La iniciativa arrancó con la celebración del Divergente Day

Arrow se vuelca con la comunidad preventa con Divergente

"Hay que ser divergentes". Iñaki López, máximo responsable de Arrow en España y Portugal, enarboló, en el Divergente Day, el valor de la divergencia como elemento disruptor y creativo en la propuesta que los profesionales de preventa, a los que se dirigía el evento, deben presentar a sus clientes. "La apuesta por el valor es una constante en Arrow", señaló. "Y esta iniciativa es una muestra de ella: tratamos de ayudar a los preventas, que son los que viven en el epicentro de la transformación que están llevando a cabo las empresas". En Arrow, reiteró, "queremos ser únicos y divergentes; con una marca propia".

Divergente Day se celebró el pasado 4 de marzo, en Madrid, consiguiendo reunir a cerca de 500 profesionales. Arrow estuvo arropado por 25 de las marcas que forman parte de su

oferta y, junto a la celebración de dos mesas de expertos, una centrada en la seguridad y la otra en el mundo del centro de datos, existieron espacios vinculados con la seguridad, la nube híbrida, la nueva generación del centro de datos, la inteligencia del dato y el IoT y el *edge* en el entorno de la nube híbrida.

El proyecto Divergente va mucho más allá de la celebración del evento. El objetico es crear una comunidad que se mantenga en permanente conexión, nutriéndose de información relevante para los profesionales que se encargan de realizar las labores de preventa en las empresas. "Es una ventana para mirar al futuro", insistió Lopéz, que recordó que el mayorista cuenta en su plantilla con cerca de 5.000 profesionales de este perfil en el mundo, que se forman en cada uno de los mercados en los que opera, como es el caso de la seguridad, el IoT, el centro de datos o la analítica. "Un espacio para el debate, la reflexión, la colaboración y el *networking*".

Los desafíos de la seguridad en 2020

La seguridad señala uno de los negocios claves para Arrow. Un apartado que mantiene su crecimiento y que sigue siendo una oportunidad para el canal. Según la consultora Gartner, el año pasado las empresas se gastaron en seguridad alrededor de 124.000 millones de dólares, a nivel mundial, lo que supone un 8 % más que en 2018. En España, las empresas también han seguido invirtiendo más en seguridad. Según la consultora IDC, en 2019 las empresas españolas se gastaron más de 1.300 millones de euros en protegerse, lo que sumó un 7 % más que en 2018. Un gasto que hasta 2021 se incrementará, año a año, más de un 7 %.

La mesa de expertos reunió a Aruba, Amazon Web Services (AWS), Check Point y Fortinet. Un cuarteto que defendió la necesidad de que las empresas diseñen una seguridad global, que exige el entendimiento de las diferentes soluciones y fabricantes, y en la que,

por encima de la detección, que sigue siendo un elemento clave, las empresas deben empoderar la prevención.

Rafael del Cerro, *cyber security systems engineer* del sur de Europa de Aruba, insistió en el valor, indispensable, que tiene la visibi-

lidad de la red. "Nuestro mantra cuenta con dos palabras: visibilidad de lo que las empresas tienen conectado a la red y control, para ir incrementando la seguridad de todos los elementos en función de lo que tienen conectado". Del Cerro recordó el cambio que se ha operado en el perímetro. "Se ha desvirtualizado. Ya no es estático", insistió. "Existe una arquitectura híbrida, que aúna los elementos que están en el centro de datos con las cargas que tienen en la nube, lo que exige contar con las herramientas que permitan a las empresas disfrutar de una completa visibilidad de lo que tengan y descubrir cómo se comportan los diferentes dispositivos".

En los entornos en la nube es necesario dejar claro el concepto de responsabilidad compartida que compete a proveedores de *cloud* y a clientes; una entente complicada en la que las "competencias" de cada uno deben estar claras. Carlos Sanchiz, *manager solutions architect* de AWS, recordó que los primeros son responsables de la seguridad del *cloud*, "como tal", lo que afecta, entre otras competencias, al control de acceso, mientras que los clientes son responsables de la seguridad dentro del *cloud*, lo que apunta al diseño de las aplicaciones adecuadas a la gestión del dato.

