteger la red, los sistemas y los usuarios corporativos.

ITSM

Soluciones de gestión de servicios TI para empresas de todos los tamaños y presupuestos.

SISTEMAS

Soluciones de nueva generación para sistemas críticos e infraestructuras del Data Center corporativo.

NETWORKING

Soluciones de fabricantes líderes del mercado para redes de cualquier tipo y tamaño.

MSP

Soluciones diseñadas para proveedores de servicios gestionados.

Áreas de NEGOCIO

Soluciones que cubren las necesidades de diferentes áreas del mercado tecnológico actual.

"Tenemos la misión de ayudar a nuestros Partners a hacer crecer su negocio a través de las mejores soluciones, el valor añadido y la diferenciación.

Además, contamos con el respaldo de fabricantes de primer nivel en el sector."

IREO
MAYORISTA DE SOLUCIONES TI

www.ireo.com