V-Valley Cybersecurity Summit: la ciberseguridad en primera línea de negocio

V-Valley celebraba en abril la tercera edición de su Congreso Anual de Ciberseguridad, V-Valley Cybersecurity Summit, en La Granja de San Ildefonso, en Segovia. El mayorista congregaba a los responsables de todos los fabricantes que componen su división de ciberseguridad para compartir con los *partners* su estrategia y sus principales focos de actuación para 2024. Como novedad, este año participaban también los fabricantes de la oferta de Lidera, así como sus clientes, creando una sinergia perfecta bajo el tándem V-Valley–Lidera.

Rosalía Arroyo

Durante dos días se compartieron charlas y networking, un encuentro que arrancó con un debate liderado por el periodista José Yélamo, quien replicó el programa de televisión que presenta, La Sexta Xplica, en el Centro de Congresos y Convenciones de El Parador de La Granja. Un debate en el que se habló de Zero Trust, del reto del *ransomware*, la inseguridad de la seguridad móvil o la evolución de SASE.

Se planteaba al inicio de la charla el problema que existe en el sector tecnológico, en general, y en el de la ciberseguridad, en particular, de la falta de profesionales. Según datos de INCIBE, hay 80.000 vacantes no cubiertas. En opinión de Enrico Dellù, *sales manager* de RedCarbon, hace falta que se ponga foco en las escuelas para buscar una solución en el medio y largo plazo, y que ahora puede afrontarse "utilizando herramientas de inteligencia artificial capaces de automatizar tareas masivas y redundantes", y que permitan acelerar el proceso. Intervenía David Gasca, *sales & marketing manager cybersecurity* en V-Valley, para apuntar que el canal de distribución suple esa falta de profesionales a través de los servicios que se ofrecen: "No podemos pretender que todas las empresas cuenten con un equipo de expertos en ciberseguridad. Son los integradores los que tienen que dar esa capa de servicios".

La inteligencia artificial, a debate

La inteligencia artificial generativa, que tiene el potencial de revolucionar la ciberseguri-

> "Lo que todos los clientes buscan con la nube es que su negocio esté disponible 24x7 de una forma global y distribuida"
>
> **Juan Asensio, *country manager* de A10**

dad, pero que también puede ser utilizada por los ciberdelincuentes para crear nuevas amenazas, ocupaba el primer bloque de debate del evento. Asegurando que es un arma de doble filo, comentaba Ricardo de Ena, *area sales manager north Spain* de WatchGuard, que mientras que los ciberdelincuentes "la están utilizando en nuestra contra, nosotros también utilizamos nuestras propias herramientas de inteligencia artificial para contener esos ataques".

Intervenía Nicolò Rossi, *account manager Iberia* de BlackBerry, para recordar que los ciberdelincuentes ya están utilizando la IA para atacar y que ya se han visto muestras de *ransomware* generadas por inteligencia artificial generativa. Hay que diferenciar entre la IA generativa, "que puede ayudar, sobre todo en la interfaz entre el usuario, el administrador y la tecnología", y la inteligencia artificial predictiva, "más importante porque las amenazas hay que pararlas antes de que lleguen".

Asegurando que las empresas necesitan tener una comprensión profunda de su infraestructura de TI para operar de manera eficiente y segura, planteaba José Yélamo que, siendo la visibilidad el primer paso, la observabilidad es el siguiente nivel. Rocío

> "El dato en sí, dónde está y quién lo tiene es lo más importante en todas las empresas"
>
> **Alberto Tejero, CEO de Arexdata**

> "En relación al *backup*, hay que poner foco en las configuraciones de los dispositivos críticos por los que pasa toda la información, como los *firewalls*, los *switches* o los *routers*"
>
> **Eduard Alegre, responsable de la unidad de negocio Backbox - V-Valley | Lidera**

Vaquero, *partner business manager* de Armis, dejaba claro que la visibilidad es necesaria y que debe ser unificada en base a una plataforma que permita tener visibilidad de todos los activos, no solo porque mejora la seguridad, también la toma de decisiones. "La estrategia de ciberseguridad completa de una empresa tiene su base a partir de la visibilidad de lo que se tiene", aseguraba.

