facebook
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

editorial

Año XXIII Nº 240 Julio/Agosto 2017 0,01 Euros

La seguridad: oportunidad de negocio inagotable para el canal

Optimismo en el canal mayorista de cara a la segunda parte del año

La seguridad: la oportunidad que no cesa

Los actores que conforman el mercado de la seguridad son unos "privilegiados". El creciente mapa de amenazas, con fenómenos malignos tan virulentos como WannaCry o PetyaWrap; la entrada en vigor el próximo año del GDPR o la perpetua necesidad de protección que presenta el entorno de la nube, señalan solo algunas de las más importantes oportunidades de crecimiento que demuestran que este mercado sigue siendo una fuente inagotable de rentabilidad.

Un área de negocio en el que los mayoristas siguen exhibiendo un enorme protagonismo. Su perfil, variado, demuestra el carácter heterogéneo de un mercado en el que conviven todo tipo de fabricantes: desde los globales que han dado profundidad a su oferta en los últimos años hasta los más especializados que buscan la protección de cualquier rincón empresarial. Cumpliendo su papel de fieles intermediarios, los mayoristas siguen dotando de recursos a sus equipos de seguridad y destinando una considerable inversión al desarrollo de este mercado. ¿La recompensa? Los buenos resultados que exhiben el grupo que conforman Azlan Technology Solutions, Aryan Comunicaciones, Arrow, Exclusive Networks, el grupo Cartronic, Ingram Micro y V-Valley Iberian (la marca de valor de Esprinet).

Marilés de Pedro

Dinámico, cambiante y convulso. Martín Trullás, *next generation technologies division manager* de Azlan Technology Solutions, define con este tridente de epítetos el mercado de la seguridad; un apartado en el que se armoniza el crecimiento de los segmentos más tradicionales, relacionados con el *firewall* o la protección del *endpoint*, con apartados mucho más novedosos identificados con el IoT o la nube. En el caso del mayorista, recién conformada la unidad de valor, que aglutina las "antiguas" fuerzas de Azlan y Avnet (Azlan TS), la seguridad, el IoT, la nube y la imprescindible analítica toman un rango diferenciado. "El IoT es uno de los vectores de crecimiento", insiste. "Es un negocio incipiente que permitirá el crecimiento de la seguridad de la mano de la analítica".

Otra compañía que también ha vivido un reciente proceso de integración ha sido Esprinet. Las compras realizadas el pasado año (primero Vinzeo, posteriormente Itway) han fructificado, en el apartado de valor, en V-Valley Iberian, donde la seguridad desempeña un papel fundamental. Fernando Feliu, *head of marketing and sales* de V-Valley Iberian, recuerda el crecimiento que ha experimentado la cartera de soluciones de algunos fabricantes del área de la seguridad hacia la movilidad o el entorno de la nube, lo que ha ensanchado el campo de actuación de los mayoristas. Feliu insiste en el área de la analítica, al que están accediendo compañías de todo tipo y condición; y en el segmento del IoT. "Democratizar la seguridad acercándola e integrándola en todos los dispositivos y sensores va a ser clave", pronostica. Por último, recuerda el potencial que tiene la seguridad "interna". "Hay que vigilar estrechamente el comportamiento de los usuarios para determinar a qué información pueden acceder y de qué manera", recuerda. "La protección no solo debe cuidar de los riesgos externos: dentro de las compañías el peligro también existe".

Un mercado en el que incluso ha despertado la Administración Pública. Iñaki López, *general manager new tech & service* de Arrow, espera que la aprobación de los presupuestos generales, el pasado mes de mayo, sume proyectos de seguridad. "Junto al mantenimiento del negocio vinculado con el *firewall* o con el UTM están desarrollándose segmentos más nuevos relacionados con el WAF, la protección en torno a los ataques persistentes y dirigidos o los entornos en la nube", corrobora. Unas áreas, cada vez más presentes en el negocio de los clásicos proveedores de seguridad. "En algunos casos pueden mover en torno al 30 o al 40 % de su actual facturación", contabiliza.

La lista de oportunidad alcanza a todo tipo de compañías y de entornos. Antonio Anchustegui, *business manager virtualization, security & networking* de

Juan José Roncero, director comercial de la división de seguridad/redes IP de **Aryan Comunicaciones**

"La seguridad gestionada está creciendo y se está potenciando de la mano de los fabricantes"

Advanced Solutions de Ingram Micro, recuerda que como dianas de ataque se incluyen todas las empresas: aquellas que son susceptibles de un ataque más dirigido y aquellas que sirven de terreno para ataques más indiscriminados. "Los que supone una oportunidad creciente y enorme para vender soluciones y servicios". En el apartado de los entornos con más posibilidades de desarrollar "nuevo" crecimiento los proyectos alrededor del cifrado, aquellos que se encargan de proteger los entornos industriales y los centros de datos; así como la nube (de nuevo). "No solo la seguridad del alojamiento sino también en el acceso a la misma", puntualiza.