"Divergente es un espacio para el debate, la reflexión, la colaboración y el networking"

Eusebio Nieva, *SE manager* Iberia de Check Point, recordó que no hay que perder de vista el dinamismo de la nube; lo que exige que hay que estar siempre pendiente de la seguridad ya que el servicio evoluciona continuamente. "Debemos proporcionar continuamente al canal las herramientas necesarias para que pueda llevar a cabo esa vigilancia permanente de la manera más sencilla posible". Nieva explicó que una gran parte de los errores de seguridad que se produjeron el pasado año en el entorno de la nube son ingenuos. "Se refieren a errores de configuración o que el acceso estaba, incluso, en el código público".

La complejidad de las amenazas ha llevado a los fabricantes a desarrollar el concepto de "plataforma". Un concepto que permite orquestar, de manera completa, la seguridad de la empresa; lo que exige que ésta sea abierta y completamente transparente. José Luis Laguna, *director systems engineering* de Fortinet, reconoció que las empresas integran soluciones de diferentes marcas, lo que exige la integración y el entendimiento entre ellas. "Y no solo con los fabricantes de seguridad sino con otro tipo de proveedores".

Laguna recordó que la superficie de los ataques se está expandiendo y el desarrollo de aplicaciones, múltiples, es muy rápido. "Hay que cubrir de forma adecuada toda esta superficie y dar respuesta a los atacantes, que también están utilizando tecnologías como la inteligencia artificial o el *machine learning*, para hacer más sofisticados los ataques". En definitiva, "se necesitan herramientas que permitan orquestar todas las soluciones de las diferentes marcas, que permitan una mayor automatización, más cuando existe una escasez de profesionales especializados en la seguridad".

En España, se tiene la sensación de que las grandes empresas, que cuentan con mayores capacidades, tanto de recursos como de presupuesto, disponen de mejores sistemas de seguridad. Sin embargo, el año pasado los ataques de los *hackers* también tuvieron grandes "éxitos" en este tipo de empresas. A juicio de del Cerro, ha faltado concienciación acerca de cómo proteger el perímetro y los nuevos activos que se han incorporado a la nube. "En esta evolución, no se sabe dónde colocar la seguridad y ver qué solución encaja en cada entorno; eso sí, adecuadamente relacionadas e interconectadas".

Nieva puntualizó que la inversión de una empresa depende, no tanto de su tamaño como de su cultura tecnológica. "Y también de la evolución de los ataques y de la percepción del riesgo de los mismos, más si han sido víctima de alguno de ellos". Para encontrar una respuesta al éxito de los ataques, más que falta de concienciación, el responsable técnico de Check Point apeló al cambio de paradigma en la seguridad. "Ante la evolución de las amenazas, la detección no es suficiente; hay que aplicar la prevención", aconsejó.

Siempre el *ransomware*... Y el *threat hunting*

El *ransomware* sigue siendo la tormenta perfecta para los *hackers*. Se calcula, según Forrester, que el pasado año este tipo de ataques se incrementó en un 500 %, con una clara tendencia hacia el *ransomware* dirigido. En España ha habido sonados ataques, que han afectado tanto al sector público como al privado. Laguna recordó que hay que hacerles frente de tres maneras diferentes. "La protección del perímetro es esencial", volvió a insistir. "Junto a él, es esencial asegurar el *endpoint*, donde no bastan un antivirus ni un *antimalware* tradicionales, debido al avance de los ataques". Y, por último, la concienciación del usuario que "sigue dando clic a los correos maliciosos".

Asegura Nieva que cerca del 90 % de los ataques de *ransomware* sucedidos el año pasado eran evitables. "Contamos con la tecnología adecuada para detenerlos", especificó. "Pero hay que implementarla".

El concepto de *threat hunting*, que apuesta por una mayor proactividad frente a las medidas más tradicionales y reactivas, también estuvo presente en el debate. La falta de presupuesto de las empresas y, sobre todo, la carencia de un equipo de expertos propio capaz de gestionar la seguridad provoca que sea muy complicado que las defensas empresariales evolucionen al mismo tiempo que lo hace el cibercrimen. Por ello, se oye, cada vez más, este concepto. Del Cerro volvió a insistir en la obligatoriedad de contar con herramientas que permitan disfrutar de la visibilidad de lo que ocurre en la red y ver dónde se han producido los problemas. "Debemos contar con sistemas que aseguren la protección desde el momento en el que se conecte el usuario. Hay que autenticarle y, a partir de ahí, darle conectividad y hablar con otros elementos para asegurar una protección completa".

