linkedin
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai editorial

Año XXXI Nº 327 Junio 2025 0,01 Euros

El **crecimiento** y la **rentabilidad** del **canal** pasan por los **servicios**

La previsión de crecimiento del mercado de la ciberseguridad para este año se prevé que sea entre el 10 y el 12 %

Los servicios gestionados: tránsito obligado para el crecimiento y la rentabilidad del canal

Inversión frente a amenazas. Es la dicotomía, perenne, que marca el paso del mercado de la ciberseguridad. Por un lado, un panorama en el que las amenazas no dejan de crecer, en número, dirección asistida y complejidad; y, del otro, la inversión de las empresas privadas y los organismos públicos, siempre un paso por detrás. De ahí el ritmo endiablado que tiene la innovación y la tecnología centrada en la protección, para tratar de acortar esa distancia. Una tecnología que, desde hace años, debe ir acompañada de una capa de servicios. Ya no basta la solución. Para ello, el concurso del ecosistema de *partners* es esencial, en el que los mayoristas han incrementado su papel. Un plantel del que forman parte ADM Cloud & Services, Arrow, Exclusive Networks, Ingram Micro, TD Synnex, V-Valley y Zaltor

Marilés de Pedro

Panorama de amenazas

A mediados del pasado mes de marzo, INCIBE ofrecía las cifras de ciberataques del año pasado en España: en 2024 los incidentes de ciberseguridad aumentaron un 15 %. Las pérdidas económicas derivadas de estos ataques alcanzaron los 10.000 millones de euros a nivel global, duplicando las cifras del año anterior.

"La combinación de ciberseguridad e inteligencia artificial es crucial"

Álex Benito,
IBM & networking Iberia director en el área Advanced Solutions Iberia de **TD Synnex**

España ocupa el quinto lugar en el ranking mundial de incidentes de *ransomware*, con 58 grandes ataques registrados en solo seis meses, lo que supone un incremento del 38 %. "El *ransomware* sigue creciendo", recuerda Ángel García, director del negocio de seguridad de Arrow, que señala la criticidad de los ataques dirigidos a los sistemas energéticos y a las cadenas de suministro. "Los ataques son, cada vez, más dirigidos y sofisticados. El foco de los ciberdelincuentes ya no solo es paralizar la actividad de las empresas sino conseguir un beneficio económico".

Los ataques provocados desde los estados (ciberguerras) siguen creciendo con las naciones exhibiendo más recursos para desplegar sus amenazas. Cada país diseña estrategias particulares, haciendo uso del *hacktivismo* (*malware* destructivo) en los conflictos bélicos. "Se observa un crecimiento, y una mayor sofisticación, en los ataques diseñados por grupos cibercriminales y que están muy orientados a hacer daño a los gobiernos", señala Martín Trullás, director del área de Advanced Solutions en Ingram Micro.

Con el aumento del trabajo remoto se ha producido un incremento de los ataques al correo electrónico empresarial (BEC) en los que el *hacker*, habiéndolo comprometido, engaña a algún empleado, generalmente directivos de alto nivel o pertenecientes al departamento financiero, para hacer que envíe dinero o revele información confidencial de la empresa. El usuario malintencionado se hace pasar por alguien de confianza y solicita el pago de una factura falsa o pide datos confidenciales para utilizarlos en otra estafa. "Son sofisticadas estafas dirigidas a las personas desde direcciones de correo que simulan ser legítimas", explica Dámaso Ramos, responsable de servicios de ciberseguridad de V-Valley. "Son ataques más dirigidos, más específicos: los *hackers* mejoran la calidad de los ataques y el foco que ponen en determinadas compañías".

Víctor Orive, CEO de ADM Cloud & Services, corrobora que la sofisticación va a seguir creciendo. "Se plantea un reto importante a las empresas que deberán asociarse con los socios adecuados para disfrutar de una cobertura segura, lo que va a implicar una constante inversión en mejores tecnologías".

Según el INCIBE en 2024 los incidentes de ciberseguridad aumentaron un 15 % en España con unas pérdidas económicas de 10.000 millones de euros

¿Mayor brecha entre "buenos" y "malos"?

