facebook
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai editorial

Año XXVIII Nº 294 Junio 2022 0,01 Euros

La eterna (y compleja) oportunidad de la seguridad

El desarrollo de los servicios gestionados, materia obligada para el canal

La eterna (y compleja) oportunidad de la seguridad

Sigue siendo uno de los mercados más atractivos y con mayores oportunidades para el canal. La seguridad sigue ganando peso en las inversiones de las empresas. La consolidación de los modelos híbridos de trabajo y el mayor consumo de los recursos de la nube ha conducido a una creciente concienciación en torno a su adecuada protección. Una extensión de la oportunidad que ha crecido pareja a su progresiva complejidad, a la que también han contribuido las amenazas que no dejan de crecer, tanto en número como en sofisticación. Con ello se conforma un panorama en el que el canal mayorista siempre tiene mucho que decir. Siempre cercanos al integrador, al distribuidor, brindan sus capacidades para que la seguridad sea canalizada de manera "sencilla" hasta el cliente final. ALSO-Ireo, Arrow Electronics, Exclusive Networks, Ingram Micro y V-Valley siguen, por tanto, al pie de la oportunidad.

Marilés de Pedro

Si 2020 fue un año excepcional para la seguridad, 2021 no le fue a la zaga y la inversión continuó. Según IDC el mercado en España creció un 8 % en ese ejercicio. En 2022, la consultora prevé un crecimiento del 7,7 %, alcanzando los 1.749,3 millones de euros, y para el año 2025 podría superar la barrera de los 2.200 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito. "Nuestras previsiones de que 2022 volvería a ser un año de muchas oportunidades se están cumpliendo, lo que demuestra que la ciberseguridad sigue siendo una prioridad en los presupuestos de las compañías", ratifica Carmen Muñoz, directora general de Exclusive Networks en España y Portugal. "La protección del puesto de trabajo sigue siendo una prioridad, un punto clave en la estrategia del canal para solucionar los principales riesgos o vulnerabilidades que tienen las compañías", relata. También son prioritarias las tecnologías SASE, el área de la concienciación de los usuarios y la gestión de identidades y autenticación. La directiva, además, apunta que la protección de los entornos industriales empieza a convertirse en una realidad. "Hay muchos integradores y distribuidores que se están especializando, con propuestas muy potentes".

David Gasca, *marketing unit manager Cibersecurity* en V-Valley, completa el panorama con las enormes oportunidades que se generan en la protección de los entornos inalámbricos y SD-WAN; así como la nube, SASE y CASB. "Los clientes están yendo hacia entornos híbridos, lo que exige una estrategia de seguridad con cimientos claros, huyendo de la instalación de soluciones arbitrarias".

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

"La ciberseguridad sigue siendo una prioridad en los presupuestos de las compañías"

La protección del área del puesto de trabajo sigue manteniéndose al alza. Martín Trullás, director del área de Advanced Solutions en Ingram Micro, señala que las tecnologías XDR, MDR y todo lo que tiene que ver con servicios avanzados de detección y gestión del *endpoint* es clave. "También es muy importante la gestión forense, que es un área que sigue creciendo". Ángel García, director de la división de Seguridad en Arrow, corrobora estas buenas perspectivas. "Nuestros principales fabricantes están apostando por ofrecer una solución de seguridad *end to end* a los clientes, bajo una misma plataforma común, que facilite la gestión y la monitorización de los diferentes entornos de seguridad, ya sea con alianzas entre diferentes fabricantes o, de manera exclusiva, con su propia plataforma". Además de la oportunidad que presenta el entorno del puesto de trabajo, por la consolidación de los modelos de trabajo híbridos, García recuerda el auge de la protección del IoT, Zero Trust y la seguridad de las aplicaciones. "La seguridad es una apuesta clara de crecimiento". Chuck Cohen, director general de ALSO Ireo, destaca el esfuerzo de los mayoristas por allanar el camino a los distribuidores para que aprovechen todas las ventanas de estas múltiples oportunidades. "Es esencial proporcionar plataformas y herramientas que les ayuden a hacer más con menos recursos", recuerda. "Gran parte de nuestro valor reside en las plataformas de pago por uso que ayudan a optimizar los costes y les permiten gestionar la facturación de muchos clientes".

