facebook

twitter

newsbook.es

»» La revista del distribuidor informático

Newsbook

Tai editorial

Año XXVI Nº 272 Junio 2020 0,01 Euros

Blindajes de canal

Las empresas aumentan su inversión en torno a la seguridad, lo que ha redundado en el negocio de mayoristas y distribuidores

El canal de seguridad afronta, con fortaleza, su enésima reinvención

Cercanía al distribuidor, soporte a todos los niveles y flexibilidad. El trío, siempre presente en el canal mayorista, ha ganado enteros en las últimas semanas, ante la situación excepcional que estamos viviendo, para ayudar a su red de distribución a mantener su actividad. Había que estar más cerca que nunca del canal y ser más sensible, aún más si cabía, a sus necesidades. Y los mayoristas han dado la talla. En el área de la seguridad, que todos reconocen que ha sido un segmento crítico en este momento excepcional, los distribuidores están viviendo su enésima reinvención para estar a la altura de las nuevas y críticas necesidades de protección que tienen las empresas y la Administración Pública en España. Una reinvención en la que el ramillete de mayoristas conformado por Arrow, Exclusive Networks, GTI, Ingram Micro, Ireo y V-Valley Esprinet, se ofrece a ser, una vez más, una pieza fundamental para apuntalarla.

Marilés de Pedro

Gran respuesta mayorista

La respuesta general del canal mayorista, tras el estado de alarma decretado el pasado mes de marzo en España, estuvo a la altura de las necesidades del canal y de los fabricantes, de los que son brazo extendido. Todos "declararon" la adopción del teletrabajo en todas aquellas áreas en las que era posible, manteniendo como prioridad absoluta la seguridad de los empleados y los clientes. "La reacción de todos los mayoristas ha sido espectacular. Muchos clientes tuvieron situaciones puntuales muy críticas y fuimos capaces de atenderles, incluso antes de que se declarara el sector TIC como servicio esencial", resume, con tino absoluto, Carmen Muñoz, directora general de Exclusive Networks en España y Portugal. "Fue un reto mantener el mismo nivel de servicio y ayudar a los *partners*", continúa. "Todos hemos sido capaces de afrontarlo, consiguiendo que el canal no haya notado ni un ápice de descontrol ni de falta de servicio. Hemos respondido a lo que ha necesitado en momentos tan complicados".

Tras la cancelación de todos los eventos presenciales y el mantenimiento, crítico, de la actividad logística sustentada en los almacenes, preservando la seguridad de los empleados de este apartado, el teletrabajo se instaló como fórmula esencial. "Esta complicada situación ha hecho que una vez más tengamos que reinventarnos en el mundo de la distribución a todos los niveles y en todas las divisiones: preventa, marketing, comercial, etc.", analiza Ángel García, director de la unidad de seguridad y redes de Arrow.

La formación *online* ha sido una de las áreas que ha vivido una explosión en todos los mayoristas, con una enorme aceptación por parte de los distribuidores. Los mayoristas anunciaron la posibilidad de realizar todos los cursos de formación y certificación de forma remota. "Los *partners* están más preparados y están aprovechando mucho este tiempo para formarse y ponerse al día", asegura Chuck Cohen, director general de Ireo, que, como el resto de los mayoristas, han debido redoblar su oferta *online* de cursos para dar cabida a todos los *partners*. "En nuestro caso, la formación más demandada ha sido en torno a la gestión de identidades y la conectividad segura".

Los mayoristas lograron dar continuidad a su negocio. "Era crítico", recuerda Roberto Alonso, *cloud & business director* de GTI. "No solo la formación, sino toda la parte técnica, la estamos llevando a cabo con nuestros clientes de manera telemática", explica. En el despliegue del teletrabajo, que hubiera debido regirse por un plan reposado, primó la urgencia. A pesar de ello, Alonso hace una lectura positiva, asegurando que se ha valorado la enorme flexibilidad y que se ha mantenido, incólume, el espíritu de equipo. "Ahora hay que ser más eficientes y eficaces".

El impacto de la situación en el mapa de distribución, a pesar de todo, ha sido enorme. Antonio Anchustegui, director del área de seguridad de Ingram Micro, reconoce que no va a haber una solución sencilla. "Alguno de nuestros *partners* está pasando por momentos complicados, soportando importantes descensos en su facturación", recuerda. "En el caso de los mayoristas, podemos compensar unos negocios con otros, lo que alivia nuestra situación".

La flexibilidad y el soporte financiero al canal han sido prácticas habituales en los mayoristas. "Hay que ser lo más flexible posible con los clientes para ayudarles en los pagos, las entregas, el soporte, etc.", relata David Gasca, coordinador de

> "También los mayoristas nos hemos tenido que reinventar, adaptándonos a todos y cada uno de los perfiles de nuestros clientes"

Ángel García
director de la unidad de seguridad y redes de Arrow

"Nuestro sector va a seguir muy activo. Ahora sigue siendo clave ayudar a las compañías y a los clientes a hacer frente a los nuevos ataques y las nuevas necesidades en materia de seguridad"

Carmen Muñoz
directora general de Exclusive Networks en España y Portugal

la unidad de seguridad empresarial en V-Valley Esprinet. "Es el momento de flexibilizar ya que no podemos estrangular a nuestros clientes; al contrario, debemos buscar con cada uno de ellos la mejor solución financiera", explica. Una estrategia que también alcanza a los fabricantes. "Muchos de ellos también han practicado esa flexibilidad".