Un panorama que siempre plantea una discusión: ¿llevan siempre ventaja los *hackers*? Javier Jurado, director de desarrollo de negocio de Exclusive Networks Iberia, asegura que cualquier disrupción tecnológica sigue ensanchando la superficie de ataque. "Contamos con más tecnología y con una mayor agilidad y automatización en los sistemas gracias al concurso de la inteligencia artificial, pero tiene un coste. Quizás los *hackers* vayan un paso por delante", analiza. Sin embargo, cree que las empresas, los organismos públicos y el ecosistema de *partners* están tomando más conciencia de que la ciberseguridad tiene una mayor dimensión de lo que

creían. "Muchas compañías tenían una falsa sensación de seguridad. Y, ahora, con los ataques, se están concienciando de que tienen que cubrir más superficie de ataque y, además, hacer uso de tecnologías vinculadas con la recuperación y la resiliencia".

Álex Benito, IBM & *networking* Iberia director en el área Advanced Solutions Iberia de TD Synnex, agrega el concurso de la sociedad para reducir la brecha. "Solamente se puede acortar si somos capaces de coordinarnos y trabajar de manera colaborativa. Los *hackers* tienen muchos recursos, más si están promovidos por determinados gobiernos, lo que hace muy difícil competir contra ellos", razona.

Joaquín Malo de Molina
chief operating officer de **Zaltor**

Sigue permaneciendo España, por su fortaleza económica, como uno de los países más atacados del mundo con la Administración pública como uno de los sectores "preferidos" por los *hackers*, junto al área educativa y la sanidad. "España es un país vulnerable, objetivo de los malhechores, por razones económicas y políticas", explica Joaquín Malo de Molina, *chief operating officer* de Zaltor. A su juicio, nos hemos convertido en objetivo sin estar preparados. "En otros países la concienciación es mucho mayor aunque nos hemos damos cuenta de que hay un problema real porque han cambiado los paradigmas: los ataques ya no son solo a las grandes empresas", continúa. "Todas las empresas saben que van a ser atacadas: el problema es cuándo. Es esencial observar que la ciberseguridad es una inversión, no un gasto".

¿Hacia dónde se dirige la inversión?

Y, frente a las amenazas, la inversión. Según IDC, el mercado de la ciberseguridad en España alcanzó los 2.729 millones de euros en 2024, lo que representa un crecimiento del 12 % respecto al año anterior. Se espera que esta tendencia continúe, superando los 3.891 millones de euros en 2027, con un crecimiento anual del 12,6 %. 2025 ha empezado con muy buena dinámica, manteniendo buenos ritmos de ascenso.

El pasado año las principales áreas de inversión fueron Zero Trust, las tecnologías alrededor del XDR y la protección de la nube. En este 2025, Álex Benito prevé crecimiento en el área de la protección del IoT y de las infraestructuras críticas. "Se calcula que hay alrededor de 17 millones de sensores activos en el sector industrial. Es uno de los puntos que hay que empezar a controlar porque se prevé un crecimiento importante".

> "Es esencial observar que la ciberseguridad es una inversión, no un gasto"

La nube sigue tirando del mercado. "También estamos notando buenos crecimientos en las áreas del puesto de trabajo y la gestión de identidades", completa Javier Jurado. "Estamos poniendo en marcha algunos proyectos vinculados con la microsegmentación, que siempre ha sido el caballo de batalla de muchos de ellos porque son complejos y requieren muchas horas para los *partners*. Hay una oportunidad de negocio para todos los fabricantes que cuentan con soluciones de microsegmentación sin agente, automatizadas".

Todas las tecnologías alrededor del gobierno del dato señalan otra área de oportunidad. "El dato es la joya de la corona; lo que define a la compañía y señala su diferenciación", recuerda Dámaso Ramos, que refuerza también las oportunidades que se abren en el segmento OT, donde son claves la visibilidad ya que "hay que entender cuál es el parque que hay que proteger; y la gestión de la inteligencia asociada a la máquina, al dispositivo que está en la red industrial".