La pyme sigue siendo tierra a conquistar. Juan José Roncero, director comercial de la división de seguridad/redes IP de Aryan Comunicaciones, recuerda que es el foco prioritario del mayorista y asegura que su concienciación ha crecido con los años. "La seguridad no era una prioridad en sus inversiones pero, poco a poco, ataques como ha sido el caso de WannaCry han permitido que se popularice la seguridad en las pymes". Unas empresas que han elevado su exigencia. "Ya no se trata solo de proteger el perímetro sino de ofrecerles una oferta más completa que alcanza protección contra el *ransomware* o incluso de recuperación ante desastres", razona.

Carmen Muñoz,
directora general de **Exclusive Networks**

"El mercado de la seguridad crece a doble dígito, algo imposible en otras áreas"

Aunque desde hace un par de años también están empezando a desarrollar, con éxito, el mercado de las medianas cuentas, del lado más alto del mercado se encargan mayoristas como Exclusive Networks. Carmen Muñoz, directora general del mayorista, insiste en la bonanza que presenta el mercado de la seguridad. "Está en constante crecimiento, a doble dígito, algo que no es posible en otros segmentos de mercado". La responsable asegura que muchos clientes han decidido renovar sus plataformas de seguridad en los últimos meses, lo que ha permitido implantar nuevas soluciones en torno a la protección de las APT o en el entorno del puesto de trabajo. "Se han desarrollado proyectos muy interesantes con tecnología que permite la evaluación continua de los sistemas de seguridad, lo que permite detectar dónde se ubican las mayores vulnerabilidades", completa; "en definitiva, una seguridad con un componente mucho más proactivo".

La seguridad que instala el grupo Cartronic identifica un área muy específica de este segmento que afecta a la videovigilancia. Un apartado que José Manuel Fernández, director de marketing y operaciones del mayorista, asegura que cada vez presenta más convergencia con la seguridad TI. "Son dos áreas de la seguridad que se encuentran en plena efervescencia". Una convergencia que reposa en el hecho de que, cada vez más, la seguridad física esté en manos de los gestores TI. "La seguridad física utiliza con más frecuencia sistemas TI que incluyen tecnología de analítica de vídeo y de análisis predictivo; en definitiva, soluciones que están mucho más en el entorno TI". No se trata solo de captar y grabar la información sino también de analizarla. Para llevar a buen puerto este análisis, los sensores que captan y recogen información (las cámaras son los productos más aparentes) han tenido que dar un salto tecnológico. "Se graban las imágenes pero en muchos sistemas la calidad de las mismas no es la adecuada", relata. Por tanto, la oportunidad de desarrollo es enorme. "Hay que instalar sistemas que permitan una grabación con calidad y, sobre todo, que posibilite el reconocimiento facial de las personas, para en algunos casos realizar un análisis forense de lo que está sucediendo para que se puedan tomar medidas preventivas".

¿Qué ha supuesto WannaCry?

La irrupción de WannaCry ha dejado en evidencia, por si alguien todavía dudaba, que la seguridad al 100 % no existe. Ni siquiera al 90 %. "El *ransomware* es la amenaza definitiva", asegura Antonio Anchustegui. "Quien se ve afectado, ve comprometida seriamente la viabilidad de su compañía". A su juicio, ha sido un *malware* que ha cambiado la manera en la que muchas compañías concebían la seguridad.

José Manuel Fernández,
director de marketing y operaciones del **Grupo Cartronic**

"La seguridad física utiliza con más frecuencia soluciones que están mucho más en el entorno TI"

arrowecs.es

Leading Information Technology **distributor**

Five Years Out is not 15 or 20 years from now, because that's science fiction. And it's not tomorrow, because tomorrow is practically yesterday. It is that special place in the very tangible future where what's possible meets what's practical.

Five Years Out

ARROW ECS • Avenida de Europa, 21 Parque Empresarial La Moraleja • 28108 Alcobendas, Madrid
Tel. + 34 91 746 09 52 • Fax +34 91 662 40 04 • marketing.ecs.es@arrow.com

Fernando Feliu,
head of marketing and sales de **V-Valley Iberian**

"Democratizar la seguridad acercándola e integrándola en todos los dispositivos y sensores va a ser clave"

Fernando Feliu recuerda que el *ransomware* es uno de los grandes "negocios" que han surgido en los últimos tiempos. "Es un negocio boyante gracias a la facilidad que exhiben las formas de pago que permiten pagar el rescate a las empresas", asegura. Incluso, hay fórmulas de propagación tan "originales" como liberar a un usuario del pago "si es capaz de infectar a un par más", recuerda. Nunca pagar es la solución. "Si una empresa paga, es susceptible de ser *hackeada* de nuevo".