La seguridad, mercado crítico

En un plano más estratégico, Chuck Cohen asegura que los mayoristas supieron anticiparse a las necesidades y enseñar al canal el camino en cuanto a qué productos y tecnologías eran las más adecuadas para afrontar esta nueva situación. "Hemos sabido educar al canal y hemos sacado catálogos de herramientas para permitir un despliegue efectivo del teletrabajo", apunta. Una expansión que supone un cambio de paradigma en la seguridad. "Debe plantearse una nueva manera de entender la protección en las redes", alerta. La urgencia para desplegar el teletrabajo dio prioridad a la conexión y a los equipos, por encima de la seguridad, que no se situó entre esas primigenias prioridades. "Prueba de ello es que se han vendido muchas soluciones de VPN y éstas no son la manera más segura de ofrecer una conexión remota", alerta. De ahí la importancia de dar un paso más y ayudar a los *partners* a ofrecer mejores garantías y dar a la seguridad la importancia que debe tener en el panorama actual. "Estamos viendo una enorme demanda de soluciones de autenticación multifactor, de soluciones de *single sign on* (SSO), de acceso a las aplicaciones y de soluciones CASB (Cloud Access Security Manager)", reconoce.

"Ahora, más que nunca en la historia, hay una gran oportunidad para los *partners* en cuanto a servicios profesionales y en el desarrollo de los servicios gestionados como modo de pago por uso que resuelve muchos problemas"

La adopción masiva del teletrabajo, las conexiones permanentes a Internet, el uso de todo tipo de soluciones de videoconferencia o el consumo desorbitado de las plataformas digitales ha provocado que los ataques, que no han cambiado de fórmulas, hayan crecido de manera desorbitada. "Una gran parte de las plantillas de las empresas está trabajando de manera remota, lo que ha permitido una exposición brutal de los usuarios", recuerda David Gasca. Se "rompió" el perímetro tradicional y éste ahora lo marca el software. Gasca, en la misma línea que Cohen, insiste en el uso intensivo de las VPN, a lo que suma el consumo desorbitado de las herramientas de videoconferencia. Ahora, tras la urgencia, se exige una mejor planificación. "Tras un despliego masivo y rápido de VPN, ahora las empresas se han dado cuenta de que necesitan mayores capacidades o la integra-

Habilite las medidas de **Seguridad**, en cualquier lugar

Garantizar la seguridad de nuestros datos hoy en día, exige una nueva forma de pensar. Las soluciones de seguridad de Arrow le ofrecen una **visión completa de la información**, desde el momento que se generan los datos, hasta el final de su vida. **Proteja los intereses y las posibilidades de su negocio sin limitar a empleados, clientes o proveedores**.

arrow.com/ecs/es

algosec | allot See. Control. Secure. | ARISTA | aruba a Hewlett Packard Enterprise company | Check Point SOFTWARE TECHNOLOGIES LTD. | f5

FIREEYE | Forcepoint | FORTINET | gemalto a Thales company | HUAWEI | IBM Business Partner

Infoblox NEXT LEVEL NETWORKING | ixia A Keysight Business | MICRO FOCUS | NETSCOUT | Pulse Secure | radware Every second counts

splunk> | swivelsecure | Symantec A Division of Broadcom | tenable | TREND MICRO | viewtinet

ARROW I Avenida de Europa, 21, Parque Empresarial La Moraleja - 28108 Alcobendas, Madrid
Telf +34 91 761 21 21 - marketing.ecs.es@arrow.com

ción en los proyectos de controladoras; en definitiva, del desarrollo de proyectos con mayor proyección". Algo parecido ha pasado con el uso de herramientas de videoconferencia como Teams. "El uso ha sido brutal pero ahora, con la expansión de los entornos *multicloud*, se necesita una adecuada protección de la misma".

Precisamente la protección del entorno *cloud* es una enorme oportunidad de negocio: DLP, CASB o el cifrado de las conexiones hacia este entorno. "La seguridad no ha sido una prioridad", insiste Roberto Alonso. "El usuario es la clave: hay que protegerlo y hay que tener un sistema de identificación multifactorial". Tras asegurar que los empleados pudieran trabajar desde sus casas, contaran con las conexiones suficientes y tuvieran acceso a las herramientas que necesitaran, "ahora se abre un nuevo escenario en el que la seguridad es fundamental y en el que hay que cumplir una normativa", explica el responsable de GTI.