Martín Trullás hace una diferenciación entre la demanda de la pyme y la de la gran empresa. En el área de la primera, observa que, tras la protección del puesto de trabajo, las pymes están dando un paso más, adoptando tecnologías de EDR, para disfrutar de capacidades de detección y respuesta rápida. "Quieren soluciones más robustas. Se trata de empresas que están evolucionando a tecnologías que formaban parte del negocio *enterprise*". Junto a estas tecnolo-

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

Dámaso Ramos
responsable de servicios de ciberseguridad de **V-Valley**

gías, también está creciendo en las pymes las soluciones en torno a la gestión de identidades y a las tecnologías de doble factor de autenticación. "Son soluciones que se instalaban en la gran empresa y a las que ahora está accediendo la pyme".

La consultora Canalys señala que este año los servicios gestionados crecerán un 12 % en la región de EMEA

Ángel García añade el crecimiento en torno a la automatización en áreas, críticas, como la protección del IoT y los servicios de SOC. "Es esencial automatizar y monitorizar todos los procesos: los recursos con los que cuentan tanto los *partners* como los clientes son finitos y disfrutar de herramientas que permitan agilizar los procesos es muy importante".

El responsable de seguridad de Arrow también resalta el valor de los *bundles*; sobre todo en el área de la pyme. "Debemos ser capaces de construir "paquetes" que incluyan los servicios asociados a las soluciones".

También se refiere Víctor Orive al valor de ofrecer soluciones y servicios de manera conjunta. "Están creciendo los servicios XDR, los vinculados con el SOC y los relacionados con unas copias de seguridad y de *backup* más estables y seguras".

"Para un *partner*, ofrecer un servicio es una obligación"

Los servicios gestionados

La prestación de servicios gestionados marca el paso del crecimiento y de la rentabilidad del canal. La consultora Canalys señala que este año crecerá a doble dígito en las principales regiones a nivel global. En EMEA prevé un crecimiento del 12 %. Joaquín Malo de Molina desvela que es lo que más crece. "Nadie sabe de todo, lo que abre una enorme oportunidad al desarrollo de los servicios", explica. El canal busca el apoyo del mayorista para desplegar en sus clientes todo tipo de servicios, ya que se requiere "conocimiento, tiempo e inversión". Hasta hace poco tiempo "el número de *partners* especialistas en el mercado de los servicios de ciberseguridad era reducido", recuerda. En el escalón mayorista, aunque sí contaban con un recorrido en el despliegue de servicios en otras áreas tecnológicas, "su presencia en el área de la ciberseguridad era más reducida". Sin embargo, el mercado manda y ha provocado, en el caso de Zaltor, un "refuerzo y una reconfiguración del equipo técnico".

Para Dámaso Ramos, ofrecer un servicio se torna en una obligación para el *partner*. "Lo puede desplegar él, de manera directa, o apoyándose en terceras compañías". El papel del mayorista es fundamental. En el caso de V-Valley cuentan con una red conformada, aproximadamente, por 600 *partners* que, de manera recurrente, le solicitan un servicio gestionado, asociado a un *bundle*. "Mientras que los *partners* medianos y grandes llevan el servicio en su ADN, en los más pequeños hay más dificultades", reconoce; sin embargo, "es obligatorio que todos los *partners*, de una manera u otra, sean capaces, no solo de revender la tecnología, sino de ofrecer a sus clientes una capa consultiva, en la que sean capaces de llevar a cabo un análisis de sus necesidades".

Víctor Orive cree que, quien no ofrezca esa capa de servicio, al final, quedará fuera del mercado. "Si no aporta un servicio, puede perder a su cliente". El CEO de ADM Cloud & Services recuerda el poder de la colaboración. "El mayorista, a través de sus plataformas, puede favorecer el establecimiento de alianzas entre diferentes *partners* con el objetivo de ofrecer a sus clientes un servicio completo".