Su éxito ha mostrado la precariedad que exhiben algunas compañías y los agujeros de seguridad con los que contaban. Asegura Iñaki López que la primera lección que se puede obtener es evidente. "La seguridad tiene que mantener una continuidad y es imprescindible mantener los sistemas y las herramientas permanentemente actualizados".

Sin embargo, a pesar de la virulencia, Carmen Muñoz asegura que la foto española no ha sido excesivamente negativa si se compara con lo que ha sucedido en otros países. "No han existido cortes de servicio", recuerda. Un hecho que ha demostrado lo importante que son las políticas internas que deben ejercer las compañías. "No solo hay que contar con las mejores soluciones sino hay que tenerlas suficientemente actualizadas, lo que incluye una correcta formación interna". Muñoz recuerda que el eslabón más débil sigue siendo el usuario. "Si no está educado, de poco vale la solución o las políticas internas; seguiremos teniendo las mismas brechas".

Lógicamente fenómenos como WannaCry van a permitir al mercado de la seguridad seguir creciendo permitiendo que las inversiones en las empresas no solo sean mayores sino también continuas. Martín Trullás recuerda que son las pymes el colectivo en el que la necesidad de inversión es mayor. "Hay muchas de estas empresas que aún no están concienciadas acerca de este tema", asegura. "Ese es nuestro gran reto: preparar a esas empresas para que se conciencien y perciban que requieren la misma protección que las empresas del Ibex35".

Por último, ha provocado un mayor celo en los fabricantes de seguridad por mejorar sus soluciones. Iñaki López identifica, por ejemplo, que han percibido las vulnerabi-

El IoT, ¿el gran agujero? ¿La gran oportunidad?

La seguridad en torno al IoT es una de las áreas más claras de expansión. Todos los mayoristas, en mayor o menor medida, tienen este mercado en su punto de mira; sin embargo la madurez mercantil es ínfima. En el caso del negocio de valor de Tech Data tiene una ubicación clara. "IoT es un puzzle que incluye un abanico de piezas de soluciones y servicios", apunta Trullás. "La seguridad debe estar embebida en este puzzle", completa. "Se trata de ofrecer al cliente una solución completa en la que le aseguremos que sus datos están seguros; lo que implica una oportunidad para el canal".

Aunque su desarrollo aún es corto, Iñaki López insiste en que ya hay muchos proyectos en este apartado que alcanzan todo tipo de segmentos (incluido, por ejemplo, la explotación ganadera). "Es un mercado enorme y tremendamente ambicioso", define. "Es el futuro pero debe ir definiéndose poco a poco".

Un IoT que abarca desde el propio usuario, con el abanico de dispositivos que le acompañan en su vida, hasta el entorno industrial, de cualquier tipo, con sensores diferentes. "No existen tecnologías estándar y los dispositivos que captan y emiten la información hacen uso de diferentes protocolos", recuerda el director de marketing y operaciones del grupo Cartronic que cree que el caballo de batalla es la protección de estas transmisiones. "Ahora apenas existe seguridad en estos procesos".

La ciberseguridad como oportunidad de negocio

No cabe duda de que estamos en un proceso de cambio donde las amenazas de seguridad han dejado de ser algo que solo afectaba a las grandes corporaciones y multinacionales con importantes intereses económicos.

La popularización de las amenazas está afectando de lleno a la pyme, que por lo general son las mas vulnerables ya que hasta ahora consideraban que sus sistemas y datos no deberían ser importantes para terceros y con ello no deberían ser objeto de ataques. A día de hoy queda claro que nada más lejos de la realidad: los ciberdelincuentes han encontrado un nuevo mercado a explotar con amenazas como WannaCry. Según informes especializados el año pasado se produjeron en España más de 100.000 ataques de los cuales el 70 % afectó a la pyme con un coste medio de 20.000 euros.

Por si fuera poco, todos los expertos del sector concluyen que de manera significativa se han incrementado las amenazas y los riesgos de seguridad en todo tipo de infraestructura empresarial, incluida móviles —aparecen numerosas aplicaciones maliciosas para Android, más de 3,5 millones anuales—. Esta falta de seguridad además está afectando a la implantación de nuevos servicios como aquellos relacionados con el *cloud*.

No cabe duda de que Internet de las cosas ayudará a extender más si cabe la amenaza, no ya al mundo pyme sino incluso a un entorno doméstico.

Las instituciones gubernamentales adquieren conciencia del riesgo latente y endurecen la legislación que insta a tomar medidas más eficientes a la hora de la salvaguarda de los datos de terceros.

