Ciberseguridad:
oportunidad y exigencia para el canal

La ciberseguridad sigue siendo uno de los segmentos tecnológicos con más oportunidades para el canal. También, por su carácter crítico, el más exigente. Un área que fue la protagonista del Ingram Micro Cybersecurity Afterwork, un evento en el que el mayorista reunió a fabricantes y clientes para analizar el panorama y recordar retos y segmentos de oportunidad. Más de 100 profesionales se dieron cita en el Hotel Oscar Room Mate, en Madrid, para dejar claro que la ciberseguridad es punta de lanza en el canal. Marilés de Pedro

Identidad digital en Europa

Tras la apertura de Martín Trullás, director del área de Advanced Solutions de Ingram Micro, donde se integra el negocio de la ciberseguridad, Julián Inza, asesor de eFirma, eAdministración, eJusticia, Blockchain, identidad digital y proyectos y servicios, habló sobre el reglamento EIDAS2 y la cartera de identidad digital. Inza empezó recordando que Europa está publicando legislaciones relacionadas con la identidad y la privacidad que van a hacer que las "vidas de las grandes compañías, como Amazon, Facebook o Google, sean un poco más duras, exigiendo medidas especiales respecto a la privacidad".

Una de las grandes iniciativas está relacionada con la gestión de la identidad. Inza recordó que además de las herramientas tecnológicas encargadas de esta área, la identidad motiva corrientes políticas, activistas, que apelan a la identidad autosoberana. "Debemos ponernos de acuerdo acerca de qué es la identidad", señaló. Inza señaló los tres elementos de los que se compone: la identificación, la autenticación y la acreditación.

"El perímetro se identifica con la persona, teniendo que acceder a una serie de servicios y acompañado de una serie de privilegios"

La identidad, recordó, nace desde el momento en el que las personas nos registramos en el registro civil, habiéndose constituido en "un derecho humano". Una gestión de la identidad que ejercemos gracias a los instrumentos que el Estado nos facilita. "En España disfrutamos, por ejemplo, del DNI, nuestra manera de demostrar la identidad, que no tienen otros países, como es el caso del Reino Unido o Estados Unidos, por ejemplo".

Desde 2014 en este contexto de la identidad se cuenta con el reglamento EIDAS, un proyecto para permitir el reconocimiento europeo de las identidades electrónicas. "Define un sistema para que los Estados comuniquen a la Comisión Europea los mecanismos de identidad digital que hubieran puesto a disposición de sus ciudadanos con la finalidad de que fueran utilizados de manera transfronteriza para que los ciudadanos europeos pudieran hacer gestiones en cualquier país de la Unión Europea".

Para ello se crearon nodos EIDAS en cada uno de los países que "no han funcionado porque las Administraciones Públicas solo se preocupan de la codificación de los números de identidad de sus nacionales, no de que los ciudadanos de otros países puedan hacer gestiones en todo el territorio europeo".

El 3 de junio de 2021 se publicó una propuesta para un nuevo reglamento EIDAS que anunciaba un nuevo *onboarding*, la manera en la que se registran las altas en un prestador de servicios de certificación, con diferentes vías. En esta propuesta, se incluye la vía para poder hacerlo a distancia, con mecanismos tan seguros como los presenciales, que se convierte en la opción prioritaria. "Va a cambiar la manera en la que los organismos oficiales expiden certificados de identificación". Entre los documentos de los que se compone se incluye una recomendación que crea un grupo de expertos para definir la arquitectura y el marco de referencia de la cartera IDUE (EUDI Wallet).

"La seguridad gestionada es panacea para el canal"

El pasado mes de junio se anunció que se había llegado a un acuerdo en los puntos más conflictivos de este reglamento EIDAS 2. Inza prevé que se aprobará definitivamente durante la actual presidencia española. "Posiblemente en septiembre u octubre".

El grupo de expertos ha trabajado en lo que se denomina Architecture and Reference Framework (ARF), que cuenta con una versión disponible desde el pasado mes de abril, que ya cuenta con casos de uso como el carnet de conducir móvil, que será una de las

primeras implementaciones que se harán de la cartera.

Los Estados proporcionarán la cartera IDUE, el elemento central, que previsiblemente será desarrollada en código abierto (se ha licitado y el adjudicatario ha sido una empresa sueca). "El usuario tiene la cartera y utilizará ciertos datos de identificación personal". Ahora, además, se incluyen nuevos servicios cualificados de confianza, como los testimonios electrónicos, y se distingue entre las partes informadas (consumidoras de información) y las informantes (fuentes auténticas). Una de las grandes modificaciones es que las primeras tienen que estar censadas por parte de los países miembros. "Cualquiera no puede pedir al usuario información. La *wallet* será quien determine quién puede hacerlo y quién no".