Complejo panorama

Este año está resultando especialmente "interesante" desde el punto de vista de la ciberseguridad. Por una parte, motivado por el incremento del número y sofisticación de las amenazas y la falta de habilidades de seguridad que obligan a las organizaciones a repensar su estrategia, y por otra, por la reciente guerra de Rusia y Ucrania, que está multiplicando los ciberataques (especialmente a entidades financieras e infraestructuras críticas), con crecimientos de hasta un 56 % en el número de ciberataques en los últimos dos meses. "Cada vez es más complicado el panorama. El perímetro como tal ya no existe, está diseminado. Y, por tanto, ese perímetro que protegía a la seguridad como tal está muerto. La seguridad hay que llevarla desde el extremo hasta el *cloud* y en cada parte de ese camino tiene que existir una protección total integrada en cuanto a las amenazas", valora Ángel García. "Debe existir una concienciación: las empresas tienen que saber que tienen que invertir una gran parte de sus presupuestos en la protección. Nadie está a salvo de sufrir un ciberataque: empresas grandes, medianas o pequeñas".

Carmen Muñoz corrobora que vivimos un momento complicado. "La situación geopolítica abre muchos frentes, y no solamente desde el punto de vista de la ciberseguridad ante los ataques dirigidos y la ciberguerra, sino por el impacto social y económico que está teniendo. Además, por supuesto, del terrible drama humano", valora. Una coyuntura que, a su juicio, supone un reto enorme para el segmento TIC, lo que incluye a los mayoristas. "Manteniendo la rentabilidad y la eficiencia, hay que seguir ofreciendo el mismo nivel de servicio a nuestros clientes". Muñoz recuerda que los costes están creciendo mientras que el margen de operación desciende, lo que limita la capacidad de inversión del canal en ámbitos como la formación. "Esto, sin embargo, es una oportunidad para seguir destacando nuestra labor

"Se están publicando muchos pliegos para poder cumplir con necesidades muy básicas que deberían estar ya implementadas en la Administración Pública pero que, por falta de inversión, no se habían cubierto"

Chuck Cohen
director general de **ALSO Ireo**

> "Es clave mantenerse al día, observar las tendencias para poder anticiparlas y, por supuesto, buscar los socios adecuados en materia tecnológica"

en el mercado. Sigue siendo una prioridad la prescripción, la formación y poder ayudar al canal, en un momento tan complejo, a arrojar luz sobre la oferta de los fabricantes, cuál es la mejor forma de abordarla y qué modelos son los que mejor funcionan según el mercado al que se dirija. Nuestro papel sigue siendo clave".

La reducción de márgenes sigue siendo cuestión complicada; más en esta época compleja. "El canal está obligado a ser cada vez más competitivo en costes, eficiencias y en optimización; a la vez que las exigencias del mercado son cada vez más difíciles de cumplir, sobre todo por parte de las pymes. Buscar y retener el talento es misión imposible para muchas empresas", valora Chuck Cohen. "Es clave mantenerse al día, observar las tendencias para poder anticiparlas y, por supuesto, buscar los socios adecuados en materia tecnológica".

Martín Trullás apela a la fragmentación del mercado de la ciberseguridad para explicar una buena parte de esa reducción de los márgenes. "Hay muchos fabricantes", recuerda. Unas marcas que compiten en muchos ámbitos tecnológicos dentro de la ciberseguridad, lo que exige un ajuste por parte de los canales. "Cuánto más grande es la oportunidad, en segmentos más altos de mercado, la reducción de los márgenes es mayor. En el segmento de la pyme el margen es más sano; aunque también se está empezando a ver una cierta caída", explica el directivo de Ingram Micro.

No se olvida tampoco de la falta de suministro que afecta a algunos productos de este mercado. "Hay proyectos que se están retrasando", reconoce Trullás. En ocasiones el suministro cubre las grandes oportunidades, lo que deja más desabastecida a la mediana y pequeña empresa, a la que no se puede servir con la suficiente recurrencia. "Vamos a seguir sufriendo la escasez de inventario de diferentes componentes".

