LA EVOLUCIÓN DE LA CIBERSEGURIDAD EN ESPAÑA Y EL ROL DEL CANAL, A DEBATE

Un año más, en 2022 se volvieron a batir récords en materia de incidentes graves en ciberseguridad, con cifras desorbitadas de ataques diarios, sobre todo a aquellas organizaciones que no están tan protegidas y que suelen responder a un perfil de pequeña y mediana empresa. ¿Cuáles están siendo las últimas tendencias en materia de ciberseguridad este 2023 y el papel del canal frente a los retos que se están produciendo en términos de protección de la información?

De estas y otras cuestiones debatimos junto a Ángel García, business unit manager de Seguridad & Networking en Arrow Electronics España; Miguel López, senior regional sales manager en Barracuda Iberia; José Manuel Medina, director de desarrollo de negocio de Exclusive Networks Iberia; Isabel López, sales engineer manager en Samsung Electronics Iberia; y David Gasca, sales & marketing manager de Ciberseguridad en V-Valley.

UN NEGOCIO EN CRECIMIENTO

Tal y como señala Ángel García, “todavía queda la mitad del año, pero el

número de ataques se va incrementando y las empresas, sí o sí, van a tener que destinar un presupuesto específico a la seguridad. Vemos una tendencia muy positiva en la gran cuenta y la Administración Pública, y esperamos que las ayudas europeas sean un motor dinamizador en la segunda parte del año".

Para Miguel López, "la tendencia es positiva, pero quizá porque el mercado español es más inmaduro que otros, de ahí que las cifras globales no sean aplicables a España. Quizá las pymes tienen más problemas para mantener la inversión, pero sí es cierto que la concienciación es mayor y muchos lo están empezando a meter en los presupuestos. Queda terreno por recorrer, eso sí, en todos los segmentos del mercado".

En palabras de José Manuel Medina, "todos los analistas estiman que vamos a crecer este año, aunque las cifras varíen. El primer trimestre ha sido muy bueno, quizá el segundo un poco más flojo, pero creo que el mercado va a ir bien. La gran empresa tiene que invertir, en la Administración nos van a ayudar los fondos europeos, aunque a lo mejor se nota el efecto de las elecciones, y, en el caso de la pyme, hay que ayudarla, porque no tiene la misma capacidad, ni económica ni de recursos humanos".

Según Isabel López, "tanto en Administración Pública como en sectores como el financiero la seguridad es esencial, y cuentan con estas soluciones. Mientras la pyme está empezando a preocuparse, porque la labor de concienciación está llegando. Quizá no tienen grandes presupuestos, pero están haciendo cosas en esta línea".

Finaliza esta primera ronda de opiniones David Gasca, recordando que "en mayo, según Context, la seguridad es el único mercado de valor que decreció, tras grandes incrementos desde principio de año. Al final, el mercado seguirá creciendo a doble dígito, porque desaparecen incertidumbres y llegan nuevas ayudas de fondos europeos. Lo bueno es que la tendencia es alcista, y esperamos un último trimestre positivo, porque la seguridad es imprescindible".

PELIGROS CONOCIDAS Y NUEVAS AMENAZAS

A nivel de amenazas, explica Miguel López, "el ransomware es la más destacada y la que más llama la atención. Si añadimos a esto la recaudación que obtienen, le granjea al ransomware una posición de privilegio en la notoriedad, pero no es la única. El phishing,

DEBATE IT >> Debatimos junto a Arrow ECS, Barracuda, Exclusive Networks, Samsung y V-Valley sobre la evolución de la ciberseguridad en España y el rol del canal.