Las empresas españolas empiezan a tomar conciencia del riesgo y ya un tercio considera alto o muy alto el riesgo de ciberataques a sus sistemas, mientras que más de la mitad declara haber sufrido ataques.

Sin embargo, las pymes se encuentran con una situación complicada: protegerse de la compleja ciberdelincuencia actual implica invertir en conocimiento y en tecnología; es por ello que según los expertos en seguridad se debería profesionalizar el servicio dejándolo en manos de personal dedicado, lo que apunta a la evolución de un modelo de seguridad gestionado y de servicios en la nube que permita estar siempre con la tecnología más innovadora sin tener que incurrir en grandes inversiones.

En Aryan somos conscientes de estas nuevas necesidades de seguridad y por ese motivo hemos implantado una campaña orientada a ayudar a nuestro canal a adentrarse en este modelo de negocio aportando todo lo necesario:

- **Conocimiento**: plan de formación comercial y técnico, con certificaciones oficiales.
- **Infraestructura y tecnología de seguridad:** acceso al catálogo de soluciones y servicios de los principales fabricantes de seguridad.
- **Procedimientos y expertos en este área.**
- **Posibilidad de externalizar el servicio:** bajo el modo de un servicio de seguridad gestionado.

Esta campaña estará en vigor durante todo el año y tiene como objetivo incrementar el número de *partners* en seguridad en un 30 % con respecto al número actual.

Juan José Roncero,
director comercial de la división de seguridad/redes IP de **Aryan Comunicaciones**

Proveedores globales *versus* especializados

La complejidad del mercado de la seguridad pinta un panorama tecnológico en el que conviven los grandes proveedores, que han extendido su oferta en los últimos años, para exhibir una estrategia de seguridad global, junto a fabricantes que cuentan con potentes tecnologías que permiten cubrir entornos concretos. Dos tipos de proveedores que conviven en una armonía, más o menos perfecta, y que ha conducido en muchos casos a la adquisición por parte de los grandes de las tecnologías, muchas veces punteras, de los especializados.

En principio, las ventajas de llevar a cabo un proyecto implantando la tecnología de un mismo proveedor parece evidente: contar con un proveedor que ofrece todas las capas de seguridad de una forma integrada resulta más sencillo. Aunque no siempre. "Hay que analizar la calidad de cada componente", advierte el representante de Ingram Micro que, sin embargo, recuerda las bondades que han exhibido desde hace años los UTM. "Han resuelto la problemática de la seguridad global aunque con el tiempo se ha demostrado que presentaban carencias en algunos apartados", continúa. Por tanto, el cliente (y, por ende, el canal) debe ofrecer un proyecto en el que se hermanen, de manera adecuada, la seguridad, la administración y la potencia de cada dispositivo.

La especialización, de cualquier manera, es un valor eterno. "Es necesaria", reivindica Iñaki López. "Los fabricantes de nicho han jugado, juegan y jugarán un papel estratégico en el ámbito de la seguridad". A su juicio, la seguridad gestionada es la fórmula más sencilla para permitir que las empresas puedan disfrutar de una plataforma "multifabricante". "Es el canal especializado el que se encarga de gestionarla, aportando su valor en la integración y la gestión".

Incluso hay áreas muy específicas que escapan de la oferta de los grandes. Fernando Feliu es capaz de identificar algunas que están cobrando una gran relevancia. "La encriptación de soluciones como Office 365 o productos que cubren el análisis de comportamiento".

Martín Trullás,
next generation technologies division manager de **Tech Data Azlan**

"El IoT es un negocio incipiente que permitirá el crecimiento de la seguridad de la mano de la analítica"

lidades y agujeros que existen en el tráfico cifrado. "Muchos están poniendo foco en concienciar acerca de la protección en este entorno".

La aplicación del GDPR, "castigo" y concienciación

En mayo de 2018 entrará en vigor el Reglamento General de Protección de Datos (GDPR). Una legislación que representa la evolución natural de la actual Ley Orgánica de Protección de Datos (LOPD) que "escala" al entorno europeo. Como es norma en los lares españoles, el conocimiento y, por tanto, la adaptación que tienen que hacer las empresas para que sus sistemas y sus estructuras estén de acuerdo con la ley deja bastante espacio a la mejora. "En otros países está mucho más avanzado que en España", reconoce Carmen Muñoz.

Los mayoristas están llevando a cabo campañas de concienciación e información para que el canal insista a sus clientes que el tiempo corre en su contra. Sin duda, hay oportunidad de negocio y tecnología suficiente para que las empresas puedan cumplir la ley. "Las grandes corporaciones presentan una mayor concienciación, con profesionales específicos para liderar su aplicación", asegura la directora de Exclusive Networks, "pero muchas otras no han dado el paso y lo ven muy lejano", denuncia.