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**

> "El mayorista tiene que ayudar al canal para que pueda prestar un servicio de seguridad gestionado"

La retención de talento es otro enorme reto. A la ya consabida falta de profesionales, el proceso de transformación de los modelos laborales ha cambiado las reglas del juego. "Las empresas que no están adaptadas a esta nueva metodología de trabajo son mucho más susceptibles de perder el talento", asegura David Gasca. A su juicio, la pandemia "nos ha hecho ver que tenemos que poner más foco en la calidad de la vida que llevamos. Ya no solo es importante el salario. Hay que ofrecer a las fuerzas laborales, sobre todo a las más jóvenes, prestaciones más interesantes". El responsable de V-Valley asegura que el canal tiene que permitir la flexibilidad. "Clave si va a retener o a captar talento".

Oportunidad en el área pública

El segmento público, motor tecnológico, sigue presentando numerosas carencias en materia de ciberseguridad. En 2021 se asistió a numerosos ataques en los ámbitos públicos (SEPE, INE, el Ministerio de Trabajo o el Área Metropolitana de Barcelona, entre muchos otros) y hay una enorme preocupación por las amenazas que se "construyen" en los entornos industriales, críticos por su actividad. "En el ámbito público hay muchas cosas que hacer", cree Ángel García. "En los entornos industriales siempre han concebido la seguridad bajo la exigencia de la disponibilidad, lo que ha provocado que muchos de ellos sean entornos muy obsoletos, sin segmentar y con muchas carencias", analiza. Para mejorar la protección, el mayorista está ayudando a sus clientes a "desplegar soluciones para mejorar, tanto cuantitativa como cualitativamente, su producción, reduciendo la exposición del riesgo".

David Gasca asegura que una parte de Administración Pública no cuenta con suficiente protección. "Exhibe un nivel muy alto de obsolescencia en sus infraestructuras, lo que ha llevado, por ejemplo, a que haya sufrido numerosos ataques de denegación de servicio". Los fondos NextGenerationUE se tornan claves para aliviar estas carencias. "Se están publicando muchos pliegos para cumplir con necesidades muy básicas que deberían estar ya implementadas en la Administración Pública pero que, por falta de inversión, no se habían cubierto", continúa Gasca.

El responsable de V-Valley no olvida puntualizar que hay que distinguir entre los grandes organismos de la Administración Pública y la AGE, y la administración local, con importantes inversiones en el ámbito local, que están siendo desplegadas en ayuntamientos pequeños, "a las que acceden los *partners* de proximidad".

La oportunidad, por tanto, es enorme. "Quedan muchos entornos *legacy* en la Administración Pública, lo que aumenta la superficie de exposición y más con las nuevas amenazas y los nuevos riesgos", corrobora Carmen Muñoz. "El reto es adecuar al canal a lo que pide la Administración Pública, proporcionándole herramientas que le permitan abordar estos

Ángel García
director de la división de Seguridad de **Arrow**

> "Todos los fabricantes tienden a dar una solución *end to end*"

V-Valley
the Value of esprinet

www.v-valley.es
seguridad@v-valley.com

MAYOR RENTABILIDAD Y VALOR
Ciberseguridad Corporativa

PROPUESTAS DE XaaS
DE ÚLTIMA GENERACIÓN

Seleccionamos e introducimos en el mercado las soluciones más innovadoras para ayudar a las compañías en el crecimiento tecnológico y acelerar su transformación digital.

- Equipo experto
- Tecnologías punteras
- Soluciones adaptativas
- Capacidad financiera

Descubre nuestra propuesta XaaS de última generación.

Network Cloud Workplace Aplicación Dato Gestión

A10 aruba BACKBOX Bitdefender BROADCOM CHECK POINT CLOUDFLARE CounterCraft
CYTOMIC deep instinct ENTRUST Hdiv helpsystems HORNETSECURITY ivanti kaspersky
McAfee MICRO FOCUS solarwinds SONICWALL Trellix TREND MICRO VMRAY WatchGuard

proyectos y que, además, sean viables financieramente. Se trata de transformar la oferta del fabricante y llevarla a un modelo de consumo que pueda dar respuesta a las necesidades, tal y como se plantean dentro de la Administración Pública".

