

TENDENCIAS EN CIBERSEGURIDAD PARA 2023 Y LOS RETOS PARA EL CANAL

¿Qué nos deparará 2023 en el ámbito de la protección de la información? ¿Cómo seguirá evolucionando el canal de distribución al respecto? ¿Qué papel jugará el mayorista? También analizaremos en qué estadio se encuentra el proceso de consolidación del ecosistema tecnológico de la ciberseguridad en España, tanto a nivel de fabricantes como de mayoristas y canales.



Debatimos sobre estas y otras cuestiones junto a Ángel García, Manager Enterprise Computer Solutions en Arrow; Alberto Carrillo, Iberia sales engineering manager de Hillstone; Sergio Martínez, Iberia regional manager en SonicWall; Antonio Martínez Algora, responsable técnico de Stormshield Iberia; y David Gasca, business unit coordinator Enterprise Security en V-Valley.

TENDENCIAS DE 2022

En palabras de Ángel García, “claramente el protagonista ha sido el ransomware. De hecho, se estima que cada 11 segundos se produce un ataque. Pese a que antes se dirigía a grandes corporaciones, ya un 40% de los ataques de ransomware se han producido en pequeñas y medianas empresas, como apunta el portal TIC de Europa Press. La sencillez y el daño que puede hacer, lo convierte en el arma perfecta para los ciberdelincuentes. Tenemos que seguir concienciando al usuario de que nadie está libre de ser atacado”.

Coincide con él Alberto Carrillo, que añade que lo que sucede con el ransomware “es que es muy rentable. Se han montado ecosistemas

completos dentro de este sector. Incluso se ofrece como servicio. Y, además, hay un gran caladero en las empresas de menor tamaño, por razones no solo tecnológicas, sino también culturales. Por tanto, la protección debe tener una aproximación más holística que nos incumbe a todos”.

Para Sergio Martínez, “es cierto que ha sido el tipo de ataque más letal, pero no el que más se ha in-

crementado frente a años anteriores. El número de ataques decreció en torno al 30% en los primeros meses del año, pero eran ataques mucho más dirigidos y letales. Es una de las preocupaciones más grandes de los responsables de seguridad”.

Continúa Antonio Martínez apuntando que “evidentemente, el ransomware es una de las principales amenazas, y, como hay mucho di-

nero implicado, se ha profesionalizado mucho. En algunos casos, con auténticas infraestructuras empresariales. Además, se ha profesionalizado, convirtiéndolo en un ransomware as a Service”.

Completa esta visión David Gasca añadiendo que la transformación “que hemos sufrido, ha hecho que los ataques de denegación de servicio sean cada vez más frecuentes, sobre todo entre las compañías de comercio electrónico. No es tan importante en número como el ransomware, pero a las empresas les afecta de manera importante en su economía”.

DE CARA A 2023...

Pensando en el nuevo año, desde el mercado se ve que “las herramientas están evolucionando”, prosigue David Gasca, “y con ellos los ataques, que nos más complejos, inteligentes, con elementos sociales, incluso, con lo que se necesita no solo saber por dónde han entrado, sino qué dato han afectado. Las empresas son conscientes de que necesitan identificar el problema y poner soluciones”.

Abundando en esta idea, Sergio Martínez apunta que la informática



MESA REDONDA >> Analizamos las principales tendencias que se van a producir en materia de ciberseguridad el próximo año y sus implicaciones en el ecosistema de canal, de la mano de Arrow ECS, Hillstone Networks, SonicWall, Stormshield y V-Valley.

“ TENEMOS QUE SEGUIR CONCIENCIANDO AL USUARIO DE QUE NADIE ESTÁ LIBRE DE SER ATACADO ”

ÁNGEL GARCÍA
Manager Enterprise Computer Solutions en **Arrow**

“ LA PROTECCIÓN DEBE TENER UNA APROXIMACIÓN MÁS HOLÍSTICA Y QUE NOS INCUMBE A TODOS ”

ALBERTO CARRILLO
Iberia sales engineering manager de **Hillstone**



“se hace por capas, y todas tienen que convivir con todas, por eso la ciberseguridad debe ser también por capas, haciendo telemetría en muchas partes y usar la IA para poder identificar los ataques que se puedan ir produciendo. En los próximos años, veremos mucha inteligencia aplicada a detener estos ataques en las organizaciones para poder reaccionar en tiempo real”.