Tras décadas vendiendo seguridad perimetral, los nuevos hábitos de los *hackers* y situaciones como las que estamos viviendo, en las que la prioridad es el trabajo en remoto, las soluciones de seguridad en torno al puesto de trabajo han sufrido un renacimiento. "Aunque el *endpoint* de nueva generación no está totalmente implantado, la seguridad en este ámbito no es el drama de hace unos años", explica Antonio Anchustegui. El antivirus, al que colgaron el San Benito durante muchos años de ser una solución, denostada por clientes, *partners* y marcas; ha sufrido una completa transformación. "Se vendía casi al peso, la percepción de la diferencia entre unas y otras soluciones era mínima y la presión de los precios era brutal", recuerda el responsable de la seguridad en Ingram Micro. Ahora hay un cambio importante. "Hay muchas empresas dispuestas a invertir, de manera razonable, en este entorno ya que nos hemos dado cuenta de que la seguridad en el puesto es vital". Una inversión que poco a poco incluye tecnologías EDR. "Lo que ha pasado ha reforzado la tendencia en la que, desde la protección heredada y sustentada en el perímetro, ahora cada vez es más necesario proteger el puesto de trabajo; lo que incluye también la protección de los dispositivos móviles que muchas veces no estaban protegidos correctamente".

Ataques que no cambian y se intensifican

No son ataques diferentes, ni utilizan técnicas distintas, pero son más masivos, usan nuevos ganchos vinculados con la covid-19 y se aprovechan de la vulnerabilidad de seguridad que ha desencadenado la adopción masiva del teletrabajo, las conexiones permanentes a Internet o el consumo desorbitado de las plataformas digitales. Desgraciadamente la covid-19 les ha permitido incrementar el éxito de sus ataques ya que la situación excepcional se tornó en la tormenta perfecta para el cibercrimen, con más usuarios en la red, más vulnerables, con más miedo y que tenían una enorme necesidad de buscar información sobre la pandemia.

Chuck Cohen explica que los atacantes no han entendido (ni entienden) de sectores y que el método más usado ha sido el tradicional *phishing*. "Sigue siendo una de las formas más fáciles para atacar cualquier sector; lo que nos obliga a orientar al canal hacia los escenarios tecnológicos donde hay que apuntalar la seguridad", explica. Escenarios que identifica con la multitud de conexiones inseguras que existen por la urgencia en la implantación del teletrabajo o en cómo ayudar a las empresas a superar retos como el soporte técnico remoto a sus empleados y la conectividad seguridad de proveedores externos a los sistemas internos.

Carmen Muñoz recalca que, más que ataques dirigidos a segmentos concretos, lo que existe son sectores más vulnerables. "Los *hackers* apuntan a todos los sectores y a todas las compañías. Su objetivo principal es buscar las puertas de entrada independientemente del área de negocio en el que opere la compañía". Una afirmación que no es óbice para reconocer que hay segmentos, tradicionalmente mejor blindados, como es el caso de la banca, y otros cuyas barreras son más laxas. En la Administración Pública, recuerda la directiva de Exclusive Networks, la obsolescencia de infraestructuras supone un grave riesgo para la seguridad. "Debería ser uno de los sectores que más invirtiera en materia de seguridad".

El presupuesto también es una variable a tener en cuenta. "Las inversiones se concentran en las grandes empresas: bancos, aseguradoras, grandes cadenas de *retail*, etc.", recuerda David Gasca. En el entorno de la pyme, el directivo de Esprinet V-Valley recomienda al canal "tirar" de flexibilidad. "Será clave el desarrollo de modelos de pago por uso que se irán implementando cada vez más, con servicios que se pagarán en pagos mensuales, trimestrales o anuales; lo que dará mayor protagonismo a todos los socios que tengan un perfil de MSP".

Tampoco el entorno *cloud*, al que muchas empresas han "acudido" ante la falta de infraestructura física, ha contado con suficiente excelencia. Para hacer un uso adecuado del *cloud*, se necesita conocimiento y, además, se requiere seguridad. "Los ataques se propagan a una velocidad de vértigo", alerta Antonio Anchustegui. Un cambio en la configuración del servidor se propaga rápidamente a todas las cargas que la empresa tiene distribuidas, lo que se convierte en un problema muy grave. "Alguno de los ataques más importantes que están sufriendo las compañías estuvieron dirigidos a las nubes públicas en las que las empresas guardan su información".

¿*Hackeando* la recuperación?

En esta fase I de la desescalada vuelven las tertulias a las terrazas madrileñas y se repite con bastante frecuencia cómo el confinamiento ha truncado el deseo de muchos padres de "perderse la infancia de sus hijos". Bromas aparte, estos días de convivencia, roces incluídos, han permitido descubrir gustos y aficiones que antes nos podían pasar desapercibidos. En mi caso, uno de esos descubrimientos, vía filial, ha sido la atracción ejercida sobre alguno de mis hijos por las distopías tecnológicas, tipo "Black Mirror", dentro de ese universo de las series que tanta influencia tienen en la creación de tendencias sociales y en el remodelado de esta nueva normalidad hacia la que avanzamos.

"Mr. Robot" y sus cuatro temporadas han llenado una parte de mi reclusión compartida, siguiendo las andanzas de Elliot Anderson, un brillante ingeniero de ciberseguridad, con problemas de ansiedad social, cuya vida da un giro al ser reclutado por un grupo ciberterrorista. Como decía, las series conforman y anticipan la realidad, una realidad en la que el cibercrimen empieza a superar en ingresos al narcotráfico.