Alcatel · Alcatel·Lucent · Allied Telesis · APC by Schneider Electric

Array Networks · AUTODESK · BACKBOX · BUFFALO · Check Point Software Technologies Ltd. · DELL EMC

D-Link Building Networks for People · EATON Powering Business Worldwide · FileMaker · Gigaset pro · Hewlett Packard Enterprise · HUAWEI

KASPERSKY lab · KEMP TECHNOLOGIES · Lenovo · Microsoft · NETGEAR · Norton by Symantec

panda · Parallels · Polycom · POSITIVE TECHNOLOGIES · Quest · RICOH

sage · SCALIX Enterprise Class Collaboration · solarwinds msp · SONICWALL · SOPHOS · SPAMINA

THALES · UBIQUITI NETWORKS · VERTIV · Vidyo · wbsgo · Yealink

ZEBRA · ZeedSecurity · ZIGOR · ZYXEL Your Networking Ally

V-VALLEY IBERIAN S.LU, Campus 3·84 - Nave 1, C/Osca, nº 2, Plaza, 50197 Zaragoza - España
Configuracion.Proyectos@esprinet.com

·Barcelona· ·Madrid· ·Zaragoza·

976 76 61 10 · 902 34 99 43

Los servicios gestionados, ¿el futuro?

Muchos fabricantes han puesto foco en los últimos tiempos en el desarrollo de los servicios gestionados de seguridad. Según un estudio de Fortinet, un 44 % de las empresas españolas reconoce que ha externalizado su protección, optando por la contratación de servicios de seguridad gestionada. Unos servicios, lógicamente, que pasan por el canal.

Un modelo que tiene un gran campo de aplicación en la pyme. "Es una fórmula que está creciendo y se está potenciando de la mano de los fabricantes", asegura Juan José Roncero. A su juicio, tiene todo el sentido del mundo teniendo en cuenta que la seguridad es cada vez más compleja. "La gestión debe ser dinámica y con un modelo descentralizado", analiza. "Las pymes disfrutan de las ventajas de contar con protección, gestionada por un socio especializada", remata.

Una tendencia, cada vez mayor, que se refleja en el hecho de que si antes los servicios que oferta un centro de operaciones de seguridad (SOC) solo eran accesibles para las grandes empresas, ahora también las más pequeñas pueden disfrutar de ellos. Incluso compañías que cuentan con 50 empleados. El canal no es ajeno a esta tendencia: muchos integradores ya han dado el salto y han creado sus propios SOC para ofertar servicios de seguridad gestionada a sus clientes.

Un servicio gestionado que también alcanza a la seguridad física. José Manuel Fernández apela al "vídeo como servicio". "La tecnología existe aunque el mercado no está todavía preparado para abordarlo porque no se ha encontrado el modelo adecuado para comercializarlo de manera efectiva y sencilla", analiza.

Iñaki López,
general manager new tech & service de **Arrow**

"La seguridad tiene que mantener una continuidad y es imprescindible mantener los sistemas y las herramientas permanentemente actualizados"

En el caso de las pymes, el panorama resulta más desolador. Juan José Roncero asegura que la predisposición a cumplir la ley de este tipo de compañías es notoria. Lo que no lo es tanto es disponer de expertos que les señalen el camino, asesorándoles para implantar tecnología y mecanismos de funcionamiento. "Lo que abre oportunidades a las consultoras especializadas, tanto en el ámbito de la tecnología como en otros campos, que van a poder ofrecer servicios externalizados de seguridad a las pymes". Una externalización en la que el mayorista puede encontrar su papel en forma de soporte y formación.

El Reglamento contempla, entre otras exigencias, que las empresas deben informar a sus clientes de las brechas de seguridad. Las sanciones por ellas no son pequeñas. Antonio Anchustegui recuerda lo "bien que funciona" en España la amenaza de los castigos. "En este asunto el esfuerzo mayor está por hacer", asegura. "Las empresas, cuando observen la cuantía y la dureza de las sanciones, van a empezar a concienciarse". Una concienciación que vendrá acompañada de una inversión y, por tanto, de mayores oportunidades de negocio. "Al igual que el *ransomware* representa una oportunidad para vender *backup*, el GDPR permite ir más allá de la seguridad informática e integrar en los proyectos tecnología que asegure un acceso protegido a los datos, por ejemplo", insiste. "Es una oportunidad para todo el TI".