Quizá ahí es donde está el reto, comenta Alberto Carrillo, “los ataques son tan sofisticados que las empresas grandes pueden tener

las herramientas y los conocimientos necesarios. El reto que tenemos es hacer permeable esta tecnología hacia las capas inferiores del mercado. Los ataques vienen de múltiples fuentes, el perímetro no existe, los dispositivos se multiplican en nuestra red... Debemos ser capaces de llevar esta tecnología a la última a clientes más pequeños. Ofrecer ciberseguridad como servicio”.

En opinión de Ángel García, “las direcciones de las compañías debe-

rían incrementar los presupuestos para ciberseguridad, porque el nivel de exposición y de estrés dentro de las empresas es mayor que nunca. De hecho, la ciberseguridad debería debatirse a nivel directivo como un elemento clave en las organizaciones. Sufrir un ataque cambia automáticamente todos los planes de cualquier empresa”.

“Es verdad que ha aumentado la concienciación”, recalca Sergio Martínez, “ha mejorado en los últimos años, pero negocio va por su cami-

no y seguridad intentan proteger la compañía”, y, por eso, “es fundamental que se discuta en el comité de dirección”.

La clave, apunta Alberto Carrillo es “la seguridad desde el diseño. Te dediques a lo que te dediques, la seguridad es algo fundamental, no algo añadido. De cara a conseguir fondos, es necesario demostrar el ROI, de ahí que haya que trabajar en unos KPI que demuestren el valor de algo que funciona. Porque hoy en día todo negocio

“ EL RANSOMWARE
ES UNA DE LAS
PREOCUPACIONES
MÁS GRANDES DE
LOS RESPONSABLES DE
SEGURIDAD ”



Clica en
la imagen
para ver
la galería

SERGIO MARTÍNEZ
Iberia regional manager en
SonicWall

que quiera escalar debe ser digital, y todo negocio digital está expuesto a amenazas que tenemos que gestionar”.

Destaca Antonio Martínez la importancia “de la profesionalización de la ciberdelincuencia, con lo que, si se usan herramientas y tecnologías para el negocio, esto implica riesgos, y debemos asumirlo. Esta profesionalización hace que, incluso antes de cifrar los datos, acceden a ellos, con el efecto que esto puede llegar a tener para una empresa”.

EL MERCADO EN CIFRAS

Con los datos de Canalys en la mano, el mercado de la ciberseguridad creció en el tercer trimestre un 16%. En el caso de España, desde V-Valley nos comenta que “el mercado va a seguir subiendo, porque hay muchas amenazas. Si la economía sigue creciendo y se sigue digitalizando, es normal que la seguridad crezca por encima del mercado”.

“Claramente, ciberseguridad crece por encima del resto del mercado”, apunta Antonio Martínez, “porque

“ LA CIBERDELINCUENCIA
AUMENTA Y LA PANDEMIA
HA SIDO UN MOTOR
PARA IMPULSAR NUEVAS
TENDENCIAS ”



Clica en
la imagen
para ver
la galería

ANTONIO MARTÍNEZ ALGORA
responsable técnico de
Stormshield Iberia

la ciberdelincuencia aumenta y la pandemia ha sido un motor para impulsar nuevas tendencias, como el teletrabajo, que hacen que se incremente la demanda de nuevas soluciones. La realidad es que las empresas necesitan más tecnología y más protección”.

A esto añade Sergio Martínez “la creciente militarización de la realidad. Solo en Ucrania, los ataques han aumentado en estos meses de manera alarmante. Además, el hecho de que cada vez haya más

dispositivos inteligentes conectados a la red, sin que sepas cómo está implementada la seguridad en ellos, hace que el entorno se complique mucho. Si a esto añadimos la falta de talento y capacidades, y la falta de recursos... Y no podemos olvidar el esfuerzo que ha hecho la Administración Pública, que puede ayudar a cerrar el año con una buena cifra de crecimiento, en torno al 9%, tras unos años muy buenos, tanto en 2022 como en 2023”.

Para Alberto Carrillo, “nosotros hemos abierto la región ibérica este año, y veníamos de abrir otras regiones los años anteriores. Pero en el caso español hemos batido todas las expectativas. Hemos firmado aquí el proyecto más grande en Europa para el mercado ISP, el canal ha absorbido muy rápida la tecnología para ofrecerla como servicio, y, sobre todo, hemos construido una propuesta muy interesante para el sector privado y el público”.