Frente de las pymes

Las pymes son el segmento que menos ha invertido en seguridad. Una tendencia que ha ido cambiando en los últimos años y que, con los fondos NextGenerationUE, puede acelerarse aún más. El Kit Digital, que se puso en marcha el pasado mes de marzo, identifica la iniciativa concreta para estas empresas. La primera fase, dirigida a empresas entre 10 y 49 empleados, cuenta con dos epígrafes concretos para la ciberseguridad (el IX y el X).

Los mayoristas con foco específico en este mercado de la pyme han notado una mayor actividad. V-Valley, con una enorme cobertura de distribuidores que se dedican a servir a este segmento, es uno de ellos. David Gasca asegura que se ha generado mucho interés. "Supone una buena oportunidad para que la pyme aumente su inversión en este apartado", asegura. En el ámbito del *endpoint*, ahora más crítico que nunca, Gasca asegura que la pequeña empresa "está dando un paso más en la implantación de tecnologías EDR o de cualquier otra solución que vaya más allá del mero antivirus".

También Ingram Micro ha llevado a cabo un enorme despliegue de acciones para activar el uso del Kit Digital. "Estamos diseñando paquetes adaptados a pymes por debajo de 50 usuarios; y facilitarlas el acceso a la seguridad", explica Martín Trullás. Por otro lado, están ayudando a que el canal se convierta en agente digitalizador, poniendo en sus manos las herramientas necesarias para que ayuden a sus clientes que aprovechen estos fondos.

No olvida Trullás apelar a la financiación; al músculo financiero necesario para que el canal soporte los proyectos que demandan fabricantes y clientes finales. "Son esenciales los modelos de suscripción", recuerda. "El cliente demanda flexibilidad para poder pagar con una cadencia de meses o, incluso, años. Uno de los pilares del mayorista es soportar esas financiaciones. El fabricante también nos necesita para cerrar los proyectos y, sobre todo, en la gran cuenta".

Un entorno, el de la pyme, en el que encaja como anillo al dedo el modelo de servicio gestionado. "Es la mejor forma de implementar las políticas de seguridad más adecuadas al entorno actual, con una baja inversión, no solamente desde el punto de vista de los recursos económicos, sino también de personal", remata Chuck Cohen.

David Gasca
marketing unit manager Cibersecurity en **V-Valley**

"Los clientes están yendo hacia entornos híbridos, lo que exige una estrategia de seguridad con cimientos claros, huyendo de la instalación de soluciones arbitrarias"

Seguridad en el *cloud*

La oportunidad de proteger el *cloud* se torna fundamental. Un entorno al que quizás los fabricantes de seguridad han accedido más tarde. Ángel García recuerda el papel crítico que tiene la protección, lo que posiblemente haya ralentizado su llegada. "Fue necesario concienciar a las empresas de que la nube era un entorno completamente seguro para alojar sus datos y cargas", recuerda. Junto a esta labor, el debate acerca de quién era el responsable de la seguridad en

La seguridad de red

A pesar de la explosión de la seguridad en los entornos del puesto de trabajo, las empresas no han olvidado la protección de la red. "Se ha roto la barrera entre el entorno de las redes y la seguridad", recuerda Ángel García. Fabricantes tradicionales del mundo del *networking* están yendo hacia la parte de seguridad y, al contrario. "El mensaje común que dan estos fabricantes es que no solo hay que proteger el perímetro, sino también la red", explica. "Todos los fabricantes tienden a dar una solución *end to end*".

Carmen Muñoz recuerda que, de manera tradicional, se priorizó no penalizar el tráfico de red, lo que fue en detrimento de la seguridad. "Es cierto que ha existido más foco en la parte del perímetro; sin embargo, ahora, con el perímetro totalmente abierto, las necesidades de seguridad se han incrementado. Cada vez más, vemos más proyectos de protección de los entornos de las redes corporativas".

Nuevo Cloud Partner Program de Microsoft

¿Por qué un cambio?

Mientras los partners se enfrentan a desafíos nuevos e imprevistos en el entorno empresarial actual, Microsoft Partner Network está evolucionando al siguiente nivel de soporte añadido. El nuevo Programa permitirá identificar las capacidades técnicas y experiencia de los partners en las áreas de soluciones de Microsoft Cloud, así como también demostrar la capacidad de ofrecer resultados de éxito para los clientes.