> EL CONCEPTO DE SEGURIDAD COMPARTIDA ES CLAVE, Y ES MUY IMPORTANTE LA CONCIENCIACIÓN DE CADA UNA DE LAS PARTES, Y EL CONOCIMIENTO DEL USUARIO PARA ELEGIR EL MEJOR PARTNER EN CADA CASO

ÁNGEL GARCÍA,
business unit manager de Seguridad & Networking en **Arrow Electronics** España

Clica en la imagen para ver la galería

> QUIZÁ LAS PYMES TIENEN MÁS PROBLEMAS PARA MANTENER LA INVERSIÓN, PERO SÍ ES CIERTO QUE LA CONCIENCIACIÓN ES MAYOR Y MUCHOS LO ESTÁN EMPEZANDO A METER EN LOS PRESUPUESTOS

MIGUEL LÓPEZ,
senior regional sales manager en **Barracuda** Iberia

Clica en la imagen para ver la galería

el robo de identidad siguen creciendo, y probablemente hacen más daño".

En opinión de José Manuel Medina, "la principal amenaza es el usuario, pero, aparte de eso, el ransomware va a seguir creciendo con ayuda de tecnologías como la IA. Cada vez es más sofisticado y eficiente, por el rédito financiero que obtiene".

La concienciación para el usuario, apunta David Gasca, "puede verse complicada porque, con el uso de la IA, se eliminan algunas de las señales clásicas para detectarlo. Va a ser más peligroso".

Coincide con él Isabel López, que señala que "se han creado miles de dominios y uno de cada 25 es falso y tiene el objetivo de introducir código malicioso en tu equipo. Hay que extremar las precauciones, además de contar con las herramientas adecuadas".

"Los ataques de ransomware son cada vez más profesionales", indica Ángel García, que añade que "son más difíciles de detectar y, por tanto, de detener. Las empresas deben invertir más, aunque su presupuesto sea limitado. Deben saber muy bien dónde invertir". La IA, comenta Miguel López. "impacta todo, también las amenazas, porque hablamos de organizaciones muy preparadas, profesionalizadas, muchos recursos y conocimientos. Además, los cos-

tes de los ataques son menores con IA, además de ser más eficientes. Necesitamos que la seguridad siga creciendo al mismo ritmo para protegernos".

En la parte positiva, continúa, "los fabricantes están integrando la IA para aumentar la protección. El problema no es solo la falta de tecnología, sino que en algunos casos no están implementadas las herramientas en todos los puntos de la cadena de valor. Es necesario que se implemente la seguridad en todos los eslabones de la cadena".

"Es necesario", señala José Manuel Medina, "que todos pongan de su parte: los fabricantes con la tecnología, las empresas con la implementación de estas herramientas y estrategias, y las administraciones con normativas que ayuden a que se alcance el nivel necesario de protección".

Algo más pesimista es David Gasca, que considera que, en líneas generales, "la industria va por detrás de las amenazas. Podemos estar por delante en algún punto específico, pero no en toda la industria de la protección. Y, encima, si tenemos en cuenta no cuándo esta disponible la tecnología, sino cuándo y cómo la implementan las empresas, vamos muy tarde".

"La seguridad total", apunta Isabel López, "no la vamos a poder alcanzar. Esto es una realidad. Los fabricantes ponen sobre la mesa herramientas que pueden enfrentar cualquier problema de seguridad. Hay que tener todas las herramientas y servicios actualizados, porque no todas las empresas lo hacen, y eso puede ser un problema".

"Los atacantes se rigen por el binomio coste/beneficio", apostilla Miguel López, "con lo que si tienes establecidas una medidas de protección razonables con herramientas actualizadas, el nivel de riesgo baja considerablemente. En un reciente estudio que hemos realizado, todos los encuestados eran conscientes de que tenían que invertir más, pero más de la mitad de ellos no contaban, para protección de correo, con una tecnología tan elemental como un sandbox. Por ello, son más vulnerables a los ataques.

