TENDENCIAS EN TORNO A LA CIBERSEGURIDAD EN 2024

En 2023 se volvieron a batir récords en materia de incidentes graves en ciberseguridad, con cifras desorbitadas de ataques diarios, dirigidos principalmente a aquellas organizaciones que no están tan protegidas y cuyo perfil suele ser el de pequeña y mediana empresa. ¿Cuáles serán las nuevas tendencias que guiarán el panorama de la ciberseguridad este año y qué papel jugará el canal frente a los retos que están surgiendo en torno a la protección del dato?

Debatimos sobre estas cuestiones con representantes de cuatro importantes jugadores del mercado de ciberseguridad del mercado español: Roland Aveillan, chief sales manager de B-FY; Martín Trullás, director de la división Advanced Solutions en Ingram Micro España; Eduardo Brenes, territory manager de SonicWall

DEBATE IT >> Debatimos junto a representantes de B-Fy, Ingram Micro, SonicWall y Stormshield, sobre las tendencias que protagonizarán el panorama de la ciberseguridad en 2024 y sobre el papel que tendrá el canal en la protección del dato.

España; y Borja Pérez, country manager de Stormshield Iberia.

UN AÑO COMPLEJO EN MATERIA DE CIBERSEGURIDAD

Tal y como explica Roland Aveillan, “no sabemos cuáles van a ser los datos definitivos de crecimiento, pero la tendencia en el mundo de la seguridad es al alza. Y va a ir a más porque los ciberdelincuentes tienen cada día unos costes más bajos, por las innovaciones tecnológicas, lo que va a provocar más operaciones y un mejor ROI, lo que, a su vez, supone que las empresas tengan que protegerse e invertir más de forma ineludible”.

En opinión de Martín Trullás, “el modelo de valor ha tenido unos crecimientos contenidos, pero en ciberseguridad hemos crecido más. Depende de las soluciones que tenga cada empresa y de la madurez de los fabricantes. Hemos crecido en 2023 a doble dígito y la tendencia se va a mantener. Las empresas van a seguir invirtiendo por necesidad, y nuevas tecnologías, como la IA o los hiperescalares, van a elevar el nivel de ciberseguridad mínimo, lo que llevará a las empresas a seguir protegiéndose, tanto en el perímetro como en el puesto de trabajo”.

Para Eduardo Brenes, “hemos estado en línea con la previsión de crecimiento que hacía IDC (que era del 9,2%). En nuestro caso, hablamos de una compañía ya consolidada con una triple apuesta muy clara por la venta a través de partners, la pyme como principal cliente y una propuesta tecnológica que hemos ido complementado a partir de los firewalls de nueva generación. De hecho, recientemente hemos realizado dos adquisiciones que complementan nuestra apuesta”.

Finaliza Borja Pérez explicando que “para nosotros el año ha sido

espectacular. A nivel global, el crecimiento ha estado en torno al 10%, pero en España hemos crecido un 40%, apoyado en Defensa, una línea que no estaba tan desarrollada en España, algo que ha cambiado este año. Sigue habiendo mucha venta de firewalls físicos, y parece que no acaba de despegar el modelo como servicio. Este año creceremos, no creo que tanto, pero los indicadores nos hacen ser optimistas”.

INCREMENTAR EL PRESUPUESTO DE CIBERSEGURIDAD

Añade Martín Trullás que “los fondos europeos van a seguir favoreciendo proyectos donde la ciberseguridad es pieza clave. Va a haber mucho movimiento en el sector público, y en la empresa privada la ciberseguridad también va a ser protagonista”.

En este sentido, para Eduardo Brenes, “la situación general, y las previsibles bajada de los tipos de interés, pueden hacer pensar en un recorte de los presupuestos, pero creo más bien que va a ser una transferencia de otras áreas como el cómputo o el networking, que se van a consolidar en ciberseguridad para minimizar los riesgos”.

Según Roland Aveillan, “el posible que crezca el peso de la ciberseguridad en los presupuestos de los CIO por encima del 20% actual”, a lo que añade Borja Pérez que “hay veces que tienes que pelear mucho con los departamentos de compras, más que con el CIO, sobre todo en empresas más grandes, para

justificar una inversión de una solución de ciberseguridad que protegen inversiones mucho mayores. Pero también es parte de nuestro trabajo ayudar al CISO a justificar internamente la inversión, dándole argumentos más allá del miedo, hablando de las ventajas competitivas de contar con una ciberseguridad bien implantada".

CIBERSEGURIDAD, UNA INVERSIÓN, NO UN GASTO

Sin embargo, en palabras de Martín Trullás, "el desconocimiento sobre la ciberseguridad en la pymes es mayor. Ellos lo ven como un gasto, cuando es una inversión para proteger la compañía. Y esto en las pequeñas empresas es complicado hacerlo entender. La gran empresa sí está más concienciada".

Pero, apunta Borja Pérez, "en este tipo de cliente el mensaje del miedo a lo que le puede pasar si no tiene una seguridad adecuada. Es nuestra labor, junto con el canal, mostrar las ventajas competitivas de hacer estas inversiones".