Un papel que también incluye un acompañamiento hasta que el *partner* consiga suficiente masa crítica para rodar por sí mismo. "Diseñar un servicio gestionado no es sencillo: se necesitan recursos, que son escasos; y conocimientos técnicos",

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

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

www.v-valley.com

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

"Las pymes quieren soluciones más robustas: están evolucionando a tecnologías que antes solo instalaban las grandes empresas"

recuerda Javier Jurado, que señala el uso de la inteligencia artificial como una vía de ayuda. "Gracias a ella es posible disfrutar de más prestaciones para diseñar un SOC o un servicio". Se trata de un concepto de "analista aumentado". "Todos los fabricantes están incorporando cada vez más interfaces de lenguaje natural para relacionarse con sus herramientas y facilitar el despliegue de un servicio, sin necesidad de que el analista cuente con conocimientos profundos sobre cómo desplegarlo. Con menos recursos humanos o con técnicos menos formados, es posible empezar a diseñar ciertos servicios, lo que permitirá que algunos *partners* puedan incorporarse a este apartado".

El pasado año las principales áreas de inversión fueron Zero Trust, las tecnologías alrededor del XDR y la protección de la nube

El mayorista, ¿un competidor?

Como generador del mayor margen para el canal, el servicio se torna en un elemento estratégico. El concurso del mayorista, como apoyo en su despliegue, ha suscitado en ocasiones algún recelo para algunos *partners*. "Somos absolutamente complementarios", defiende Martín Trullás. "El mayorista es clave en el desarrollo de los servicios, sobre todo en la pequeña y mediana empresa". En el apartado de las medianas y grandes cuentas, el directivo de Ingram Micro recuerda que CEO y CISO ya no están en la operativa diaria, sino en la gobernanza y en el *compliance*, por lo que "delegan una gran parte de los servicios que quiere implementar en un *partner*, en una empresa de servicios. Los *partners* tradicionales de este mercado de ciberseguridad nunca se han planteado no ofrecer servicios", asegura. Unos servicios, bajo un modelo de pago por uso, que se extienden hasta el SOC. El trabajo del mayorista está claro: "Debemos adaptarnos a las necesidades del *partner* y del mercado", recuerda Ángel García. "Nuestro trabajo es formar y capacitar a los *partners* para conseguir un adecuado nivel de certificación". También en el servicio. "En algunos momentos, bien porque su equipo técnico esté ocupado en un determinado proyecto o porque no cuente con recursos especializados en una cierta tecnología, el mayorista le sirve de soporte". Nunca es competencia. "Si el *partner* necesita ayuda, ahí estamos. Un soporte que no tiene que ver con su tamaño sino con su necesidad de recursos".

Para Joaquín Malo de Molina el principal reto de los servicios lo tiene el mayorista. "Debemos ser un soporte para el *partner*, que tiene que buscar una especialización", explica. "Colaborar con el mayorista es la mejor de las opciones".

Plataforma *versus* especialización

El mercado de la ciberseguridad es enorme, congregando desde fabricantes globales hasta marcas especializadas en el despliegue de soluciones para un entorno completo. Un abanico que abre importantes retos, tanto a los mayoristas como al ecosistema de *partners*, para ordenar su oferta. ¿Qué es más rentable? ¿Apostar por proveedores, con una estrategia global, que ofrecen una protección completa con

INGRAM MICRO®

JUEVES | 02-10-2025

SIMPOSIUM

Fira Barcelona

Impulsando el futuro de la distribución

Fira Barcelona Gran Vía

#IngramMicroSimposium

Víctor Orive
CEO de **ADM Cloud & Services**

un mensaje basado en un modelo de plataforma? O, por el contrario, ¿conformar un catálogo con fabricantes especializados, con soluciones concretas para las diferentes áreas tecnológicas?

En el lado del mayorista, Ángel García recuerda que deben combinar ambos apartados. "Junto a los fabricantes, más tradicionales, con un largo recorrido en el mercado y un gran peso de volumen de facturación; están los proveedores especialistas, con un enfoque específico en una tecnología en concreto".

> Según IDC, el mercado de la ciberseguridad en España alcanzó los 2.729 millones de euros en 2024, lo que representa un crecimiento del 12 % respecto al año anterior

En el caso del *partner*, la estrategia depende de sus clientes y de los recursos y las tecnologías por las que haya apostado. "Existen compañías que han apostado, claramente, por el desarrollo de determinados fabricantes, basado en un modelo de plataforma que aplican a una tipología determinada de clientes o para sectores concretos. Y, por otro lado, hay *partners* que ha decidido apostar por tecnologías específicas, donde hay una capa de servicios de mucho valor", explica el directivo de Arrow.