> "Un ataque de *ransomware* no solo supone el secuestro de la información, sino que la información se fuga y te extorsionan con ello"
>
> **Víctor Molina, *security engineering team leader* de Check Point Software**

Para Alberto Algarra, *channel manager* de Ivanti, uno de los retos de la visibilidad es mantener el inventario de activos al día en entornos cada vez más complejos y con redes que están vivas. "Debemos entender cómo está interconectado todo el ecosistema para poder saber cómo puede afectar un ataque", aseguraba, añadiendo que hay que apostar por plataformas unificadas que sepan sacar partido de la inteligencia artificial para automatizar muchos procesos; "eso va a ser el futuro".

Zero Trust

Ponía sobre la mesa José Yélamo el concepto de Confianza Cero o Zero Trust, que se basa en la idea de que, por defecto, ningún usuario o dispositivo es de confianza y exige verificar la identidad y el acceso a los recursos de forma continua, independientemente de la ubicación del usuario o del dispositivo.

Para Juan González, *enterprise account executive* de Invicti, el concepto de Confianza Cero es una buena iniciativa que debería implementarse en todo momento, "pero también hay que tener mucha cautela en cómo se maneja".

En opinión de Juan Molina, senior *partner solutions engineer* de Cloudflare, poner en práctica el concepto de Zero Trust es fácil desde el punto de vista técnico, "pero vender ese concepto es la parte en la que todos estamos trabajando" porque supone un cambio radical respecto el modelo estándar de seguridad perimetral. La Confianza Cero, aseguraba, "exige concienciar de que hay que pasar de un mundo a otro".

Dentro de ese modelo de Zero Trust y validación continua, apuntaba Juan Pedro Martínez, *enterprise account executive* de Red Sift, hacia el mundo de los protocolos. Mencionaba concretamente DMARC, un mecanismo de autenticación de correo electrónico que evita la suplantación de identidad en el correo electrónico. "Utilizar por defecto este protocolo, que ya está en el mercado, cumple con el modelo de confianza cero".

"La pandemia influyó enormemente en la importancia que tiene Zero Trust", decía Sergio Martínez, *country manager* de SonicWall. Los despliegues de VPN durante la pandemia, que permiten "acceder al cora-

> "El problema real es que la gran mayoría de empresas ni tiene tiempo, ni recursos, ni dinero, ni gente"
>
> **Albert Barnwell, *sales director* Iberia de CyberArk**

zón de todas las empresas", generaron una gran cantidad de ataques a los que puede hacerse frente permitiendo que "cada uno pueda acceder a lo que le toca y nada más", comentaba el directivo. "Aún queda muchísimo por hacer".

En opinión de Javier Barandiaran, p*artner & alliance manager* de Opentext, los usuarios sí que están concienciados con Zero Trust, y no son proyectos complicados, pero "es la parte de autenticación de usuario donde queda más por hacer".

"Al final Zero Trust tiene que estar implementado en todo, desde la red a la identidad, o los procesos que se ejecutan en una máquina", aseguraba durante su intervención Dámaso Ramos, responsable de servicios en Lidera Cloud|V-Valley, añadiendo que "hay concienciación de aplicar Zero Trust en el acceso a la red, pero falta la globalidad del concepto".

Apostaba Ana Martínez, *enterprise account executive* de SailPoint, por que sea el canal el que "enseñe a los clientes de una forma holística cómo hay que implementar Zero Trust y ayudarles a poner las piezas de todos nuestros mensajes en una única visión". Añadía que, si el cliente no tiene nadie que le ponga todo sobre la mesa, "no va a ser capaz de implementar esa estrategia".

> "Las empresas protegen los datos con cifrado, pero pocas se plantean qué se está haciendo con las claves de cifrado"
>
> **Rocío Martínez, *sales director* de Entrust**

Mencionaba Rocío Martínez, *sales director* de Entrust, que el término Zero Trust se ha utilizado tanto desde el punto de vista de marketing, "que está demasiado manido. Hay que ir a lo básico, como es la criptografía asociada a la identidad". Mencionaba la regulación como palanca de apoyo para la adopción de este tipo de modelos.