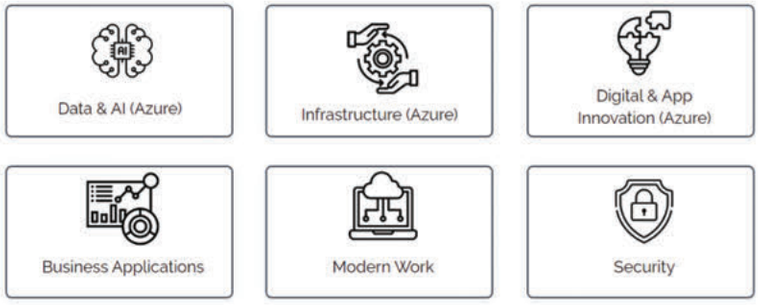
¿Cuándo?

El programa comenzará el **3 de Octubre de 2022**

Aspectos importantes a tener en cuenta

- **Habrá tres niveles de partners**

- Los Solutions Partners serán reconocidos en seis designaciones de **áreas de soluciones**



- Se **mantendrán todas las especializaciones y el estatus de experto.** Microsoft introducirá especializaciones adicionales para ayudar a los partners a destacar aún más.

¿Necesitas más información? Descubre cómo ALSO puede ayudarte

Ingresa en nuestro sitio web y ¡apúntate a nuestros webinars!

Próxima sesión

Jueves, 16 de junio 2022 - 10:00

Lo que necesitas saber sobre el nuevo Cloud Partner Program de Microsoft: sesión 1

este entorno ha provocado que esta tecnología haya escalado más lenta que la subida que desplegó, por ejemplo, la infraestructura. "Sin embargo, la tendencia, imparable, hacia un entorno híbrido en el que haya cargas en un entorno *on-premise* mientras otras estén en la nube, va a acelerar la inversión en seguridad".

Carmen Muñoz apela más al cierto retraso que tiene España en la adopción de la nube para explicar el paso por detrás que exhibe la seguridad en este entorno. "No es un problema de oferta, sino más bien de demanda", explica. También hay que tener en cuenta que la ciberseguridad es un entorno tremendamente complejo; a lo que se suma la carencia de habilidades. "El cliente necesita asesoramiento y control sobre su inversión; lo que no es sencillo".

A su juicio, los fabricantes de seguridad sí se han subido al carro de la seguridad. "Llevan años intentando crear marca en los entornos de los hiperescalares y, de hecho, las alianzas de nuestros principales fabricantes de ciberseguridad con este tipo de compañías tienen años de recorrido", completa la directiva.

> "La seguridad es una apuesta clara de crecimiento"

El canal también debe aprender a jugar en un doble campo. Ángel García recuerda que los *partners* que vienen del mundo tradicional de seguridad están yendo, en mayor o menor medida en función de su perfil, hacia el *cloud*. "Algunos ya cuentan con divisiones específicas para este negocio y otros están empezando a abordar la protección de este entorno", completa. También hay *partners*, nativos *cloud*, que ahora están dando pasos hacia la seguridad. "Los fabricantes tradicionales de seguridad tratan de reclutar y de formar a este tipo de *partners*, que nunca han formado parte de su ecosistema".

David Gasca ofrece otro argumento para explicar este, por el momento, menor despliegue de seguridad en la nube, apelando a su vocación, primigenia, por los modos de suscripción. "La seguridad se vendía bajo estos formatos, que permitían la renovación y el mantenimiento, lo que supuso que cuando la nube se empezó a implementar por la flexibilidad en los costes y la disponibilidad que permitía, la seguridad, que se vendía bajo esos modelos de suscripción, no viera la eficiencia de sumarse a la nube". Sin embargo, ahora, el mercado exige su "conversión" a los modelos de pago por uso. "No siempre es fácil articularlo con herramientas financieras", reconoce.

La falta de talento, cada vez más preocupante

La falta de talento en ciberseguridad es uno de los problemas que se está agravando. El año pasado buscaban empleo en ciberseguridad 39.072 personas, mientras que el número de profesionales necesarios se elevaba a 63.191. Y para el año 2024 se espera que busquen trabajo en este ámbito 42.283 personas, pero la demanda superará las 83.000. Estos datos se desprenden del "Análisis y diagnóstico del talento en ciberseguridad en España", un informe elaborado por ObservaCiber, que se presentó en el marco del pasado MWC2022.