En estos momentos de crisis sanitaria los ataques cibernéticos se han incrementado aprovechando, tanto del uso más intensivo de la Red, como de la situación de mayor vulnerabilidad que ha provocado la improvisación, en muchos casos, de la infraestructura habilitada para teletrabajar o seguir el curso.

Hemos visto circular mensajes con información del covid-19 o de oferta de mascarillas con enlaces que dirigían a páginas falsas con la promesa de regalar muestras y robar así sus datos. También, hemos visto la extensión de *malware* oculto en archivos con supuesta información sobre la pandemia. E incluso algún ataque relevante de *ransomware*.

Desafortunadamente, las amenazas evolucionan muy rápidamente y no es fácil identificar las nuevas vulnerabilidades ni la respuesta más adecuada para cada ataque. La inteligencia artificial se ha revelado como un gran arma de defensa para identificar patrones y actuar en consecuencia. Las grandes compañías, con sus avezados CISO, dan la batalla con grandes inversiones y recursos dedicados.

Sin embargo, para la pyme no es posible lastrar su cuenta de resultados con estos gastos y al partner de proximidad le cuesta igualmente mantener actualizados los conocimientos y los recursos necesarios.

Para cubrir esta necesidad, hemos diseñado en Ingram Micro un abanico de servicios destinados tanto a identificar vulnerabilidades, como a gestionar en tiempo real la cobertura de las mismas.

Hemos diseñado un centro de excelencia en ciberseguridad que provee al canal de servicios preventivos y consultivos, como la ciberseguridad forense, la detección de *malware*, el cumplimiento de normativas y el *hacking* ético.

Una vez realizada la prevención, hay que pasar a la acción. Mantener actualizados los productos y protocolos es muy costoso, así como el personal experto para operarlo. Para ello, nuestro centro de excelencia presta servicios de seguridad gestionada, contando con una amplia gama de productos, tanto de los distribuídos por nosotros como de otros complementarios.

Pasada la crisis, viene la recuperación. Una recuperación que es un entorno VUCA de manual, marcada por la volatilidad, la incertidumbre, la complejidad y la ambigüedad. Debemos trabajar para conseguir esa recuperación en uve que suponga un rebote rápido y vigoroso para nuestra economía, evitando un drama social añadido al sanitario, en todos sus aspectos y vertientes.

"Debemos trabajar para conseguir esa recuperación en uve que suponga un rebote rápido y vigoroso para nuestra economía"

Pongamos los medios para que no *hackeen* nuestra recuperación.

Alberto Pascual,
director ejecutivo de Ingram Micro

> "El usuario es la clave: hay que protegerlo y hay que tener un sistema de identificación multifactorial"

Roberto Alonso
cloud & business director de GTI

Y la prevención. Como bien recuerda Carmen Muñoz, el usuario sigue siendo el eslabón más débil. Eso no ha cambiado. Como no han variado un ápice los ataques. "Hay sectores, muy críticos, en los que la seguridad es fundamental; lo que hace que todo lo que tenga que ver con la prevención y con ayudar a los usuarios, a través de su formación y concienciación, a mejorar su protección, es clave". Ahora bien, no olvida recordar el carácter "privilegiado" que siguen exhibiendo todas las compañías que se dedican a ofrecer esta seguridad. "Nuestro sector va a seguir muy activo. Ahora sigue siendo clave ayudar a las compañías y a los clientes a hacer frente a los nuevos ataques y las nuevas necesidades en materia de seguridad".

Papel del canal

Ángel García extiende a los distribuidores ese carácter privilegiado. Un canal que debe reinventarse en estos momentos tan complicados. "Los *partners*, más que nunca, tienen que escuchar las necesidades del cliente y encontrar la mejor solución para cada uno de ellos. Además, tienen que actuar de forma urgente ya que de esa manera tendrá mucho ganado en los clientes". A juicio del responsable de la unidad de redes y seguridad de Arrow, la capacidad de adaptación que ha demostrado el distribuidor ha sido francamente buena. Una metamorfosis que, por supuesto, también ha alcanzado al canal mayorista. "Es increíble cómo se han adaptado todas y cada una de nuestras unidades: desde el área de la preventa, hasta el soporte técnico, pasando por los departamentos de formación y, por supuesto, el área de financiación",

GTI
Software & Networking

TU MAYORISTA ESPECIALIZADO EN CIBERSEGURIDAD

Si estás pensando en implantar un proyecto de ciberseguridad, o si quieres convertirte en proveedor de servicios de ciberseguridad en la nube, GTI puede ayudarte.

Ponemos a tu disposición todo lo que necesitas para que tu proyecto sea un éxito:

- Experiencia y conocimiento de la gama más amplia de soluciones de ciberseguridad.
- Servicios profesionales de instalación, despliegue y consultoría.
- Formaciones técnicas y comerciales.
- Cursos de Certificación Oficial.