"Los clientes no nos entienden cuando hablamos de Zero Trust", aseguraba Raúl Guillén, director de estrategia de ciberseguridad de Trend Micro. "Hay que medir el riesgo tecnológico, colocarlo al nivel del riesgo de negocio y hablar el lenguaje que los clientes entiendan". Aseguraba que hay que acercarse a las necesidades de negocio usando la tecnología. "Si seguimos hablando con conceptos tan técnicos estamos perdiendo la ventana de elevar el lenguaje de la ciberseguridad a la alta dirección".

> "Los dispositivos móviles tienen tanto o más peligro que cualquier otro dispositivo que está dentro de la red"
>
> **Alberto Algarra, *channel manager* de Ivanti**

Formación y concienciación del usuario

Salían a relucir durante el debate temas relativos a la formación y concienciación al empleado, considerado desde hace años como el eslabón más débil de la cadena de la ciberseguridad. Comentaba Juan Pedro Martínez que es habitual cargar la responsabilidad en que el empleado siempre está pinchando en el *phishing* malicioso pero a veces cuando todo apunta a que el *email* que se ha recibido es del jefe, "parece inevitable que no se pinche". Apuntaba David Gasca que ahora, con la expansión de la inteligencia artificial, el *email* de *phishing* podría estar mejor escrito que el del CEO de la compañía, añadiendo, entre risas, que "a lo mejor, hasta sabe más que él".

> "Toda la estrategia de ciberseguridad tiene su base a partir de la visibilidad de lo que se tiene"
>
> **Rocio Vaquero, *partner business manager* de Armis**

Durante su intervención, Mar Sánchez, *country manager* de Cyber Guru, coincidía en que los ataques son cada vez más sofisticados gracias, en parte, a la IA y advertía que los falsos mensajes ya no tienen que ser escritos; "ahora te pueden llamar por teléfono y te pueden clonar la voz. Y esto, que parece de película, son cosas que están ocurriendo", añadiendo que ahora es mucho más difícil identificar este intento de fraude.

"Sigo rompiendo una lanza por el pobre usuario al que le echamos la culpa de que siempre pincha en el *phishing*", decía Juan Pedro Martínez asegurando que existen muchas compañías "que siguen sin aplicar unos mínimos pro-

tocolos para evitar un tipo de *phishing* muy específico, que es el de suplantación".

Ransomware

Llegaba el momento de hablar de *ransomware*, una de las principales ciberamenazas a nivel mundial. Hablar de *ransomware* es hablar de secuestro de datos, decía José Yélamo, preguntando a los participantes del debate por las tendencias de un problema que afecta a todo tipo de empresas y al que "todos estamos expuestos". David Baldomero, *senior systems engineer* de Trellix, tomaba la palabra para comentar que sí, que el secuestro de datos es un gran problema. En su opinión, "la seguridad debería orientarse hacia la protección de la información, pero es un reto complejo que todavía no está siendo abordado lo suficientemente bien por parte de todas las empresas". Planteaba que todo está conectado "y que la parte de control de datos tiene mucho que ver con la prevención de amenazas".

> "La seguridad de los datos es un problema muy serio. Al final, todos somos un poco Diógenes"
>
> **Dámaso Ramos, responsable de servicios en Lidera Cloud | V-Valley**

> "En Zero Trust es en la autenticación del usuario donde queda más por hacer"
>
> **Javier Barandiaran, *partner & alliance manager* de OpenText**

Frente a un ataque de *ransomware*, lo primero que hay que hacer es poner en marcha las contramedidas, decía Víctor Molina, *security engineering team leader* de Check Point Software. Mencionaba no solo medidas de mitigación, sino de recuperación y, por supuesto, no pagar nunca el rescate. Recordaba que un ataque de *ransomware* no solo supone el secuestro de la información, "sino que la información se fuga y te extorsionan con ello".

En opinión de Mar Sánchez, las estrategias de *backup* son importantes en un ataque de *ransomware*, así como contar con un buen plan de continuidad de negocio, "desarrollado y probado", y, sin ninguna duda, entrenar a los empleados para que sepan, en la medida de lo posible, "discernir un mensaje real de uno fraudulento".