Se muestra de acuerdo con él Eduardo Brenes, que añade que "queda mucho por hacer en materia de concienciación en ciberseguridad, y es labor nuestra ayudar tanto al canal como al cliente final. Para las empresas, ser más ciberseguras que su competencia es un valor diferencial, y debemos hacerles entender que la seguridad es una ventaja competitiva. Ser más ciberresiliente y ser capaces de recuperarse antes que la competencia de un ataque, es una ventaja competitiva".

Para Martín Trullás, "cuando hablamos de otras áreas, las empresas ven la inversión como una necesidad para seguir creciendo, facturando, haciendo negocio... pero en ciberseguridad no es así, porque piensan que con una solución básica están cubiertos. Es una realidad que siguen viendo la ciberseguridad como un gasto, no como una inversión", pese a que los datos del año pasado muestran un claro incremento de los costes para las empresas en caso de ciberataque. "El cliente debe decidir dónde coloca el presupuesto, y en ciberseguridad, en empresas pequeñas y medianas, cada día es más costoso explicarlo", concluye Martín Trullás.

> "CUANDO HABLAMOS DE CIBERDELINCUENCIA A GRAN ESCALA, HABLAMOS DE ORGANIZACIONES QUE PLANEAN ATAQUES SOBRE EL PUNTO MÁS DÉBIL DE LA CADENA, PORQUE TAMBIÉN TIENEN SU PROPIO ROI Y SUS OBJETIVOS DE INGRESOS"
>
> **ROLAND AVEILLAN,** chief sales manager de **B-FY**

Desde la perspectiva de Roland Aveillan, "el CISO o, incluso, el CIO, tienen que vender la seguridad internamente. El problema es que hablan leguajes diferentes, pero el CEO sí entiende de costes, y eso solo sucede a posteriori, una vez que se ha producido el ataque".

LA IA Y LA CIBERSEGURIDAD

El papel de la IA en la creación de amenazas, comenta Eduardo Brenes, "va a incrementarse mucho en los próximos años, y los fabricantes tendremos que hacer mucho hincapié en ello. Las empresas deberían asumir unos aspectos básicos de ciberseguridad para hacer frente a amenazas como los deep fakes o los deep voices. Hay que seguir apostando por la formación y la concienciación de los usuarios y las empresas".

Sin embargo, la IA también puede ser una herramienta muy potente de protección para las empresas, recuerda Borja Pérez, "y cada vez hay más herramientas basadas en machine learning e inteligencia artificial. Y cada vez hay más interoperabilidad entre fabricantes y proveedores de servicios para potenciar la ciberseguridad, porque es una

batalla desigual contra el malware, y debemos colaborar".

AMENAZAS PARA EL NUEVO AÑO

En opinión de Roland Aveillan, "la superficie de ataque se ha ampliado, el paradigma ha cambiado, y el objetivo ya no son las grandes organizaciones, porque cada vez hay más un negocio de malware como servicio. Los atacantes van a aprovechar vías como IoT, coches eléctricos, domótica, conectividad... y esta capilarización de los puntos de entrada puede ampliar las posibilidades de ataque".

Añade Eduardo Brenes "la inteligencia artificial, que va a proporcionar no solo nuevos vectores de ataque, sino que permite a los ciberdelincuentes lanzar ataques más sofisticados con menos conocimientos técnicos. La IA generativa y su capacidad para generar contenidos de manera automática, perfecciona amenazas como el phishing. También es preocupante el uso de la IA generativa para adquirir datos biométricos de los usuarios".

"El problema es que nos adentramos en un entorno que no está suficientemente regulado", apunta Martín Trullás, que añade que "es un problema global y necesitamos una regulación clara para saber cómo defendernos. Es la IA, pero también la seguridad biométrica y otros muchos resquicios que pueden aprovechar los ciberdelincuentes".

Clica en la imagen para ver la galería

Apunta Borja Pérez que "IoT y 5G tienen problemas de inseguridad desde su diseño, pero el despliegue es una necesidad y la seguridad ha pasado a un segundo plano. Esto aumenta la superficie de exposición desde el propio diseño, lo que es un problema mucho más grave".

> "LAS EMPRESAS VAN A SEGUIR INVIRTIENDO POR NECESIDAD, Y NUEVAS TECNOLOGÍAS, COMO LA IA O LOS HIPERESCALARES, VAN A ELEVAR EL NIVEL DE CIBERSEGURIDAD MÍNIMO"
>
> **MARTÍN TRULLÁS,** director de la división Advanced Solutions en **Ingram Micro** España

Según Roland Aveillan, "por desgracia, cuando unos ciberdelincuentes quieren meterse en una organización, tienen las herramientas y el conocimiento adecuado para hacerlo. Pero, cuando hablamos de ciberdelincuencia a gran escala, hablamos de organizaciones que planean ataques sobre el punto más débil de la cadena, porque también tienen su propio ROI y sus objetivos de ingresos".