EL CATÁLOGO DE CIBERSEGURIDAD MÁS COMPLETO

Seguridad de Endpoints
Soluciones de protección para dispositivos remotos que se comunica con una red a la que están conectados.

EDR
EndPoint Detection and Response. Sistemas de detección y respuesta avanzada.

Seguridad para OFFICE 365
Soluciones de seguridad para la plataforma de productividad, comunicación y colaboración alojada en la nube de Microsoft.

EMAIL
Soluciones de seguridad para el correo electrónico.

SIEM
Security Information and Event Management, las soluciones SIEM se basan en detectar actividades sospechosas que amenazan los sistemas de una empresa y las resuelven de forma inmediata.

MDM
Mobile Device Management: Soluciones de gestión de dispositivos móviles. Son tecnologías diseñadas para gestionar, controlar y proteger los datos corporativos en los smartphones usados por los empleados de una compañía.

DLP
Data Loss Prevention: prevención de pérdida de datos, soluciones y estrategias para asegurarse de que los usuarios finales no envían información sensible o crítica fuera de la red corporativa.

WAF
Web Application Firewall: dispositivos hardware o software que permiten proteger los servidores de aplicaciones web de determinados ataques específicos en Internet.

DDoS
Herramientas para evitar los ataques de denegación de servicio que tratan de inhabilitar servidores, servicios o infraestructuras.

GESTIÓN TI
Soluciones para la supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información de una organización.

PAM
Las soluciones PAM (Privileged Access Management) son un conjunto de tecnologías diseñadas para ayudar a las organizaciones a abordar los problemas inherentes relacionados con las cuentas privilegiadas.

CYTOMIC
IBM Security
kaspersky
MICRO FOCUS
Microsoft
MAILINBLACK
ONE IDENTITY
TREND MICRO
radware
panda
Restorepoint

¿QUIERES POTENCIAR TU NEGOCIO DE CIBERSEGURIDAD?

CONTACTA CON NOSOTROS: ciber@gti.es / www.gti.es

> "Muchos *partners* van a salir reforzados de esta situación, con más valor añadido, más capacidad técnica y con soluciones más adaptadas a los actuales escenarios"

enumera. "También los mayoristas nos hemos tenido que reinventar, adaptándonos a todos y cada uno de los perfiles de nuestros clientes".

Para Roberto Alonso, esta capacidad de metamorfosis no es nueva en el canal. "Siempre ha sido así. El canal siempre ha demostrado su agilidad y flexibilidad". Ahora bien, el responsable del negocio *cloud* de GTI recuerda que lo que no cambia nunca es la proactividad del *partner*. "Ahora más importante que nunca".

Lo que tampoco muta es la especialización. "El canal de la seguridad es uno de los canales más especializados y más cualificados que existe en el entorno TI", recuerda Carmen Muñoz. En estos momentos tan complicados, se han intensificado los modelos de oferta de servicios y el uso de los SOC. "Han sabido presentarles rápidamente a sus clientes cuáles eran los caminos para abordar una situación complicada, llena de incertidumbre, con ataques que ponían en riesgo la continuidad del negocio".

David Gasca insiste en el apoyo financiero aunque alerta que éste, por sí solo, no garantiza el negocio. "Es cierto que aquellos *partners* que no cuenten con suficiente capacidad financiera van a sufrir muchísimo. Pero no es suficiente: o el canal es capaz de adaptarse a los cambios que van a producirse o pondrá en riesgo su supervivencia".

El giro hacia el desarrollo de servicios profesionales es otro ámbito de adaptación, como recuerda Antonio Anchustegui, sobre todo vinculado al ámbito *cloud*. "Estamos utilizando de manera intensiva y masiva herramientas, ubicadas en el *cloud*, que hay que configurar de manera correcta".

Una idea en la que insiste Cohen. A su juicio, las empresas han cambiado sus prioridades y se han incrementado los proyectos en los que éstas buscan una nueva organización, con una red más extendida y la seguridad en torno al usuario. "Ahora, más que nunca en la historia, hay una gran oportunidad para los *partners* en cuanto a servicios profesionales y en el desarrollo de los servicios gestionados como modo de pago por uso que resuelve muchos problemas", corrobora. "Muchos *partners* van a salir reforzados de esta situación, con más valor añadido, más capacidad técnica y con soluciones más adaptadas a los actuales escenarios".

Reflejo en el negocio

La criticidad, aún más grande, que ha tomado el mercado de la seguridad en este primer semestre del año y la mayor concienciación de las empresas en torno a ella, ha permitido que toda la cadena de seguridad haya visto crecer su negocio. Ángel García desvela que los crecimientos del primer trimestre en el negocio de seguridad de Arrow han estado por

> "Hay muchas empresas dispuestas a invertir, de manera razonable, en el entorno del puesto de trabajo ya que nos hemos dado cuenta de que su seguridad es vital"

Antonio Anchustegui
director del área de seguridad de Ingram Micro

esprinet® V-Valley the Value of esprinet vinzeo

Para nosotros, la **ciberseguridad** es un factor importante que debe estar en el ADN de todas las organizaciones. Nuestro **equipo de profesionales compacto, competente, especializado en marcas y tecnologías específicas**, y al servicio del canal, es el valor único para que la seguridad sea un facilitador más del negocio.