Tenía claro Ricardo de Ena que hay que "seguir haciendo hincapié en la concienciación" porque todavía hay muchos CEO que siguen sin saber lo que es un ataque de *ransomwa-*

> "Las empresas necesitan conocer todos sus activos y sus interacciones con fabricantes y clientes"
>
> **Enrico Dellù, *sales manager* de RedCarbon**

> "SASE está empezando a implantarse con el objetivo de reducir la exposición y corregir la anomalía que se produjo en la pandemia con las VPN"
>
> **Sergio Martínez, *country manager* España y Portugal de SonicWall**

re, o porque hay planes de recuperación que no se han puesto en práctica.

Para José Antonio Morcillo, responsable de canal en Kaspersky Iberia, si bien las medidas de mitigación y restauración son importantes, "lo fundamental es la predicción" y contar con expertos que estén analizando cuáles son las tendencias y qué está ocurriendo, porque "si en la *dark web* estoy viendo que se está comerciando con credenciales de mi empresa, está clarísimo que voy a recibir un ataque".

Planteaba Raúl Guillén que la clave es medir el riesgo de forma global "y ser capaces de colaborar entre nosotros". Se mostraba de acuerdo Santiago Álvarez de Cienfuegos, *country manager Spain* de XM Cyber, en que hay que ver la situación de forma global porque, de otra forma, difícilmente vamos a ser capaces de medir el riesgo. "Tiene que haber una forma de transmitir cuál es mi postura con respecto a los posibles adversarios para dejar de pensar como un defensor y empezar a pensar como un atacante".

Recordaba Albert Barnwell, *sales director Iberia* de CyberArk, que "el problema real es que la gran mayoría de empresas ni tiene tiempo,

> "Los clientes no nos entienden cuando hablamos de Zero Trust"
>
> **Raúl Guillén, director de estrategia de ciberseguridad de Trend Micro**

ni tiene recursos, ni tiene dinero, ni tiene gente". No todas las empresas son iguales y, por tanto, "no les podemos dar a todos la misma medicina porque no les servirá".

Gestión de identidades y accesos

La gestión de identidades y accesos (IAM) es fundamental para la seguridad de cualquier organización ya que permite controlar quién tiene acceso a qué recursos y en qué momento y, sin embargo, "cuando vamos a los clientes y les hablamos de IAM no saben qué es la gestión de identidades", comentaba Ana Martínez.

A la hora de hablar de gestión de identidades y accesos, propone Rocío Martínez ir a lo básico: ¿cómo dotas a un usuario de una identidad digital? ¿Cómo chequeas que esa persona realmente es quien dice ser?

Durante su intervención comentaba Albert Barnwell que, cuando hablamos de accesos, no sólo hablamos de personas, sino que podemos hablar de inteligencias artificiales, de automatismos, de aplicaciones...; que el robo de las credenciales continúa siendo una de las mayores problemáticas de seguridad; que cada persona, en cualquier momento,

> "Hay que diferenciar entre la IA generativa y la inteligencia artificial predictiva, más importante, porque las amenazas hay que pararlas antes de que lleguen"
>
> **Nicolò Rossi *account manager Iberia* de BlackBerry**

> "Ahora es mucho más difícil identificar un intento de fraude"
>
> **Mar Sánchez, *country manager* de Cyber Guru**

puede tener una elevación de privilegios; y que hay que plantear que cada usuario tenga el mínimo privilegio para poder hacer lo que tenga que hacer en ese momento.

Hablando de identidades y accesos planteaba Ricardo de Ena la necesidad de contar con un gestor de identidad para ayudar con las contraseñas.

Backup y SASE

El *backup*, la copia de seguridad, ha sido, tradicionalmente, un asunto a tratar por los equipos de sistemas. Sin embargo, el discurso de la copia, de la recuperación y, en definitiva, de la continuidad de negocio, se está trasladando al terreno de la cibersegu-

> "Hay que dejar pensar como un defensor y empezar a hacerlo como un atacante"
>
> **Santiago Álvarez de Cienfuegos, *country manager Spain* de XM Cyber**

ridad poco a poco. Para Eduard Alegre, responsable de Backbox dentro de V-Valley|Lidera, el *backup*, entendido como copia de seguridad de los datos de las estaciones de trabajo o de los servidores, es algo que se lleva mucho tiempo empleando. Pidió que se ponga foco en la copia de seguridad de aquellas configuraciones de los dispositivos críticos por los que pasa toda la información de las empresas, como los *firewalls*, los *switches* o los *routers*, "que son el eslabón olvidado".