Clica en la imagen para ver la galería

> PODEMOS TENER LAS TECNOLOGÍAS, PERO SIN UNA ADECUADA IMPLEMENTACIÓN EN LA EMPRESA NO PODEMOS HACER NADA

JOSÉ MANUEL MEDINA,
director de desarrollo de negocio de **Exclusive Networks** Iberia

Clica en la imagen para ver la galería

> EN NUESTROS DISPOSITIVOS, LA SEGURIDAD ES ESENCIAL DESDE EL DISEÑO, PERO ES NECESARIO IMPLEMENTAR SERVICIOS ADICIONALES QUE NOS PERMITAN PROTEGER LA RED Y LA INFRAESTRUCTURA DE LA EMPRESA

ISABEL LÓPEZ,
sales engineer manager en **Samsung Electronics** Iberia

Clica en la imagen para ver la galería

Las tecnologías están, pero, en general, los atacados no lo son por un fallo de la tecnología, sino porque no estaba implementada".

En palabras de David Gasca, "algunos de nuestros fabricantes hablan de ciber-inmunidad, y la basan en que el coste del ataque sea mayor que el beneficio. Si un ataque es más caro que el beneficio que van a obtener, una empresa puede considerarse segura".

El problema, en opinión de Ángel García, "es que la superficie de exposición es cada vez mayor. Podemos proteger con una visión tradicional del dispositivo, el firewall... pero hay que añadirle la realidad de la IoT. Tu red ya no es la tradicional, sino que se ha multiplicado exponencialmente el número de dispositivos conectados, con lo que es necesario tener un control total sobre todo lo que ocurre en tu res. Y esa protección solo se puede dar con la integración de múltiples actores y tecnologías. El paradigma de la empresa cien por cien segura, es imposible, y más si tenemos en cuenta el presupuesto destinado a la protección en las empresas. Así que con presupuesto limitado, muchos aspectos que proteger y unos recursos humanos limitados, no es trivial ni sencillo protegerse".

> ALGUNOS DE NUESTROS FABRICANTES HABLAN DE CIBER-INMUNIDAD, Y LA BASAN EN QUE EL COSTE DEL ATAQUE SEA MAYOR QUE EL BENEFICIO, Y, SI ESTO ES ASÍ, UNA EMPRESA PUEDE CONSIDERARSE SEGURA

DAVID GASCA,
sales & marketing manager de Ciberseguridad en **V-Valley**

"Hablamos de tecnologías", puntualiza José Manuel Medina, "pero sin una adecuada implementación tampoco hacemos nada".

UNA NUEVA REALIDAD A PROTEGER

Tal y como comenta Isabel López, "en nuestros dispositivos, la seguridad es esencial desde el diseño. Pero no es suficiente. Vamos a tener que implementar servicios de seguridad que nos permitan proteger la red y la infraestructura de la empresa".

En palabras de David Gasca, "se están incorporando a las redes millones de dispositivos sin la adecuada seguridad, con lo que se nos viene encima un reto muy importante. Hay que avanzar mucho en la securización de IoT".

Para hacer frente a esto, añade Ángel García, "el concepto de seguridad compartida es clave. Es muy importante la concienciación de cada una de las partes, y el conocimiento del usuario para elegir el mejor partner en cada caso".

Al tener que proteger una zona de exposición tan grande como IoT, señala Miguel López, "debes tener en cuenta que hay dispositivos que no van a poder ser protegidos ni gestionados, y que son inseguros por definición. Lo que hay que establecer es una infraestructura de seguridad que configure cada punto como un más en tu plataforma de seguridad".

Hay que tener claro qué podemos dejar y qué no que se conecte a Internet, "y en el caso de los dispositivos IoT es algo esencial", indica José Manuel Medina, que añade que "hay mucho camino por recorrer, pero las tecnologías de protección van por buen camino".