¡La ciberseguridad es nuestra pasión!

Hablamos tu idioma Seguridad, Cloud y Networking Enterprise

McAfee
IPS CASB EPP Mobile ATP Sec Content EDR SIEM DLP

Microsoft
CASB EPP IAM IRM

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

A10
DDoS ADC SSLi

PulseSecure
IdP Mobile ADC VPN NAC SDP

BROADCOM connecting everything
Management IT IAM SSO Intelligent Automation

CounterCraft
Honey Pot Deception Threat Hunting

kaspersky
EPP Mobile ATP EDR Sec Content Encryption

SONICWALL
NGFW IPS vSec ATP EDR Sec Content VPN WIFI

CLOUDFLARE
DDoS DNS SEC CDN WAF

CIPHER™
HSM Secure PKI Digital Sign

BACKBOX
Intelligent Automation

solarwinds
Management IT

aruba a Hewlett Packard Enterprise company
VPN UEBA WIFI

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

www.v-valley.com Tel. + 34 690 756 403 seguridad@v-valley.com

BARCELONA | BILBAO | MADRID | LISBOA | SEVILLA | ZARAGOZA

"Estamos viendo una enorme demanda de soluciones de autenticación multifactor, de soluciones de *single sign on* (SSO), de acceso a las aplicaciones y de soluciones CASB (Cloud Access Security Manager)"

Chuck Cohen
director general de Ireo

encima de los cosechados el año pasado. Un balance similar al vivido en el segundo trimestre. "Vamos a cerrar un buen primer semestre", reconoce, con los fabricantes con soluciones en torno al teletrabajo, VPN SSL, el doble factor de autenticación o la protección de los dispositivos móviles, como los principales receptores del crecimiento.

La situación del negocio de Exclusive es similar. Carmen Muñoz desvela que el ascenso logrado en el primer trimestre ronda el 30 %. "Hay mucho dinamismo y seguimos viendo mucha generación de nuevas oportunidades", reconoce. Aunque no esconde su preocupación por la situación económica y es cautelosa de cara a la segunda parte del año, la directora de Exclusive Networks prevé que se llegará al verano manteniendo esta tendencia favorable. Tras él, Muñoz recuerda que la actividad productiva en España debería empezar a ganar un mayor dinamismo. "De lo contrario deberemos encarar una situación bastante complicada".

Antonio Anchustegui corrobora que la ciberseguridad es uno de los sectores que mejor comportamiento está teniendo en el segmento TIC. El responsable de Ingram Micro asegura que en el área del *run rate* el negocio se ha mantenido y que, en el segmento de los proyectos, con un mayor abanico de situaciones, la media es esperanzadora. "Estamos haciendo una buena cifra de negocio, llegando a los objetivos que nos marcamos, sobrepasándolos, incluso en el primer trimestre". De cara a la segunda parte del año, Anchustegui sí prevé, incluso, una reactivación.

"Estamos ayudando, de manera intensiva, a nuestros distribuidores a encontrar nuevas oportunidades de negocio en sus clientes"

La situación se repite en el dúo nacional. Roberto Alonso desvela que GTI ha cerrado un excelente primer semestre fiscal (el año del mayorista arranca en octubre) aunque también se muestra más cauteloso de cara al segundo tramo de su ejercicio. Una incertidumbre que también observa Cohen a pesar de que el director general de Ireo reconoce que sus recientes alianzas con fabricantes que se mueven en los entornos relacionados con la seguridad del teletrabajo les ha ayudado a hacer crecer el negocio. "Vamos a poner foco en este ámbito vinculado con la gestión de identidades y la conectividad segura".

David Gasca presume de la "juventud" del negocio de seguridad en Esprinet V-Valley. Una juventud que, a su juicio, les concede los ratios de crecimiento que debería exhibir cualquier *startup*. "Han sido muy grandes en estos años, gracias también a la enorme inversión que ha dedicado Esprinet a esta parte del negocio". Gasca, a pesar de la incertidumbre, inevitable, reconoce que van a seguir apostando por el crecimiento. "Dentro de la cautela, somos optimistas", reconoce. "El mercado del *run rate* se ha recuperado y han aparecido nuevos proyectos interesantes, más ágiles, que otros que teníamos abiertos desde hacía más tiempo".

Nuevas e inminentes oportunidades de negocio en el sector de la ciberseguridad

La complicada situación generada por la pandemia de la covid-19 ha golpeado de lleno a casi todos los mercados, poniendo en alza tendencias como el teletrabajo, que se ha convertido en una nueva "normalidad".

Por nuestra experiencia y especialización en las áreas de la seguridad y el cloud, y lo percibido durante estos meses de confinamiento, en los que hemos mantenido una colaboración activa con las distintas capas que conforman el canal (partners integradores, distribuidores de valor añadido y fabricantes), hemos sido conscientes de que la correcta protección de este proceso forzado de transformación digital que ha supuesto el teletrabajo, debe ser muy tenida en cuenta, lo que se suma al creciente número de ciberataques sufrido a nivel internacional. Por ello, las empresas deberían apostar por tecnologías avanzadas y por integraciones más robustas para asegurar sus infraestructuras.