> *"Por encima de la detección, que sigue siendo un elemento clave, las empresas deben empoderar la prevención"*

Por último, se apeló a la GDPR, una ley que regula la responsabilidad que compete a las empresas que almacenan y gestionan los datos; así como las sanciones en el caso de que se produzcan brechas y filtraciones. Del Cerro aseguró que se articula como una oportunidad de oro para el canal. "Los profesionales del ámbito de la preventa pueden aportar valor y convertirse en el socio de confianza de las empresas en el campo de la seguridad". El directivo de Aruba aprovechó para recordar que el mercado tiene cada día más claro que el entorno *cloud* "es mucho más seguro que el área *onpremise*".

Pasado, presente y futuro del centro de datos

La segunda mesa de debate se centró en el área del centro de datos, que es el apartado que más peso tiene en Arrow. Participaron IBM, Lenovo, Microsoft y NetApp. Lo que se conoce como "*next generation data center*" o, lo que es lo mismo, "la próxima generación del centro de datos", está marcado por dos factores. El primero son los proyectos de transformación digital que están llevando a cabo las empresas. Una transformación digital que no la marca la tecnología sino los objetivos de negocio de las empresas. El segundo factor es la nube. Un entorno, en el que en cualquiera de sus sabores (pública, híbrida y privada), las empresas están trasladando una gran parte de sus cargas.

En la definición de los elementos que debe exhibir un centro de datos para, primero, responder a las necesidades actuales del negocio y, segundo, convertirse en una herramienta eficaz al servicio del mismo; el

cuarteto apeló a la flexibilidad. "Tiene que adaptarse de manera rápida al negocio", arranca Alberto García, *technical sales leader* de IBM SPGI. En ocasiones, a su juicio, el departamento técnico no responde, de manera ágil, a lo que exige el negocio. "Incluso, los técnicos deberíamos ponerles retos a los responsables del negocio y no al revés". Junto a la flexibilidad, García no olvida la seguridad, vital, ni el *expertise*. "Un profesional con talento marca la diferencia".

Gregorio Chillón, *solutions architect* de Lenovo, añade la escalabilidad de los servicios que la empresa puede requerir. Junto a ella, la conectividad. "No tiene sentido un centro de datos aislado del mundo: es necesaria la conexión con otros centros de datos, moviendo cargas entre ellos".

No olvidaron apelar a la agilidad. Enrique Ruiz, director de tecnología de *partners* de Microsoft, recuerda que el negocio demanda inmediatez. "Por las exigencias del mercado ya no hay proyectos a seis meses, ni a un año".

La eficiencia se suma también al centro de datos. Jaime Balañá, director técnico de NetApp, asegura que es un concepto que va más allá del mero ahorro energético. "Se trata de hacer más con menos". Unos centros de datos que deben estar mucho más automatizados para alcanzar la flexibilidad y agilidad requerida. "Se requieren, cada vez más, portales de autoservicio o provisiones automáticas de recursos", recuerda. "Y las tecnologías, tipo DevOps, van a permitirla mucho más".

Híbrido y *multicloud*

Alberto García recordó que el cliente está instalado en un entorno *multicloud* e híbrido. "Es esencial ofrecer un control del entorno de los clientes, que se mueven en un entorno disgregado, de manera efectiva y segura". Un entorno en el que, recuerda Balañá, los clientes deben mover sus datos, con facilidad, al lugar que mejor les convenga en cada momento. "La gestión de los datos es uno de los retos principales; más ahora que los datos son más diversos", explica. "La posibilidad de que éstos residan en un único *data lake*, para poder analizarlos y sacar partido de ellos en beneficio del negocio".

"La gestión de los datos es uno de los retos principales; más ahora que los datos son más diversos"

Un movimiento de los datos en el que aparecen retos como la facturación. "En un entorno *multicloud* el cliente debe ser capaz de gestionar los costes que se generan en cada una de las nubes públicas; lo que puede disparar los gastos si no se hace de manera adecuada", reiteró Balañá. Además, hay que tener en cuenta los costes de operación y la manera de sincronizar los datos, definiendo quién tiene acceso a ellos. "Hay que protegerlos porque son los activos más importantes de las empresas y además hay que hacerlo en diferentes escenarios". Por último, las empresas requieren contar con equipos preparados para ello. "Hay una escasez de profesionales especializados en el *cloud*", denunció. "Es un reto retener ese talento".