Según recoge el informe, el año pasado se había alcanzado una fuerza laboral en ciberseguridad cercana a los 149.774 trabajadores con una brecha de talento estimada de 24.119. Por tanto, una de las prioridades que tiene la Administración es identificar, atraer, desarrollar y retener el talento en los diversos campos de la ciberseguridad.

INCIBE ha puesto en marcha un proceso de análisis y diagnóstico del talento en ciberseguridad en España, en línea con su Plan Estratégico 2021-2025, que sitúa la promoción y detección del talento en ciberseguridad como objetivo estratégico e identifica la generación de conocimiento sobre ciberseguridad.

El informe destaca que el 40,1 % de las organizaciones consultadas reconoce que reciclan el talento proveniente de otros departamentos hacia el área de ciberseguridad. Sin embargo, solo 2 de cada 10 posiciones internas reciben formación o poseen conocimientos para poder desempeñar las funciones que se requieren.

El estudio también analiza la presencia femenina en el sector e indica que la brecha de género se refleja en la etapa universitaria en la que solo el 18 % de las personas graduadas en esta materia son mujeres.

A pesar de esto el porcentaje de mujeres que han elegido estudiar carreras tecnológicas ha aumentado en 5 puntos porcentuales en 5 años, al pasar del 24 % de mujeres matriculadas en el curso 2016-17, al 29 % de las matriculadas en el curso 2019-20. Al mismo tiempo, la presencia de mujeres en puestos de dirección en seguridad sigue siendo minoritaria.

Por otra parte, las plantillas de los Departamentos de Ciberseguridad de las empresas son pequeñas y la rotación de los perfiles alta.

X·OD

exclusive networks.
on demand.

La era del everything **as-a-service**

Transición hacia el modelo as-a-service

Personalización de servicios: inclusión del hardware y software

Elección del tipo de suscripción (mensual, trimestral, anual)

Ya disponible:

FORTINET paloalto NETWORKS proofpoint SentinelOne wasabi

Más información en **nuestra web**

La seguridad, preocupación al alza

Según las conclusiones que se desprenden del último "Informe de InfoJobs sobre ciberseguridad", la seguridad es una de las principales preocupaciones de las empresas y los trabajadores. De hecho, 8 de cada 10 organizaciones y el 62 % de los trabajadores en España declaran estar preocupados con la ciberseguridad. Esta inquietud aumenta cuanto mayor es el nivel laboral del empleado. Mientras que el 61 % de los especialistas muestran preocupación, en el caso de los directivos esa inquietud sube al 69 %.

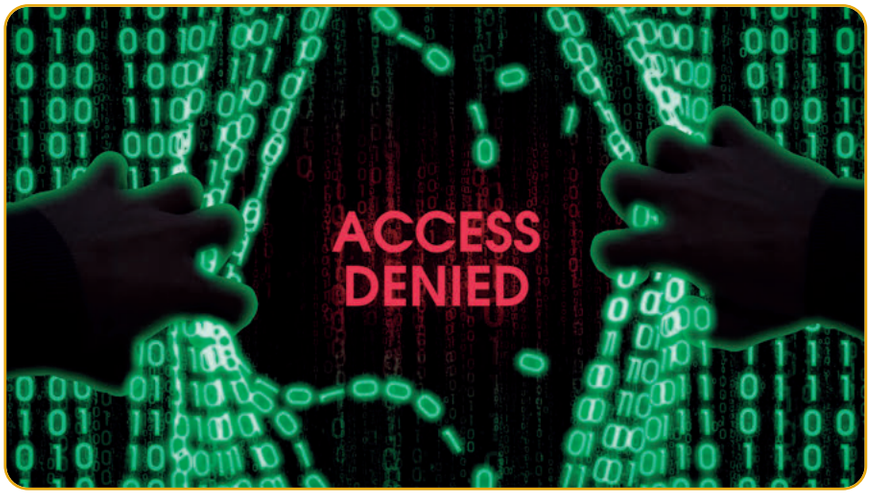
En cuanto a la percepción del hecho de haber sufrido algún ciberataque, el estudio muestra una gran diferencia entre la postura de las empresas y los trabajadores. Solo el 17 % de los empleados son conscientes de haber sufrido algún ciberataque, frente al 44 % de las empresas que declaran haber sido víctimas de algún ataque a sus sistemas informáticos.