Coincide con él Eduardo Brenes, que añade que "la IA generativa ha democratizado esa capacidad y ya no son necesarios grandes conocimientos para ataques sofisticados. Pero lo cierto es que casi todos los ataques comienzan con un robo de credenciales, y tienen como objetivo monetizar cualquier ataque. En los próximos meses vamos a ver cómo se incrementa esta tendencia".

FALTA DE CAPACITACIÓN EN LOS PROFESIONALES

Esto coincide con una gran falta de capacidades de tecnología, en general, y de ciberseguridad, en particular, en el mercado. Como indica Martín Trullás, "hay un problema de personas cualificadas en el canal para poder dar servicio a sus clientes, porque no son capaces de obtener y retener este talento. Y es un problema que va en aumento".

Según reciente informe, apunta Eduardo Brenes, "hay 317.000 vacantes por cubrir de profesionales

de ciberseguridad en Europa y se estima que en España son 60.000. Hay un gap cada vez más grande, y no hay el relevo generacional necesario para cubrir estas vacantes. Es algo muy preocupante, y va a ser imprescindible el reskilling y el upskilling de profesionales de otros segmentos de TI hacia la ciberseguridad. Y tenemos que ayudarles a hacerlo".

"Hay dos elementos para paliar esta necesidad", explica Roland Aveillan, "los copilotos, para ayudar a incrementar la capacidad de defensa y, por otra parte, no pensar tanto en la defensa, sino en la parte más proactiva de formación y concienciación. Junto con esto, proteger el punto de entrada, porque si consiguen entrar el problema es más difícil de solucionar".

Frente a esta realidad, los MSSP, comenta Martín Trullás, "pueden ayudar", pero "tienen el mismo problema de obtención y retención de talento", apostilla Borja Pérez, que añade que "el canal es el departamento de TI de muchas organizaciones, y muchos elementos de protección de estas empresas ya se estaban ofreciendo como servicio. No podemos pensar solo en los

Clica en la imagen para ver la galería

grandes MSSP, sino en el canal que lo está haciendo con sus clientes".

Estos partners, recalca Martín Trullás, "se han adaptado a sus clientes, y les están proporcionando estas herramientas como servicio, aunque no hayan instalado la infraestructura en el cliente. Ofrece la TI como servicio y añade también

> "LAS EMPRESAS DEBERÍAN ASUMIR UNOS ASPECTOS BÁSICOS DE CIBERSEGURIDAD PARA HACER FRENTE A AMENAZAS COMO LOS DEEP FAKES O LOS DEEP VOICES"
>
> **EDUARDO BRENES,** territory manager de **SonicWall** España

la capa de ciberseguridad. Tiene que dar al cliente un servicio que incluya todos los elementos que este necesita, tanto si venden la infraestructura como servicio o el servicio sobre la infraestructura. Es algo que estamos viendo también en los pequeños partners con un foco más local".

Pero el canal tiene un problema, señala Borja Pérez, "porque no tiene capacidad para retener a los profesionales, porque ya no solo compite contra otros partners, sino contra fabricantes o, incluso multinacionales, pero a lo mejor es que están cobrando baratos los servicios, y deberían adecuar sus estructuras de costes incrementando el coste del servicio, aunque esto es algo complicado".

Otro elemento a securizar es la cadena de suministro, pero quizá hay que dar un paso atrás y, como apunta Martín Trullás, "contar con una cadena de suministro local en un mercado global. Necesitamos cadenas de suministra más próximas", y es que, como añade Eduardo Brenes, "hay estudios que afirman que en 2025 el 45% de las organizaciones van a sufrir un ataque a través de su cadena de suministro. Por eso es tan importante establecer arquitecturas de ZTNA y hacia estas opciones es hacia las que vamos todos los fabricantes".

CONSOLIDACIÓN EN EL MERCADO DE LA CIBERSEGURIDAD

En palabras de Martín Trullás, "los mayoristas globales tienen cada vez más fuerza en el mercado por la propia naturaleza del negocio, y porque los clientes demandan una cobertura global para la que necesi-

Clica en la imagen para ver la galería

> IOT Y 5G TIENEN PROBLEMAS DE INSEGURIDAD DESDE SU DISEÑO, PERO EL DESPLIEGUE ES UNA NECESIDAD Y LA SEGURIDAD HA PASADO A UN SEGUNDO PLANO

BORJA PÉREZ, country manager de **Stormshield** Iberia

tas unos activos más potentes y un mayor respaldo. Un mayorista global puede ofrecer más herramientas a sus clientes, y eso es algo que puede darse también con fabricantes pequeños que necesiten a otros para crecer".

"En el mercado mayorista ha habido una gran consolidación", comenta Eduardo Brenes, "ha sido una tendencia clara en el mercado, y también ha habido una gran convergencia en la capa de fabricantes, porque la seguridad debe ser cada día más integral. Es una forma de completar los catálogos de los fabricantes". Y, apunta Martín Trullás, "también lo hemos visto en los integradores, porque, al final, necesitas una propuesta mayor para poner delante de tu cliente. La consolidación la vemos en todos los ámbitos de TI". ■

Clica en la imagen para ver la galería

MÁS INFO +

» Tendencias de ciberseguridad a debate

COMPARTIR EN REDES SOCIALES