Muchos fabricantes están tendiendo hacia un modelo de plataforma para proteger todos los entornos. Una estrategia que va más allá de las compras, necesarias en algunos casos para conformar este modelo, y que también apuesta por el desarrollo tecnológico.

> "Si el *partner* no aporta un servicio, tiene el riesgo de perder a su cliente"

Un modelo que defiende la integración con el resto de los fabricantes que, en los entornos en la nube, abre un abanico inmenso con los hiperescalares y con proveedores como Nvidia, por ejemplo.

En el otro lado, la realidad es que los fabricantes especializados están fortaleciendo su estrategia. Son proveedores que tienen claro que se requiere una plataforma, con prestaciones de observabilidad y de gestión, para facilitar el despliegue de sus soluciones en cualquier entorno.

La elección, en cualquier caso, depende del cliente final al que se dirige el *partner*. "Hay compañías que, por su capacidad de inversión, se pueden permitir lo mejor de cada escenario y hay empresas que apuestan por una solución consolidada", explica Dámaso Ramos. El mensaje de plataforma, de cualquier forma, está calando en todas las capas de los clientes: desde el pequeño hasta el grande. "Están adquiriendo una madurez que antes no tenían: ahora ya hay plataformas que ya lo hacen prácticamente todo", explica el responsable de servicios de ciberseguridad de V-Valley.

Para Víctor Orive, las plataformas se tornan en la tendencia natural. "Permiten una cobertura amplia, ajustada a la inversión de las compañías".

Joaquín Malo de Molina cree que el entorno de plataforma es ideal para un tipo de cliente que demanda una protección amplia, completa, sin una casuística específica. "En cambio, cuando una empresa tiene una necesidad concreta, generalmente requiere una solución muy especializada". El reto, a su juicio, está en el mayorista que se ha convertido en un consultor: por qué la plataforma, qué hay detrás, qué servicios puedes dar.

El doble "valor" de la IA

El concurso de la inteligencia artificial observa un doble uso. En el lado de los *hackers*, ha allanado el camino al despliegue de ataques más complejos, mucho más dirigidos y adaptados; y a perfilar el *phishing*. Los fabricantes, por su lado, llevan muchos años haciendo uso de herramientas de *machine*

N-ABLE ADM Cloud & Services edorteam

¿LA DATA IMPORTA?

Save the date

10 JUNIO 2025 | 11:00 H.

¡APÚNTATE YA!

**Se recomienda llegar con 15 min. de antelación.*

N-ABLE, EDORTEAM Y TÚ ► UNA MAÑANA EN MADRID

Casos reales *Soluciones efectivas* *Networking*

GRATIS
**por asistir*

3 meses de N-able
2 meses de Edorteam DLP

Espacio Jorge Juan
Calle de Jorge Juan, 137
28028 · Madrid

te esperamos

Ángel García
director del negocio de seguridad de **Arrow**

"En el uso de la IA la clave es la concienciación"

learning, antecesor natural de la actual inteligencia artificial. ¿Será, por tanto, una herramienta que haga más grande la brecha entre unos y otros; o por el contrario la acortará?

"Lo importante es la inversión", señala Víctor Orive, que alerta del enorme montante del que disfrutan algunos *hackers*, a sueldo de algunos gobiernos, para diseñar ataques a la infraestructura crítica; "cifras que están por encima de las que destinan las empresas en protegerse".

También Javier Jurado apela a la inversión, en este caso, la de los fabricantes. "Llevan mucho más tiempo destinando altas inversiones para integrarla en sus soluciones", reconoce. "Sin embargo, cuando se convierte en un arma, en una vía estratégica para conseguir fines económicos y políticos, los *hackers* están incrementando su uso. La inteligencia artificial generativa ha democratizado el acceso a los ataques: personas que no tenían excesivos conocimientos ni medios, gracias al uso del lenguaje natural, han sido capaces de acortar los tiempos para codificar un *ramsonware* o para hacer una filtración de datos. Lo que antes tardaba semanas ahora son días", explica el director de desarrollo de negocio de Exclusive Networks. El *phishing* se vuelve mucho más persuasivo y dirigido. "En ocasiones, resulta imposible distinguir si ha sido redactado por una máquina o por un humano".