EL VALOR DEL ECOSISTEMA EN SEGURIDAD

Con la vista puesta en la eficacia del ecosistema, continúa José Manuel Medina, "es fundamental ayudar a todos los implicados a seguir creciendo e incorporando piezas de tecnología. Algunos partners ya tienen una capacidad suficiente para ofrecer sus propios servicios a terceros, pero otros necesitan ayuda. Nosotros ofrecemos la posibilidad de cambiar un modelo de venta tradicional de tecnología por uno de suscripción basado en unos servicios gestionados que aporten valor al cliente, algo esencial si hablamos de la pyme, que no tiene los recursos ni los conocimientos adecuados".

Pero es algo que aplica también a la gran empresa, añade Isabel López, "porque para securizar tu parque, necesitas diferentes herramientas, y no es sencillo ser experto en herramientas tan diferentes, y es el canal el que cuenta con equipos especializados que te pueden apoyar. Sin embargo, en nuestro canal veo que quizá vamos un poco más lento de lo esperado".

Según explica David Gasca, "lo que más valoran los partners es la formación, y por eso invertimos mucho en ello. Esta capacitación es esencial para entender las soluciones disponibles. La velocidad de los modelos de pago por uso es diferente

en los distintos negocios, y nosotros estamos preparando al canal para seguir añadiendo soluciones a estos modelos. Ofrecemos hasta 8 formaciones a la semana alrededor del cloud. Quizá va lento, porque el empuje de todos los jugadores no es el mismo, pero trabajamos con muchos partners muy interesados".

En palabras de Ángel García, "como el mercado de la ciberseguridad es tan amplio y los recursos limitados, es importante contar con partners especialistas que puedan ofrecer estos servicios. Antes estos partners se concentraban en la gran empresa, y ahora están apuntando a la pyme, lo que es un gran avance".

Para Miguel López, "el mercado de MSP esta evolucionando rápidamente, pero quizá no es un modelo para todos los partners. En nuestro caso, es en torno al 25 por ciento. Nosotros estamos ofreciendo nuestra tecnología como servicio, para facilitárselo, pero, además, les permitimos desplegar servicios de SOC como servicio con herramientas propias y de terceros, de forma que el partner, independientemente de su tamaño, puedan ofrecerlo como un servicio añadiendo su propia capa de valor. Podemos facilitar la integración para los que no tienen esa capacidad por sí mismos, y, para los que sí, darles las piezas del puzle para que construyan su propia solución".

En palabras de David Gasca, "en seguridad siempre es han comercializado las soluciones con licencias temporales y servicios al cliente, pero quizá no esta costando más dar el paso a los puros servicios de tarificación mensual".

En todo caso, apunta Miguel López, "es importante diferenciar un modelo de pago por uso de un podemos MSP, que, a veces, coincide, pero otras veces no. Y quizá el mercado español es menos maduro en este punto por esta confusión. Porque no hablamos solo de facturación mensualizada, sino de aportar una capa de servicios de valor por encima".

UN FUTURO DE ¿CONSOLIDACIÓN?

Señala David Gasca que "cada vez hay más interés en los servicios, y los mayoristas queremos ayudar en ese sentido, y un paso para ello fue la compra de Lidera. El futuro pasa por desarrollar nuevos servicios, potenciar los ecosistemas, y veremos cómo aparecerán nuevos jugadores incluso con nuevas mentalidades, se integran otros y desaparecen pocos. En todo caso, seguiremos trabajando para potenciar los ecosistemas y desarrollar nuevos servicios".

"Es un mercado tan amplio y cambiante", comenta Ángel García, "que es difícil abordarlo desde una única empresa, por lo que seguirán existiendo las compras o las alianzas en todos los segmentos. Pero no es algo nuevo en el mercado".

"Las adquisiciones o fusiones son la forma más rápida de poder crecer", apunta José Manuel Medina, "sobre todo para avanzar en segmentos donde no se está presente", con lo que veremos un proceso muy similar al de estos años anteriores", finaliza Miguel López. ■

DIÁLOGO IT >> "La seguridad forma parte del ADN de nuestra compañía", Isabel López (Samsung)

MÁS INFO +

» La evolución de la ciberseguridad en España y el rol del canal