Una adecuada estrategia de seguridad para entornos de teletrabajo

Como punto de partida y más allá de hacer crecer los despliegues de acceso remoto más "tradicional" (VPN, presentación de aplicaciones o VDI), las empresas deberían optar por soluciones de MultiFactor Authentication (MFA), basados en tokens para móvil, o incluso opciones más cómodas para el usuario final y de Single-Sign On (SSO), para asegurar una mejora fundamental en la gestión de las credenciales de usuario.

Con el teletrabajo, la desaparición del perímetro de seguridad ha expuesto aún más los servicios y los datos críticos. Así, la inversión en soluciones EDR (Endpoint Detection and Response) ya se percibe como un "debe", al entender que las consecuencias de un ataque efectivo al puesto de trabajo serían inmediatas, con enormes costes por el descenso de la productividad.

Tras ello, la siguiente prioridad es el fortalecimiento de las ya poco efectivas soluciones de protección del correo electrónico, el mayor vector de ataque. Esta mejora puede acompañarse con un ciclo formativo de autoprotección de todos los usuarios a través de una plataforma *online* diseñada específicamente para ello y con herramientas de testeo de la maduración de la compañía en esta cuestión.

Para incrementar la seguridad ante ataques y errores humanos peligrosos, una solución PAM (Priviledge Access Management) que permita una gestión de privilegios y permisos de los perfiles más privilegiados, o incluso, una solución de gestión de identidades completa (IAM), cubrirán este espacio frecuentemente olvidado.

La defensa de elementos críticos no puede ser dejada al margen. Un buen nivel de auditoría en el acceso a los datos (no estructurados, bases de datos y SaaS/Cloud), con algún motor de análisis del comportamiento, o incluso, el despliegue de una solución UEBA que asegure una gestión asumible de la solución, permitirá aumentar el grado de protección real. De igual modo, el conocimiento del directorio activo y de sus vulnerabilidades, junto al análisis de los escaneos e intentos de exfiltración de información que en él está almacenada, debería ser también, más que considerado, a tenor de nuestra actual dependencia de este motor.

Con todo ello, queda claro la existencia de muchas opciones en materia de seguridad. Queda por conocer el impacto del fenómeno SASE (Secure Access Service Edge) y su capacidad para consolidar la protección perimetral perdida, la conectividad segura global (desde oficinas remotas hasta usuarios de teletrabajo), o la aplicación de protecciones adicionales (*health checking* de terminal, URL *Filtering*, FWaaS a nivel de aplicación, *Sandboxing* o CASB). Y todo ello con ciertas capacidades de CDN global y conectividad directa a los principales proveedores de cloud pública y una mejorada experiencia de usuario.

Desde Exclusive Networks, invitamos a divulgar tanto este tipo de análisis como aportar información crucial para conocer las importantes carencias aún por cubrir.

Alberto Pérez Cuesta,
director de desarrollo de negocio de Exclusive Networks Iberia

Echando un vistazo al futuro...

No es sencillo otear lo que va a pasar en los próximos meses. Ni en el segmento de la seguridad, ni en España. Ángel García asegura que va a haber muchísimos cambios. "Tanto los mayoristas como el canal hemos tenido que trabajar de una forma urgente y critica para poder dar servicios y soluciones rápidas a estas necesidades críticas del entorno de trabajo", insiste. Una nueva manera de entender el puesto de trabajo que ha venido para quedarse. "Todas las compañías, en mayor o menor medida, van a implantar el teletrabajo", aventura. Por tanto, se exige una mayor comprensión de las nuevas casuísticas que van a implantar cada uno de los clientes. "Ya no sirven los parches temporales", alerta. "Caminamos hacia una gestión del acceso universal, en la que, con independencia de dónde se ubique el usuario, deberá estar siempre totalmente protegido".

La proactividad del canal seguirá siendo clave. "Toda crisis genera nuevas oportunidades", señala Carmen Muñoz. Junto a la proactividad, la directora general de Exclusive Networks apela a la creatividad, la ilusión y a buscar nuevas vías para incrementar o mejorar el servicio a los clientes. "Y seguir formándose de manera continua, la búsqueda de nuevas soluciones y la especialización a todos los niveles". En un mercado que siempre va a toda velocidad, "siempre se ha demostrado que los que han sido rápidos y han sido capaces de reinventarse y adaptarse rápidamente a situaciones complicadas son los que han salido reforzados".

Antonio Anchustegui recuerda que los mayoristas surten al canal de información constante, de buenas prácticas acerca de cómo hacer negocio en estos momentos y en la mejor manera de cómo cambiar el foco de la solución a los problemas. "Una de las herramientas más útiles, que tanto nosotros como los fabricantes con los que trabajamos estamos ofreciendo al canal, le permiten observar la situación de sus clientes y que estos puedan enfrentarse, de manera sencilla y eficaz, con su realidad".