Las normativas, factor de oportunidad

El cumplimiento de las normativas, por parte de las empresas y organismos públicos, supone una enorme oportunidad para el ecosistema tecnológico. Dos son las que marcan el paso en este 2025. Desde el pasado mes de enero rige la Ley de resiliencia operativa digital (DORA), una normativa específica para las entidades financiera que deben establecer requisitos para la gestión del riesgo de las TIC, la notificación de incidentes, la realización de pruebas de resiliencia operativa, el establecimiento de acuerdos de intercambio de ciberamenazas y la monitorización del riesgo de la cadena de suministro de las entidades financieras.

Junto a ella, se está a la espera de la transposición de NIS2, la Directiva Europea de Ciberseguridad, que debería haberse llevado a cabo el pasado 17 de octubre. Una legislación que supone un punto de inflexión en la implementación de medidas de protección en empresas y organismos públicos, ya que obliga a contar con un sistema de ciberseguridad mucho más eficaz.

Álex Benito reconoce que se está empezando a observar un cierto crecimiento. "Esperamos que sirvan de impulso al negocio, especialmente en temas de formación alrededor del desarrollo de soluciones que ayuden a cumplir con ambas normas, en áreas concretas como la monitorización o la gestión de incidencias".

Martín Trullás insiste en la evangelización. "Las empresas deben cumplir con ciertos requerimientos, lo que les debe conducir a sus *partners* de confianza: en Ingram Micro estamos llevando a cabo campañas para que informen a sus clientes de sus obligaciones".

La labor del mayorista es "hacer ver al ecosistema de *partners* la enorme oportunidad de negocio que supone", insiste Joaquín Malo de Molina. "El *partner* debe convertirse en el consultor de confianza de sus clientes: debe ser capaz de entender la normativa y mostrar a sus clientes la manera de cumplir con ella, con las tecnologías precisas para ello".

Especialmente crítica es la cadena de suministro: NIS2 obliga a que todos los proveedores que formen parte del ecosistema de negocio de las empresas que deben cumplir con la normativa, también estén conformes con ella. "Las pequeñas empresas, que no se sentían concernidas, se han dado cuenta de que, al formar parte de la cadena de suministro de grandes empresas, que sí están requeridas por la normativa, deben cumplir también con ella", señala Javier Jurado. Unas empresas, con recursos limitados, que están demandando "opciones en formato MSP o *bundles* que ofrecen una solución completa, aunando las tecnologías de varios fabricantes".

TD SYNNEX

¿Listos para liderar el futuro de la ciberseguridad?

El momento es ahora.

Las soluciones y servicios gestionados de ciberseguridad no son una opción, son el pilar de cualquier estrategia y tu cliente los necesita. Descubre cómo te podemos ayudar en esta nueva realidad.

Contacta con TD SYNNEX y te ayudamos a liderar el futuro.

Security_ES@tdsynnex.com

Javier Jurado
director de desarrollo de negocio de **Exclusive Networks** Iberia

"Diseñar un servicio gestionado no es sencillo: se necesitan recursos, que son escasos; y conocimientos técnicos"

Joaquín Malo de Molina cree que, aunque la IA puede estar generando esta brecha, "se trata de una brecha a corto plazo". Aunque reconoce que los ataques son mucho más automáticos, más dirigidos y mucho más complejos "ya hay herramientas que se utilizan para contrarrestar este mal uso de la IA". Álex Benito asegura que la combinación de ciberseguridad e IA es crucial. Según IDC, un 81 % de las empresas está haciendo pilotos (POC) con inteligencia artificial, aunque solo el 20 % tiene ya proyectos que no sean pilotos. Solamente el 1 % de estas empresas está utilizando datos propios. "Aún queda mucho camino de desarrollo para la IA", analiza.

La concienciación y el buen uso deben marcar el camino. Martín Trullás alerta del uso incorrecto de las herramientas que incluyen la IA. "Todo se sube al ChatGPT, lo que incluye los documentos corporativos". Un comportamiento del que empiezan a ser conscientes las empresas. "Se está empezando a trabajar en soluciones de ChatGPT en entornos privados, con herramientas que no estén en la nube".