De cualquier manera hay que ir más allá de la sanción. Carmen Muñoz está convencida de que lo que más va a

EXCLUSIVE NETWORKS

www.exclusive-networks.es
info@exclusive-networks.com

EXCLUSIVE GROUP,
EL ÚNICO VAST MUNDIAL LÍDER EN INNOVACIÓN DE TECNOLOGÍAS Y SERVICIOS

Exclusive Networks es parte de Exclusive Group, organización que conecta proveedores mundiales de tecnología emergentes y visionarios para los mercados paneuropeos a través de su modelo de distribución de valor añadido VAST (Value Added Services and Technologies). Especializado en los mercados de seguridad, redes, infraestructura, y Data Center para la "Empresa Social Inteligente", Exclusive Group trabaja con miles de socios integradores.

- NG Firewall Platform
- Distributed Denial of Service
- Network Response
- Cloud Access Security Brokerage
- Email Protection
- Endpoint Protection
- File Access and MDM
- Mobile Security
- Key Generation and Management
- Network Plumbing
- Web application Firewall
- Privilege Access Management
- Vulnerability Assessment and Patch Management
- Encryption
- Audit & Compliance
- Endpoint Response
- Network Packet Capture
- Data Protection
- User Entity Behaviour Analytics
- PIM
- SIEM
- Strong Authentication
- Automatization
- Multivendor Management
- Virtual Execution (Sandbox)

C/ Arturo Soria, 336. Planta 8. 28033 Madrid
Tel: +34 902 10 88 72 | Fax: +34 917 662 634

Antonio Anchustegui, *business manager virtualization, security & networking* de Advanced Solutions de **Ingram Micro**

"El *ransomware* es la amenaza definitiva: quien se ve afectado, ve comprometida seriamente la viabilidad del negocio"

mover a las empresas es el impacto que las brechas de seguridad (su comunicación, más bien) van a tener en su reputación. "Su mayor exposición pública va a mover a una mayor inversión".

No falta la demanda de apoyo por parte de la Administración. "Debe existir una predisposición administrativa a ayudar a las pymes a poder instaurar una estrategia de protección de datos", exige Fernando Feliu. "El oro negro del siglo XXI son los datos; representan la energía de las empresas, un bien común por el que deben velar también las políticas de los gobiernos", analiza. A su juicio, y como bien refleja este reglamento, los mercados son cada vez más globales, lo que exige una regulación global para normalizar la actuación en todos los países. "Hay que crear la infraestructura jurídica suficiente para crear la necesidad de la seguridad", remata. Una solicitud a la que se une la directora general de Exclusive Networks. "El papel de la Administración Pública es crucial", corrobora. "Y no solo en España sino a nivel europeo. Es uno de los grandes retos: que sea capaz de acompañar y de proteger".

Los mayoristas exigen, además, una mayor concreción del Reglamento en su aplicación. El representante de Cartronic demanda más claridad en la aplicación del mismo. "Resultaría esencial que se señalara la manera de guardar los datos, de manera adecuada, en la infraestructura apropiada", resume. Pide un formato estándar "que permita a las pymes más pequeñas una aplicación adecuada de la ley".

Mapa de canal

El mercado de la seguridad siempre ha mostrado una complejidad que ha asegurado que fueran los distribuidores que exhibieran un conocimiento en este mercado los que se encargaran de desarrollarlo. Carmen Muñoz mantiene que, a pesar del atractivo que ha mostrado en los últimos tiempos y de la universalización que ha experimentado, los principales nombres especializados en este mercado siguen siendo los mismos. "Es un canal altamente especializado y por la complejidad de la materia, tiene que ser así", afirma. "Es cierto que existen áreas de cooperación y que hay integradores que han sido capaces de desarrollar en su estructura diferentes áreas de negocio, pero el liderazgo corresponde a los mismos socios desde hace mucho tiempo".

Una especialización que parece tornarse obligatoria en las grandes cuentas pero que, sin embargo, parece perder valor a medida que se desciende en la pirámide empresarial. Al menos, así lo cree Martín Trullás que asegura que distribuidores que se han movido en áreas como el almacenamiento, la virtualización o las redes, están accediendo a la seguridad. "Todas las empresas se han dado cuenta, en mayor o menor medida, de la necesidad de estar protegidas y, en principio, se lo demandan al integrador TI con el que trabajan, que ve así una oportunidad".

Es un tipo de socio que aplica a la pyme. En el caso de Aryan Comunicaciones, cuyo foco de negocio es este mercado, Juan José Roncero asegura que el 80 % de los socios que el mayorista ha captado para desarrollar la seguridad no procedían de este mercado. "Son distribuidores que trabajaban con Aryan en otras áreas y a los que hemos ido acercando a la seguridad a través de planes concretos de formación".

Una visión que se comparte en el grupo de valor de Esprinet. Fernando Feliu insiste en la formación como vía de reclutamiento. "Presenta todavía mucho desconocimiento y algunos creen que la seguridad supone simplemente hacer un *backup*", reconoce. El soporte y los servicios del mayorista abren una oportunidad, no sólo a su canal, sino también a él mismo. "Se trata de ofrecer los servicios de seguridad a un mayor número de clientes y con una focalización cada vez más alta".