Todo es susceptible de subirse a la nube. Ruíz asegura que incluso en el área de las comunicaciones, que podría presentar alguna limitación por la necesidad de estar siempre conectado, también se están subiendo cargas sin restricción. Sin embargo, Balañá señaló

que las únicas cargas que no son, por el momento, susceptibles de subir a la nube son aquellas que por motivos regulatorios deben residir en España. "Por el momento los proveedores de *cloud* pública no disponen de ubicaciones locales en nuestro país".

Y lo "propietario"...

Sin embargo, a pesar de todo lo que se habla de esta "nueva" generación de los centros de datos, en España existe todavía un gran número de centros de datos, complejos, con tecnologías propietarias, que deben sostener grandes cargas. En el debate, se habló de si son entornos que se mantendrán a pesar de las "nuevas" tendencias o acabarán optando por la externalización, por modelos con mayor flexibilidad o se trasladarán a proveedores de *hosting* y de nube. Para el representante de IBM, director técnico del negocio *mainframe*, lógicamente serán entornos que se mantendrán. "Van a estar en el mercado para siempre", defendió. "No son tan estancos como los percibe el mercado ya que se pueden integrar con entornos abiertos", aseguró. La fuerza prevenía, a su juicio, no tiene que dirigir su discurso hacia su eliminación sino en explicar sus capacidades de flexibilidad y de conexión con el *cloud*. "Son entornos conectables y que se pueden comunicar con otros centros de datos".

Chillón ratificó que no se trata de eliminarlos. "No sé que valor aportaría al cliente su eliminación", valoró. La clave, aseguró, es focalizarse en las áreas de innovación como repositorio de lo nuevo.

Enrique Ruiz, sin embargo, apeló a que todo, más pronto o más tarde, acabará en la nube pública "por la racionalidad de la ubicación de los sistemas". Que no es acceso público, especificó. "Hay que asegurar, de manera adecuada, el mismo".

Nace Divergente: el espacio que Arrow consagra a la comunidad preventa de España

Alrededor de 500 personas acudieron el pasado 4 de marzo al Divergente Day, el evento organizado por Arrow, centrado, por primera vez, en los profesionales que se dedican a las labores de preventa en el canal español. Iñaki López, máximo responsable del mayorista en España y Portugal, apelaba al término, divergente, que daba nombre al proyecto. "Hay que ser divergentes", animaba en la presentación. "Una divergencia, que se presenta como un elemento disruptor y creativo, en la propuesta de este tipo de profesionales a sus clientes".

Iñaki López, director general de Arrow en España y Portugal

El proyecto Divergente va mucho más allá de la celebración del evento en el que Arrow estuvo arropado por 25 fabricantes, claves en su oferta. El objetivo es crear una comunidad que se mantenga en permanente conexión, nutriéndose de información relevante para los profesionales que se encargan de realizar las labores de preventa en las empresas. "Un espacio para el debate, la reflexión, la colaboración y el *networking*".

"Debemos ayudar al canal a ganarse la confianza de sus clientes"

Aruba fue una de las 25 marcas que arroparon a Arrow en la presentación de su proyecto Divergente, que arrancó con la celebración del Divergente Day. Rafael del Cerro, *cyber security systems engineer southern Europe* de Aruba, valora especialmente las relaciones que se establecen en este tipo de eventos, que pueden ayudar a los fabricantes a acercar su propuesta de valor al canal.

Rafael del Cerro, *cyber security systems engineer southern Europe* de Aruba

En el acercamiento del canal al cliente final, del Cerro recomienda que es primordial observar cuál es la problemática que tienen en el ámbito de la seguridad y que les aporten soluciones que les permitan "ganarse su confianza". En el caso concreto de Aruba, el directivo insiste en la importancia que tiene la visibilidad de la red en la definición de las estrategias de seguridad. "Es el paso previo para desarrollar una buena protección".

"Estamos viviendo un momento de transición tecnológico único"

La comunidad preventa del canal es una referencia en el negocio de Amazon Web Services (AWS). "Se enfrentan a importantes retos a la hora de migrar cargas a la nube, que es un paradigma totalmente diferente", reconoce Carlos Sanchiz, *manager solutions architect* de AWS, que valora que eventos como Divergente Day, ayudan a intercambiar impresiones y analizar los retos.