Se habla de concienciación. "Es la clave", remarca Ángel García. "Es crítico concienciar, tanto a las empresas como a los usuarios, de que lo que se sube a la IA es vulnerable de ser compartido y, por tanto, atacado". Como bien recuerda, todos los empleados deben tenerlo claro, sean cual sean sus competencias. "Hay que cuidar qué se puede publicar y qué es información confidencial".

La nueva ley de IA, que todavía no está implementada, señala el concurso de un IA *compliance manager* "que se encargue de analizar e, incluso, recomendar a las empresas establecer una política interna de su uso de la inteligencia artificial", recuerda Víctor Orive.

En este uso empresarial, Dámaso Ramos recuerda que ya hay compañías que, en el sistema de protección del puesto de trabajo, "ya han implementado sistemas para controlar lo que se hace con la inteligencia artificial y observar qué información o qué documentos son los que se comparten".

Microsegmentación basada en identidad: seguridad dinámica y escalable para redes modernas

En un entorno donde los modelos de trabajo híbrido, la nube y el "edge computing" redefinen continuamente los perímetros tradicionales, las organizaciones necesitan controlar el tráfico interno de red con precisión quirúrgica. En este nuevo escenario, la seguridad ya no puede depender exclusivamente de cortafuegos perimetrales, subredes o VLAN; proteger los activos críticos demanda una gestión minuciosa del tráfico interno.

La microsegmentación es una estrategia avanzada de seguridad que permite crear políticas de control de acceso granulares dentro de la red, definiendo qué dispositivos o identidades pueden comunicarse entre sí, cómo y ante qué condiciones. A diferencia de la segmentación tradicional, la microsegmentación actúa más cerca del endpoint y se apoya en el contexto -como la carga de trabajo, la identidad del usuario o del dispositivo y la aplicación- para definir las políticas de acceso.

Gracias a este enfoque contextual y dinámico, se convierte en una herramienta esencial para afrontar los desafíos de seguridad actuales, al aislar amenazas, limitar el movimiento lateral y adaptarse rápidamente a los cambios sin necesidad de rediseñar la arquitectura de red. Además, es un habilitador fundamental para conseguir la madurez en estrategias Zero Trust, al minimizar brechas, proteger datos críticos, brindar visibilidad y asegurar el cumplimiento normativo, todos ellos elementos clave en arquitecturas híbridas y cloud modernas.

Retos en su adopción

Pese a sus considerables beneficios, la adopción de la microsegmentación aún enfrenta notables barreras. Una de las más críticas es la resistencia al cambio por parte de los equipos de red y seguridad, inquietos ante posibles interrupciones de servicios críticos. A esto se suma la complejidad técnica y operativa que implica aplicar controles manuales en entornos amplios y dinámicos, lo que dificulta su gestión efectiva.

> "Proteger los activos críticos demanda una gestión minuciosa del tráfico interno"

En el caso de las pymes, la situación es aún más compleja. La escasez de recursos y de experiencia técnica pueden frenar la implementación de proyectos que exigen una infraestructura especializada o personal cualificado para su despliegue y mantenimiento.

Por estas razones, resulta fundamental optar por soluciones de microsegmentación que automaticen los procesos, se autoconfiguren y adapten ante cualquier cambio en la red. Estas herramientas, además, deben poder implementarse sin necesidad de rediseñar la red existente y con un esfuerzo operativo mínimo.

Soluciones tecnológicas adecuadas

En la actualidad, las herramientas más eficaces para aplicar microsegmentación son aquellas basadas en la identidad, no en la topología de red. Frente a las soluciones tradicionales, más rígidas y difíciles de escalar ante los cambios, estas plataformas operan sin necesidad de agentes, aprenden automáticamente el comportamiento de usuarios y dispositivos, aplican políticas de acceso de forma distribuida y dinámica y permiten simular sus efectos -de las políticas- antes de aplicarlas, evitando así interrupciones. Todo ello, además, de forma rápida y sin necesidad de complejas configuraciones manuales.

Como especialistas en ciberseguridad, desde Exclusive Networks impulsamos soluciones que, como las de Zero Networks, simplifican la configuración, el despliegue y la gestión, ofreciendo seguridad proactiva, autónoma y escalable para las redes modernas.