También se cumple el perfil en Ingram Micro. "Los distribuidores que venden seguridad en las pequeñas, e incluso

Ransomware: Ingram Micro recomienda cómo prevenirlo

No existe una única solución en el mercado que prevenga del ransomware *y ni siquiera todas las medidas correctoras pertenecen al mundo de la seguridad IT. Desde Ingram Micro hacemos las siguientes recomendaciones, basadas en los fabricantes que distribuimos.*

¿Cómo identifico problemas de seguridad?

La herramienta de monitorización continua de la seguridad de **Zeed Security** inspecciona continuamente mi red en busca de problemas, los reporta junto a la solución que debe aplicarse y mediante un sistema de *ticketing* permite vigilar que se solucione.

¿Cómo impido o dificulto la entrada del *ransomware* a mis sistemas?

El parcheo actualizado de los puestos y servidores, de aplicaciones y sistemas operativos, elimina rendijas por las que se nos pueden colar los ataques de *ransomware*. **Symantec Altiris**.

Mediante la protección *antimalware* de puesto prevenimos cualquier amenaza conocida que pueda entrar en nuestros *endpoints*. **Symantec Endpoint Protection 14**.

Mediante un Web Security Gateway **Symantec Bluecoat**, **Barracuda** o un servicio *antimalware* activado en mi *firewall* prevendremos de la entrada de una amenaza en el perímetro. (**Sonicwall**, **Barracuda**, **Juniper**).

Con respecto al correo electrónico los equipos de seguridad de correo electrónico y los servicios *cloud* de filtrado podrán parar los correos que contengan amenazas conocidas. (**Sonicwall**, **Barracuda**, **Symantec**).

Las amenazas desconocidas o Zero-Day pueden ser mitigadas en gran parte con servicios anti-APT de Sandboxing. Buena parte de los fabricantes de seguridad de perímetro y de correo ofrecen esta opción, que analiza cada posible amenaza en un entorno aislado, para estudiar cómo funciona y bloquearla en caso de comportamiento diagnosticado como maligno. (**Sonicwall**, **Barracuda**, **Juniper**).

Hay un fabricante que ofrece soluciones integrales anti-APT que coordinan agente de puesto, solución perimetral y protección del correo. (**Symantec ATP**).

¿Cómo bloqueo la ejecución de *ransomware* cuando el ataque ha sobrepasado mis sistemas de protección?

Debemos asumir que habrá ocasiones en las que ese correo malicioso llegue a su destino. Aun así, no está todo perdido. Utilizando la inteligencia colectiva de los empleados, **Phishme** educa al usuario para reducir al mínimo el clic a correos con *malware* y permite que el usuario alerte a la organización de amenazas no detectadas.

Por otra parte, mediante una adecuada solución de bastionado, es posible proteger los equipos para que no ejecuten procesos no autorizados, como es el *ransomware*. (**Symantec Datacenter Security**).

¿Qué hago en caso de infección?

Un adecuado *backup* permitirá volver a los sistemas a un punto anterior al del incidente. (**Barracuda Backup, Datacore CDP**).

Un novedoso sistema de aplicación de políticas de seguridad desde elementos de seguridad de *switches* y *routers* bloqueará el tráfico desde el equipo afectado. (**Juniper Security Director**).

Antonio Anchustegui
Business manager virtualization, security & networking
División Advanced Solutions de ***Ingram Micro***

Excelente panorama 2017

Cerrada la primera parte del año, en la que el grupo mayorista exhibe crecimiento, el segundo semestre se vislumbra con muy buenas perspectivas. El "repunte" del *ransomware*, con la irrupción el pasado mes de junio de Petya, representa una nueva excusa para seguir vendiendo seguridad. Sin dejar de lado la adecuación al GDPR, hay áreas de oportunidad relacionadas con los entornos WAF, la movilidad, la seguridad en las aplicaciones y el repunte de la seguridad en el puesto de trabajo.

Y en el horizonte, el desarrollo del IoT, la seguridad en la nube, la protección de las áreas inalámbricas y los entornos virtualizados.

Por último, en el creciente mercado de la analítica de vídeo se observa una creciente necesidad de integrar un abanico enorme de elementos, además del vídeo, lo que añade complejidad a la gestión del sistema. Para facilitar la misma, el grupo Cartronic ha invertido en el desarrollo de una plataforma de integración. El pasado mes de julio el mayorista inauguraba un centro de desarrollo encargado de parametrizar la plataforma para aplicaciones verticales concretas para el entorno del transporte, la sanidad, energía, etc.; con la creación de un panel de control que gestione no solo el vídeo sino todos los elementos que emitan datos. Una plataforma que abre numerosas oportunidades al canal de distribución del mayorista en esta segunda parte del año.

en las medianas empresas, son socios generalistas", explica Anchustegui que puntualiza que se ha ganado en complejidad. "Antes, a una empresa le bastaba con un antivirus y un *firewall*, pero ahora requieren soluciones de cifrado o de monitorización; lo que exige al canal una cierta especialización".