> "Es el momento de flexibilizar. Debemos ofrecer a cada uno de nuestros clientes la mejor solución financiera posible"

A pesar de que, en un principio, el entorno *online* pudiera ser un obstáculo para la realización de demostraciones o para cerrar reuniones previas a los proyectos, la experiencia ha demostrado que no ha sido así. "Estamos ayudando, de manera intensiva, a nuestros distribuidores a encontrar nuevas oportunidades de negocio en sus clientes", asegura David Gasca. "Es todo más ágil y más rápido". A su juicio, además, se ha intensificado la capacidad de trabajar en equipo. "No solo ha pasado en Esprinet; también lo he percibido en los *partners* y en los clientes finales. Sin lugar a dudas, es cuando más cerca tenemos que estar los unos de los otros: los mayoristas de los *partners* y de los fabricantes".

Un cambio de escenario que no ha hecho perder ni un ápice de importancia a la parte que Roberto Alonso califica de táctica, vinculada con la financiación, el soporte comercial, los recursos técnicos o la formación. "El mayorista siempre ha tratado de ser una extensión del fabricante y también de nuestros clientes, con el fin de facilitar y acelerar todos los procesos". En una visión más estratégica y particular, Alonso recuerda que GTI va a seguir centrado en su foco exclusivo en el desarrollo de la nube, el "como servicio" y los modelos gestionados. "Trabajamos de manera muy intensa en los programas de pago por uso que permiten a los *partners* montar un servicio gestionado". Un propósito que, como bien explica, cala mucho en distribuidores que ya cuentan con un recorrido en este apartado, mientras que otros necesitan todavía descubrir más la oportunidad. "Ahora bien, a cada uno le proveemos de lo que necesite".

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

Soluciones de trabajo para TI de la mano de IREO

__IREO__, mayorista especializado en soluciones para la gestión de servicios TI (ITSM) y seguridad TI, representa a fabricantes de primer nivel que ofrecen todas las ventajas para herramientas de teletrabajo que demandan tanto sus partners como sus clientes: fácil implantación, bajo coste y máxima fiabilidad con fabricantes líderes como __BeyondTrust__, __Datto__, __DeepnNet Security__, __ManageEngine__, __Ping Identity__, __Sophos__, __Stormshield__ y __TP-Link__, entre otros, que abarcan las áreas de conectividad segura, autenticación y acceso y soporte y administración remota, entre otras soluciones y que, sobre todo, se adaptan a todo tipo y tamaño de organización.

- **Conectividad segura:** Las soluciones VPN permiten una conexión rápida, fiable y segura a la red corporativa desde cualquier lugar, a través de Internet. VPN es la solución de conectividad más utilizada para trabajadores remotos. IREO ofrece soluciones que combinan la seguridad de un cortafuegos, con la facilidad de conexión de una VPN.
- **Autenticación y acceso:** Estas soluciones permiten dar un acceso directo a las aplicaciones y sistemas corporativos, sin dar acceso a toda la red corporativa. Por lo tanto, se trata de las soluciones idóneas para dar acceso limitado a recursos específicos, tanto para empleados como para proveedores externos.
- **Soporte y administración remota:** Una vez implantado el sistema de teletrabajo, el siguiente reto al que se enfrentan las empresas es administrar y dar soporte a los equipos remotos. IREO propone soluciones fáciles de implantar, que permiten configurar y administrar todos los aspectos del equipo.

Además de otras soluciones que están especialmente indicadas para empresas con las redes de teletrabajo. Puedes ver el detalle de todas ellas aquí: soluciones de teletrabajo para TI (*http://www.ireo.com/wp-content/uploads/2020/teletrabajo/IREOSoluciones Teletrabajo.pdf*).

Dotar a los empleados de soluciones tecnológicas eficientes y de calidad es la clave para no perder la eficiencia y, tal y como indica IREO, se puede conseguir de manera rápida, sencilla y asequible para todo tipo de empresa. Todos nuestros fabricantes proporcionan las herramientas necesarias para que el acceso desde cualquier dispositivo y ubicación sea seguro y cubra las necesidades que toda empresa necesita para poder trabajar desde cualquier lugar.

En un esfuerzo por colaborar en mitigar el inevitable impacto económico derivado de la crisis sanitaria en las empresas, IREO y sus fabricantes ofrecen promociones y licencias gratuitas de excelentes soluciones.

Todas ellas accesibles desde el apartado de promociones en su página web: *https://www.ireo.com/promociones*

En palabras de Chuck Cohen, director general de IREO, *"ahora más que nunca, necesitamos ofrecer a nuestros empleados la mejor tecnología disponible para que dispongan de todos los recursos necesarios de cara a poder desarrollar su jornada laboral de manera eficiente sin necesidad de realizar un gran desembolso ni grandes despliegues tecnológicos"*.

Además de las excelentes promociones, IREO ha programado un completo calendario de eventos y de formación *online* con el objetivo de dar a conocer estas soluciones a sus clientes y *partners*, y mantenerles actualizados en todas las novedades y oportunidades de negocio.

Para más información, consulte la web de eventos de IREO: *https://www.ireo.com/eventos*.