Rafael García Pomar
business development manager en Exclusive Networks Iberia

Ciberseguridad: una inversión estratégica para el crecimiento empresarial

Vivimos en un mundo hiperconectado en el que las amenazas digitales avanzan sin descanso. En este entorno la ciberseguridad ya no es un asunto opcional ni exclusivo de las grandes corporaciones. El riesgo de sufrir un ataque es una realidad para empresas de todos los tamaños y sectores, por eso, es imprescindible contar con especialistas capaces de diseñar, implementar y gestionar soluciones que se adapten a cada negocio.

La constante evolución tecnológica en la que nos vemos inmersos es innegable. Las amenazas digitales se han sofisticado, pero también se han hecho más accesibles a ciberdelincuentes con diferentes niveles de experiencia. Se ha producido, además, un cambio en el paradigma de los ciberataques, que ha evolucionado en dos vertientes: por un lado, el target se ha democratizado; hace unos años los delincuentes dirigían sus ataques a grandes corporaciones, ya no. Por otro, se ha vuelto algo inevitable: la experiencia demuestra que ya no tenemos que preguntarnos si seremos atacados, sino cuándo.

Ante esta nueva realidad, es crucial que las empresas entiendan que la seguridad no es un gasto, sino una inversión estratégica que impacta directamente en su crecimiento y estabilidad. Proteger los sistemas, los datos y la infraestructura tecnológica no sólo evita pérdidas económicas, interrupciones en el servicio o filtraciones de información; también optimiza la eficiencia en los procesos internos. El uso de los recursos tecnológicos facilita la integración de nuevas herramientas sin comprometer la seguridad, fortalece la confianza de los clientes y garantiza la estabilidad operativa.

Todas las compañías necesitan protección; pero es evidente que pocas pueden contar con especialistas en ciberseguridad en sus equipos internos, por ello, la seguridad gestionada permite que los expertos diseñen, apliquen y supervisen las medidas de seguridad que se ajustan a las necesidades de cada empresa. Los servicios gestionados de ciberseguridad representan una solución clave que permite externalizar el seguimiento, localización y respuesta ante incidentes sin tener que destinar enormes recursos internos.

Uno de los principales beneficios que aportan es la monitorización continua e integral; los proveedores especializados utilizan tecnologías de detección temprana de amenazas, sistemas de inteligencia artificial y análisis de datos para reconocer patrones sospechosos y mitigar posibles ataques antes de que causen daños significativos. También es clave su respuesta ante los incidentes: en el caso de que se produzca una brecha de seguridad, un equipo capacitado de especialistas puede desarrollar un plan de acción a medida que incluya protocolos de contención, recuperación de datos y análisis forense, garantizando que la empresa pueda retomar su actividad habitual en el menor tiempo posible (y lo menos afectada posible).

Otro punto a tener en cuenta es que los servicios gestionados facilitan el cumplimiento de la legislación vigente. La ciberseguridad está íntimamente relacionada con la protección de datos y la privacidad; en el marco legislativo de normas como el Reglamento General de Protección de Datos (GDPR) en Europa y otras normativas a nivel global, se marcan directrices estrictas que las compañías deben cumplir para evitar sanciones, y, por supuesto, las estrategias diseñadas por los expertos en seguridad gestionada garantizan el cumplimiento de estas regulaciones. Por último, la escalabilidad de los servicios gestionados de ciberseguridad permite que cada empresa reciba un "traje a medida": una solución adaptada a sus necesidades concretas. Una gran corporación precisa infraestructuras más robustas y de alto rendimiento, mientras que las pymes pueden beneficiarse de modelos más flexibles y económicos. La personalización de estos servicios asegura que cualquier compañía, independientemente de su tamaño, tenga acceso a una protección de calidad.

En Zaltor, desde nuestro rol de mayoristas de soluciones de software, animamos a las organizaciones a protegerse: no sólo hay que reaccionar cuando se ha producido algún daño, hay que anticiparse y diseñar estrategias preventivas sólidas que aborden los desafíos actuales, respondan a los desafíos futuros y garanticen la continuidad del negocio.

Joaquín Malo de Molina
Chief operating officer de Zaltor