También la oferta de los fabricantes se ha adaptado a este tipo de empresas, con una oferta que incluye soluciones estandarizadas, apostando por los modelos de servicios gestionados. Juan José Roncero asegura que una buena parte de su canal está optando, de la mano del fabricante, por esta vía. "Se trata de adaptar los servicios al cliente y de incluir la seguridad, un área que además supone un coste mucho menor que otros apartados tecnológicos". Una idea que apoya Martín Trullás. "Es posible que el canal no especializado ofrezca, en un mismo servicio gestionado, un servidor, un *firewall* y un conmutador", corrobora. "E incluso un PC". A su juicio, se trata de un canal que hace unos años ni se atrevía a vender un *firewall*. "Ahora sí".

Carmen Muñoz, insiste, sin embargo en la dificultad de ofrecer una propuesta global de ciberseguridad, aunque sea en el mercado de las pymes. "No es un mensaje acotado a las grandes empresas", recuerda. "No es lo mismo reclutar socios que desarrollen el mercado de la pyme, basada la propuesta en la implantación de una determinada solución, que acercarse a estas empresas con una propuesta global de ciberseguridad", distingue.

TechData®

NUEVA DIVISIÓN

NEXT GENERATION TECHNOLOGIES

CLOUD

SMART IOT & ANALYTICS

FORMACIÓN Y SERVICIOS PROFESIONALES

SEGURIDAD

NETWORKING

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

www.holatechdata.com - 902 519 251

PSIM: el presente de la seguridad en infraestructuras críticas

Physical Security Information Systems (PSIM) es un software que se utiliza para implementar plataformas de integración de alto nivel con el objetivo de automatizar la gestión y el manejo de situaciones en los centros de operaciones. Debido a que el PSIM funciona, por encima de todos los sistemas existentes, las posibilidades de comunicación y colaboración con nuevos subsistemas son prácticamente ilimitadas.

Esta herramienta facilita la resolución segura, eficaz y oportuna de eventos y alarmas y de gestión de incidencias más complejas que involucran a múltiples alarmas simultáneas en una o más ubicaciones.

Como solución, la plataforma permite a los operadores facilidad para administrar los activos de una instalación, un gran campus o varias ubicaciones dispersas en una ciudad o en todo el mundo.

Es una plataforma de arquitectura abierta que proporciona integración con prácticamente cualquier tipo conocido de sistemas, sensores y dispositivos de seguridad, además de permitir el control de cualquier equipamiento industrial o de sistemas de un edificio, tales como iluminación, climatización, elevadores, control de suministros críticos o gestión del mantenimiento del equipamiento.

El trabajo de un PSIM es unificar la gestión de todos los elementos de una infraestructura, incluida la seguridad física. El elemento clave de un PSIM es su capacidad para integrar subsistemas muy dispares y complejos, así como su interoperabilidad con aplicaciones de terceros, más allá de las operaciones normales de un sistema de gestión de video convencional.

En la mayoría de los casos, las empresas que optan por soluciones PSIM ya cuentan con sistemas de seguridad que han sido previamente instalados o varios sistemas del mismo tipo que les gustaría centralizar, como los sistemas de control de acceso o de video provenientes de varios fabricantes. Los sistemas PSIM también son una opción ideal para organizaciones que tienen, además de los que regulan la seguridad, muchos sistemas diferentes, en múltiples ubicaciones distintas, y necesitan integración para optimizar su control y reducir significativamente los costes OPEX.

Podemos aplicar soluciones PSIM en diferentes entornos y mercados, basta con disponer de, al menos, 3 sistemas o plataformas de gestión diferentes, para que la implantación de un PSIM tenga sentido. Desde un hospital, pasando por edificios de Administraciones Públicas, ayuntamientos, plantas de producción, infraestructuras energéticas, medios de transporte, túneles, peajes, puertos, aeropuertos o cualquier proyecto en torno a las *"smart cities"*, pueden ser el escenario ideal para la implantación de esta herramienta.

Desde Cartronic desarrollamos y ayudamos a implementar proyectos de PSIM, disponiendo de una sala de desarrollo para realizar las pruebas de concepto y facilitar la integración.

El trabajo de un PSIM es unificar la gestión de todos los elementos de una infraestructura, incluida la seguridad física

José Manuel Fernández Cobo
Director de marketing y operaciones del **Grupo Cartronic**