Carlos Sanchiz, *manager solutions architect* de AWS

Sanchiz cree que vivimos un "momento de transición tecnológico único". La comunidad preventa, puntualiza, "debe convertirse en un consultor para asegurar una relación continua con sus clientes".

"Los preventas deben anticiparse, incluso, a lo que los clientes aún no saben que necesitan"

Eusebio Nieva, *SE manager* Iberia de Check Point, explica que un evento como Divergente Day, dirigido a la comunidad preventa, tiene un enorme valor para este tipo de profesionales ya que les permite, ante la exigencia de ofrecer una solución completa al cliente final, disfrutar de una visión completa de todas "las opciones que existen en el mercado".

Nieva les recomienda que, no solo deben cubrir las necesidades de los clientes, sino "incluso anticiparse a lo que aún no saben que necesitan".

Eusebio Nieva, *SE manager* Iberia de Check Point

"Divergente Day nos ha permitido dar más valor a nuestras soluciones tecnológicas"

Alejandro Reyeros, *systems engineer* de Fortinet, valora muy positivamente la celebración del Divergente Day, destinado a la comunidad preventa del sector TIC. "Es una forma inmejorable de dar valor a las soluciones tecnológicas", asegura. Reyeros invita a estos profesionales a acercarse a Fortinet. "Antes de desplegar cualquier propuesta el punto crítico es escuchar a los clientes, que es el camino para ganar su confianza".

Alejandro Reyeros, *systems engineer* de Fortinet

"Arrow ha sido pionero con Divergente Day, un evento pensado para la comunidad de preventa"

Alberto García, director técnico para el área de sistemas de IBM en España, Portugal, Grecia e Israel, reconoce que llevaban mucho tiempo esperando un evento de las características que tuvo Divergente Day. "Tiene un valor inigualable y Arrow ha sido pionero en dedicar un evento, con carácter exclusivo, a la comunidad de preventa de los *partners*", reconoce. "Es vital para que esta comunidad continúe evolucionando".

Alberto García, director técnico para el área de sistemas de IBM

El directivo de IBM recomienda al canal incidir en la confianza. "Nadie compra sin una confianza en quién le comercializa la solución", insiste. "No asume riesgos, por lo que, además de la calidad de la solución, es básica esa relación".

"Es clave tener actualizada a la comunidad preventa"

Para un profesional que se dedica a la preventa no es sencillo mantenerse permanentemente actualizado en todas las tecnologías que existen en el mercado. Rafael Herranz, director del negocio de centro de datos en Lenovo, es consciente de ello y asegura que eventos como Divergente Day ayudan a "transferir conocimiento", sobre todo en el caso de una empresa como Lenovo, que exhibe una oferta tan amplia. "La comunidad preventa está siempre aprendiendo y es vital que esté al día de todas las tecnologías".

Rafael Herranz, director del negocio de centro de datos en Lenovo

"La formación es fundamental para que los preventas lleven a cabo su labor"

Enrique Ruiz, director de tecnología de *partners* de Microsoft, reconoce que en ocasiones se ha dejado desatendidos a los profesionales de preventa técnicos de los *partners*. "Contar con un evento como Divergente Day es estupendo para Microsoft". El directivo señala la formación como la recomendación principal para estos profesionales de preventa. "En un momento de transformación continua como es éste, es fundamental que los preventas conozcan lo que está disponible para llevar a cabo su tarea de integración". Ruiz recomienda el uso de los canales oficiales de formación, gratuitos para todos los *partners*.

Enrique Ruiz, director de tecnología de *partners* de Microsoft

"Los profesionales de preventa no pueden estancarse: siempre deben seguir aprendiendo"

Lógicamente, Jaime Balañá, por su vocación 100 % técnica, valora de manera muy positiva Divergente Day. "No hay muchos eventos centrados en nuestro perfil y que nos permita hacer piña y ver lo que está sucediendo en el mercado", recuerda.

El director técnico recomienda a la comunidad preventa que no se estanque: que siga aprendiendo y formándose en todas las tecnologías que vayan surgiendo, lo que les "va a ayudar en su trabajo en el día a día".

Jaime Balañá, director técnico de NetApp