Durante su intervención, aseguraba Marcus H. Gregory, *Iberia sales manager* de Acronis, que las teorías que había en torno a las copias de seguridad son totalmente aplicables y que lo que cambia es "el tipo de dato y la ubicación del mismo", elementos que deben tenerse en cuenta para realizar recuperaciones de manera correcta y con un tiempo adecuado.

SASE (Secure Access Service Edge) también contó con su parcela de protagonismo. Una tecnología que, en opinión de Sergio Martínez, está empezando a implantarse con el objetivo de "reducir la exposición y corregir la anomalía que se produjo en la pandemia con las VPN".

Recordando que los responsables de ciberseguridad se enfrentan a entornos cada vez más complejos, comentaba Víctor Molina que la clave de SASE, que busca unificar herramientas de red y seguridad, "está en poder darlo todo de una forma unificada" porque hay que reducir la complejidad y simplificar la administración.

Nicolò Rossi recordaba que SASE se extendió después de la pandemia, cuando la necesidad de teletrabajo incrementó la superficie

> "Un error de configuración también es una vulnerabilidad. Y no es parcheable"
>
> **Juan Pedro Martínez, *enterprise account executive* de Red Sift**

de ataque, dificultando, no solo el control y la visibilidad de los activos, sino de los accesos de los usuarios a las aplicaciones.

Dejaba claro Alberto Tejero, CEO de Arexdata, que "el dato en sí, dónde está y quién lo tiene, es lo más importante en todas las empresas". Mencionaba que aún es más relevante saber qué dato hay que proteger, saber quién es el que lo mueve y de qué manera se mueve.

Entornos híbridos y *multicloud*

Lo que el debate dejó claro es que los entornos híbridos y *multicloud* son cada vez

más comunes en las empresas. Estos entornos combinan infraestructura local, pública y de varios proveedores de nube, lo que crea una superficie de ataque más compleja y aumenta los riesgos de seguridad. Planteaba José Yélamo cuáles son los principales retos de seguridad de estos entornos o cómo afrontar la seguridad de los mismos.

Decía Juan Asensio, *country manager* de A10 Networks, que la nube es una realidad desde hace unos años y que, al final, lo que todos los clientes buscan utilizándola "es que su negocio esté disponible 24x7 de una forma global y distribuida".

Asegurando que hay muchos productos para proteger en estos entornos híbridos y *multicloud*, decía David Baldomero que el problema fundamental es que "la seguridad se ha hecho tan compleja que es muy difícil, incluso con consolas unificadas con asistentes o con inteligencia artificial, que los propios clientes puedan gestionar la seguridad adecuadamente". Apostaba por que los clientes se apoyen en *partners* e integradores "capaces de darles un servicio que les dé valor".

> "En los entornos de *backup* lo que cambia es el tipo de dato y su ubicación"
>
> **Marcus H Gregory, *Iberia sales manager* de Acronis**

En opinión de Raúl Guillén hay que ir más allá e "intentar concienciar a los clientes de que hay que incorporar ciberseguridad en fase de diseño". Aseguraba que la seguridad en la nube no es tanto un problema tecnológico como "un problema en el modelo de diseño de los servicios y los productos".

> "La Confianza Cero es una buena iniciativa que debería implementarse en todo momento, pero hay que tener mucha cautela en cómo se maneja"
>
> **Juan González, *enterprise account executive* de Invicti**

La cadena de suministro

Trajo al debate José Yélamo la seguridad, o inseguridad, de la cadena de suministro, un ecosistema complejo que involucra a múltiples actores, como proveedores, fabricantes, distribuidores y clientes. Cada uno de estos actores tiene sus propios sistemas informáticos y procesos, lo que crea una superficie de ataque amplia y vulnerable a los ciberataques. ¿Es posible evaluar el riesgo de seguridad de la cadena de suministro? Respondía Enrico Dellù, poniendo sobre la mesa dos aspectos. Por un lado, la visibilidad, porque "las empresas necesitan conocer todos sus activos, así como sus interacciones con fabricantes y clientes"; y el segundo, la responsabilidad, sobre la que comentaba que, sabiendo que puede producirse un ataque, "debe contarse con la ayuda de *partners* competentes".