Por otro lado, el nivel laboral del empleado también influye en las posibilidades de recibir un ciberataque: a mayor nivel del puesto de trabajo, más probabilidad de ser atacado. 1 de cada 4 profesionales en puestos de dirección comenta haber recibido un ataque informático en sus dispositivos personales durante los últimos doce meses, frente al 15 % de los mandos especialistas.

En cuanto al tipo de empresa, las medianas y grandes son las que sufren más ataques, más de la mitad (56 %) afirma haber recibido algún ciberataque en el último año, proporción que disminuye a cerca de 1 de cada 3 (37 %) entre las pequeñas empresas. Respecto a las medidas de seguridad más utilizadas, las copias de seguridad de archivos importantes (73 %), la protección *antimalware* (65 %) y el almacenamiento de datos en la nube (61 %) son las empleadas por las empresas.

Servicios gestionados, obligatorios

Según IDC, los segmentos que mayor crecimiento tendrán este año son los relativos a los servicios gestionados de seguridad (que crecerán un 11,8 %), servicios de integración (con un 11,8 %) y los servicios de red (un 10,6 %). Son, sin duda, el horizonte hacia el que todos los distribuidores deben mirar.



"Los mayoristas debemos aportar al *partner* las herramientas que les ayuden a prestar servicios gestionados y dar servicios avanzados de ciberseguridad con un mínimo de recursos y de inversión de negocio", explica Chuck Cohen. Muchos *partners*, sin embargo, "siguen empeñados en vender de todo y, además, de golpe. Los distribuidores que intentan maximizar la facturación en una venta inicial no están viendo hacia dónde va el mercado", continúa. "Y los que no se sumen a estos modelos de negocio se van a quedar atrás".

Recuerda Martín Trullás que las empresas lo que piden es un servicio. "Y pagar por él". Una exigencia que no es tan fácil de gestionar, ni de llevarla a la realidad. Más en la pyme. "Muchos *partners* no están preparados para dar ese tipo de servicios gestionados: no tienen talento, les faltan recursos y además su negocio tradicional está perdiendo peso". La oportunidad, por tanto, está clara. "El mayorista tiene que ayudarles, cubriendo sus carencias y proporcionándoles ese nivel de escalabilidad que necesitan para dar servicio a sus clientes finales".

Carmen Muñoz también diferencia entre los modelos *enterprise* y las pymes. "Las aproximaciones son totalmente distintas". En el entorno *enterprise* cree que hay destacados ejemplos de *partners* que tienen una oferta muy buena, que cuentan con una propuesta muy potente y que han hecho grandes inversiones para aprovechar las oportunidades que se presentan en las grandes cuentas. "Hay grandes clientes que han dejado la gestión y el control de su seguridad en manos de este tipo de compañías".

No olvida el concurso del mayorista. "Hay otros *partners* que necesitan complementar sus capacidades. En estos casos desde Exclusive les podemos brindar nuestras propias infraestructuras, nuestra oferta de servicios y los SOC con los que contamos a nivel global". El reto, reconoce, es, en ocasiones, el idioma, que no es en español; y el precio, ya que normalmente el modelo es unificado, y el coste que se marca es muy diferente al que se requiere en España.

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
- CYBERSECURITY
- POWER & COOLING
- DATA MANAGEMENT

Life Is On APC by Schneider Electric | AREXDATA | aruba a Hewlett Packard Enterprise company | authUSB Safe Door | Barracuda | cisco Distributor

cisco Meraki | citrix | DATACORE | Delinea | EATON Powering Business Worldwide | Flexxible IT Leading a revolution in digital transformation

FUJITSU | Hewlett Packard Enterprise | OVERLAND TANDBERG | Praim Transforming Enterprise Computing | Progress | PURE STORAGE | riello ups

RSA | SONICWALL | SOPHOS | submer | Trellix | UiPath | VERTIV

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