Desde la perspectiva de Arrow, “analizando los tres primeros trimestres, parece que será un año bueno para todos, sobre todo por el incremento de los presupuestos de la Administración Pública y por los proyectos de grandes multinacionales. Sin embargo, ha habido algunas incertidumbres en el mercado, algunos problemas en la entrega de productos y el cambio euro/dólar, en la parte negativa. Con todo, la tendencia del mercado es muy positiva”.

CAPEANDO EL PROBLEMA DE LA FALTA DE EXPERTOS

Tal y como explica Ángel García, “nos encontramos en un mercado con un crecimiento importante, lo que se traduce en que la demanda

de profesionales también es alta. Además, son profesionales con altas capacidades y un coste elevado para las empresas, que tienen unos presupuestos limitados. Si a esto le sumamos que en muchos casos el canal es la cantera de este tipo de profesionales para otros jugadores más grandes, esto hace que nos tengamos que reinventar todavía un poco más. Nuestra estrategia frente a esto es hacer cultura de empresa, que el empleado sienta Arrow como una compañía en la que poder tener un proyecto y crecer. Es la principal arma para retener talento”.

Para David Gasca, “en el mercado no hay recursos para atender la demanda de profesionales, por eso el papel del canal es fundamental, contando con esas capacidades para facilitar la labor de los clientes. En nuestro caso, tenemos la ventaja de ser una multinacional, pero con los beneficios de ser un grupo pequeño, el de la seguridad, con lo que somos un sitio muy interesante para trabajar”.

Según comenta Sergio Martínez, “tenemos un problema con la educación en España. Y en nuestro sector es muy evidente cuando vemos la brecha de género, por

“ SI LA ECONOMÍA SIGUE CRECIENDO Y SE SIGUE DIGITALIZANDO, ES NORMAL QUE LA SEGURIDAD CREZCA POR ENCIMA DEL MERCADO ”

DAVID GASCA

business unit coordinator
Enterprise Security en **V-Valley**





Clica en la imagen para ver la galería

ejemplo, porque no se ha hecho el impulso necesario en las vocaciones STEM de las mujeres. Hay mucho por hacer, pero, para empezar, hay que asumir que el mundo de la ciberseguridad es muy amplio, y hay que suscitar el interés en las personas desde pequeños para que

vayan adquiriendo ese gusto por la tecnología”.

Añade Alberto Carrillo que, efectivamente, “hay un problema de raíz en la educación, y otro muy importante en la necesidad de atraer talento, y lo que tenemos que hacer es ver cómo balanceamos los recursos con la capacidad económica que tenemos, recordando que competimos no solo entre nosotros, sino con otros países. El canal es la clave para mutualizar recursos para dar cobertura a las necesidades de las empresas con ciberseguridad como servicio”.

Desde el punto de vista de Antonio Martínez, “la formación es la clave, hay que insistir en ello. Y hay que concienciar a los alumnos de que sean proactivos, porque los conocimientos son variables, y debemos darles las armas para que puedan reaccionar ante un incidente o problema. Estamos haciendo mucho esfuerzo en esto, con colaboración con centros formativos, porque es lo que vemos que falta y lo que más valoran los usuarios”.

LA REALIDAD DEL MERCADO

A lo largo de este año, apunta David Gasca, “va a seguir habiendo operaciones de consolidación en el mercado. En nuestro caso, seguiremos vigilando las áreas de interés, y valorando operaciones que puedan aportar valor”, y coincide con él Antonio Martínez, que añade “además de posibles acercamientos de fabricantes, también lo vamos a ver en grupos sociopolíticos”.

“El mercado se está consolidando”, indica Sergio Martínez, “porque mucha innovación proviene de startups que aportan oportunidades de negocio”, y es que, en general, recalca Alberto Carrillo, “la tecnología se mueve a más

velocidad que el mercado, y siempre surgen compañías nuevas que aportan ideas, pero que no tienen el volumen para ejecutarlas. Y más en el mundo de la ciberseguridad, donde estamos en una carrera constante para potenciar y perfeccionar la protección frente a las crecientes ciber-amenazas”.

Para Ángel García, “si no hay consolidación, habrá colaboración. La compra de empresas está en el ADN de este sector. Para llegar a un mercado donde no tienes entrada o no eres predominante, necesitas hacerlo por adquisición. Y como este es un mercado tan cambiante, hay que estar muy atentos”. ■

MÁS INFO +

» [Tendencias en Ciberseguridad para 2023 y los retos para el canal](#)



COMPARTIR EN REDES SOCIALES