En tanto en cuanto todos los sistemas se hablan con todos los sistemas a través de API, "hay que tener una solución para protegerlas, para que el mensaje que sale de un sistema llegue a otro sin estar corrupto", comentaba Juan Molina.

> "Hay que tener una solución para proteger las API, para que el mensaje que sale de un sistema llegue a otro sin estar corrupto"
>
> **Juan Molina, *senior partner solutions engineer* de Cloudflare**

> "Cuando vamos a los clientes y les hablamos de IAM no saben qué es la gestión de identidades"
>
> **Ana Martínez, *enterprise account executive* de Sailpoint**

Coincidió Rocío Vaquero con Enrico Dellù sobre la importancia de la visibilidad para proteger la cadena de suministro y saber no solo "dónde están esos dispositivos, quién los tiene y con quién se están comunicando"; también hay que priorizar los dispositivos más críticos "para desplegar una estrategia de ciberseguridad adaptable a cada negocio".

Apuntaba Santiago Álvarez de Cienfuegos que, a la hora de determinar la seguridad de la cadena de suministro, no todo queda en el plano de sistemas y que no hay que olvidar que "el comportamiento del usuario también es un riesgo per se". Añadía que las vulnerabilidades son infinitas pero que no hay que

confundir vulnerabilidad con riesgo: "No todas las vulnerabilidades suponen un riesgo. De hecho, estadísticamente solo el 2 % de las vulnerabilidades son explotables en entornos determinados".

El dato, el rey

En la era digital, los datos se han convertido en un activo esencial para las empresas. La capacidad de encontrar, analizar y protegerlos es fundamental para el éxito en el mercado actual.

Aseguraba José Yélamo que vivimos en la era del dato, que se ha convertido en un activo esencial para las empresas. A la hora de explicar por qué es tan importante proteger bien los datos de una empresa decía Alberto Tejero que, antes de protegerlo, las empresas tienen que saber qué tienen y dónde está. Asegura también que, en muchos casos, las empresas no saben qué información tienen, cómo se mueve o quién accede a ella.

> "El canal de distribución suple la falta de profesionales a través de los servicios que se ofrecen"
>
> **David Gasca, *sales & marketing manager cybersecurity* en V-Valley**

Apuntaba Rocío Martínez que muchas veces las empresas protegen los datos con cifrado, pero que pocas se plantean qué se está haciendo con las claves de cifrado, que también deben estar convenientemente protegidas.

Javier Barandiaran recordaba que hace tiempo que existen tecnologías de cifrado para proteger los datos, y que incluso ya se han definido y diseñado los cifrados *post quantum*. El reto, aseguraba, es que sigue habiendo mucho *legacy*, donde la tarea de proteger los datos estructurados y no estructurados es muy compleja. "No son proyectos fáciles de acometer", decía.

> "Hay que seguir haciendo hincapié en la concienciación"
>
> **Ricardo de Ena, *area sales manager* de WatchGuard**

Para Dámaso Ramos el punto clave de la ciberseguridad empresarial son los datos y su seguridad "es un problema muy serio en la mayoría de las compañías porque al final todos somos un poco Diógenes".

Recordó Nicolò Rossi que muchas veces el cliente no sabe que ha sido robado y gran parte de los datos que son robados acaban en la *darkweb*. "Cada vez son más las empresas que están desarrollando soluciones que analizan y monitorizan esta red oscura".

Gestión de vulnerabilidades

La gestión de vulnerabilidades es un proceso continuo que se encarga de identificar, evaluar y corregir las vulnerabilidades en los

> "La seguridad debería orientarse hacia la protección de la información"
>
> **David Baldomero, *senior systems engineer* de Trellix**

sistemas informáticos de una empresa. Este proceso, fundamental para proteger la empresa, se ha convertido en un auténtico quebradero de cabeza para los responsables de TI y ciberseguridad de las empresas.

Sobre la gestión de vulnerabilidades, comentaba Santiago Álvarez de Cienfuegos que la clave es "cómo seleccionamos cuáles de esas vulnerabilidades son críticas o explotables dentro de mi entorno". Para ello, hay que colocarse en la visión del atacante para ver cuáles se pueden explotar y así, "hacer una priorización de las mismas".

Apostaba Raúl Guillén por el parcheado virtual, asegurando que una vulnerabilidad no sólo es un parche mal instalado, sino una mala configuración o entornos que están expuestos. "Está claro que el contexto y el nivel de criticidad define dónde tienes que poner el foco a la hora de actuar".

Apuntaba Juan González que uno de los desafíos más grandes en cuanto a vulnerabilidades son los falsos positivos y que son las tecnologías las responsables "de contar con la capacidad de confirmar que esas vulnerabilidades están presentes".

Estaba de acuerdo Juan Pedro Martínez en que un error de configuración también es una vulnerabilidad. "Y no es parcheable". Aseguraba que se hace necesario contar con una solución que se encargue "de

> "Las medidas de mitigación y restauración son importantes pero lo fundamental es la predicción"
>
> **José Antonio Morcillo, responsable de canal en Kaspersky Iberia**

descubrir todo lo que tenemos expuesto y monitorizarlo desde el punto de vista de la configuración".

En opinión de José Antonio Morcillo el problema de las vulnerabilidades existe desde hace tiempo y el secreto está en la automatización, tanto a la hora de identificarlas como al establecer la criticidad y realizar un parcheo.

Siguiendo con el tema de las vulnerabilidades, ponía foco Javier Barandiaran en el desarrollo de código aportando un dato impactante: "El 80 % de lo que se está ejecutando no lo han desarrollado nuestros clientes. Son librerías de terceros y normalmente de alguien de *open source*".

Añadía Sergio Martinez que las vulnerabilidades tienen muchas caras "y en muchos casos son polimórficas"; y David Baldomero apuntaba la falsa sensación de seguridad como otro tipo de vulnerabilidad.

La movilidad segura

Pasó José Yélamo a hablar de la seguridad de la movilidad, un aspecto fundamental desde el momento en el que las empresas permiten a sus empleados utilizar dispositivos móviles para acceder a recursos corporativos.

Dejaba claro Alberto Algarra que, actualmente, quizás de toda la superficie de ataque de las compañías, una de las grandes olvidadas, o un mercado en el que todavía no hay madurez, es la protección del dispositivo móvil. Explicaba que cuando se accede a los datos corporativos desde el teléfono móvil existen varias posibilidades: "Si el móvil nos lo ha dado la compañía, teóricamente debería de tener ciertas medidas de seguridad, pero si nuestro móvil es el privado y accedemos al correo corporativo, podemos estar abriendo una puerta bastante grande desde la que pueden atacar a la seguridad de nuestra

compañía". Añadía que las compañías deben tener claro que "los dispositivos móviles tienen tanto o más peligro que cualquier otro dispositivo que está dentro de su red".

En opinión de José Antonio Morcillo "los dispositivos móviles están completamente olvidados". Aportaba un dato contundente: en 2023 los ataques a dispositivos móviles aumentaron un 52 % y añadía que, además de no prestar demasiado interés, "se tiene la falsa creencia de que los que realmente son vulnerables son los dispositivos Android, cuando realmente no es así".

En ocasiones se cree que un MDM, un administrador de dispositivos móviles, es una solución de seguridad, pero no lo es, aclaraba David Baldomero, añadiendo que "la manera de proteger un dispositivo móvil tiene que ser diferente".

Aunando dispositivos móviles y gestión de identidades, comentaba Rocío Martínez que debe hacerse un *device reputation*: "Chequear que esos dispositivos no tienen troyanos, no tienen vulnerabilidades que puedan afectar luego a la empresa e introducirlos en el ecosistema de una manera segura".

En su intervención comentaba Víctor Molina que hay dos temas a tener en cuenta en relación a la seguridad de la movilidad. Por un lado, proteger el propio dispositivo; y, por otro, proteger al propio usuario en el dispositivo, evitando que sea víctima de un SMS fraudulento, por ejemplo.

Finalizaba así un debate amplio, en el que se pusieron sobre la mesa más de una docena de temáticas de seguridad que están de plena actualidad.