Se trata, en definitiva, de un camino hacia un marco europeo común de la identidad digital. "Va a ser obligatorio que los estados lo emitan, pero no que los ciudadanos lo usen.

El reto es que el usuario vea útil este EUDI *Wallet*. Aquí está la gran batalla".

El "nuevo" perímetro

El evento contó con un debate, "Identidades, *endpoint* y *cloud*, o el nuevo perímetro de seguridad", en el que se habló de los nuevos retos surgidos en torno a esta realidad. Juan Denia, responsable de canal de Delinea, identificó al usuario como el elemento donde se ubica el actual perímetro. "Es esencial identificarnos: va a haber una fase de autenticación y otra de acreditación para determinar a qué se va a poder acceder. El perímetro se identifica con la persona, teniendo que acceder a una serie de servicios y acompañado de una serie de privilegios".

Sergio Martínez, director general de Sonicwall en España y Portugal, recordó que la mayoría de los ataques actuales comienza

con un robo de identidades. "Después suceden movimientos laterales, robo de identidades privilegiadas y, como último incidente, desactivan consolas, por ejemplo, de gestión de *endpoints* o de *backup*, para poder encriptar todo y difundir el *ransomware*, diseñando toda la estafa".

Se pinta, por tanto, una nueva realidad, mucho más compleja. "Antes el centro de datos marcaba el perímetro, que quedaba circunscrito al ámbito de la oficina", explica Ángel de la Encarnación, ingeniero de sistemas de HPE Aruba. "Muchas soluciones y aplicaciones han ido a la nube, lo que ha transformado la forma de trabajar e, incluso, de manejar los datos". El perímetro ha cambiado, lo que ha provocado que contemos con más puntos ciegos. "Es esencial que las empresas disfruten de una visibilidad para observar qué sucede en la red".

Carlos Galdón, director de canal de Sophos, señala que esta nueva realidad ha trasladado la responsabilidad al usuario. "El perímetro señala la protección de los recursos de la compañía". Un usuario que es un elemento más, que hay que proteger; pero "también todos los activos que forman parte de la empresa".

Un nuevo perímetro que señala nuevos desafíos para el canal. "El mayor reto es que se adecúe a la velocidad del cambio", apunta Galdón. "La evolución se hace a una velocidad tremenda: cada vez hay mayores desarrollos tecnológicos por parte de los fabricantes, lo que complica que el canal esté al día de todos ellos". La formación, recuerda, también es esencial.

Los *hackers* siempre van un paso por delante, con el uso de la inteligencia artificial para atacar las infraestructuras. "El *malware* se aloja en la nube y utiliza plataformas a las que el usuario accede de manera cotidiana, como OneDrive, para lanzar sus ataques", re-

cuerda Ángel de la Encarnación. "Su tráfico transita a través del tráfico que utilizamos", concluye. El reto es analizar este tráfico que va a la nube. "Es esencial para poder armar una buena protección".

Sergio Martínez recuerda que el tráfico encriptado supone el 70 % del tráfico total y la mayor parte de los *firewalls* y de los dispositivos de ciberseguridad no lo inspeccionan por la complejidad que implica. "Es una autopista para la entrada de todo tipo de *malware*", señala. "Más con el trabajo remoto". Junto a él, la mayor preocupación de los CIO es el *ransomware*.

En el informe anual de amenazas que lleva a cabo SonicWall, casi el 70 % de los CIO entrevistados creía que el panorama iba a ir a peor, con los ataques a los dispositivos IoT, que han crecido un 90 %, como el área con mayor crecimiento.

Juan Denia señala que ante este complejo panorama, con una mayor exposición de ataque, el canal debe encontrar elementos

comunes que permitan una protección mayor. "El canal necesita proponer servicios de valor a las empresas para ayudarlas a mejorar la seguridad". Denia no olvida señalar la especial protección de áreas claves como, por ejemplo, las credenciales con privilegio (*Privileged Access Management*), lo que limita el daño de la mayoría de los ataques que se producen en la organización.

El canal habita, como las empresas, en una realidad polimórfica, donde el acceso a los datos se lleva a cabo desde más dispositivos. "El canal es la pieza clave", recuerda Sergio Martínez. "Es el departamento de ciberseguridad de las pymes, que no cuentan con profesionales específicos para gestionar su seguridad". Cualquiera que sea el entorno en el que se ubiquen los datos, son las empresas quienes los atesoran, siendo las responsables de su gestión. "El canal tiene que ges-

tionar estos entornos", insiste el responsable de Sonicwall. "El canal tiene que estructurar los planes de seguridad de las compañías, pensando que en algún momento va a haber algún incidente".

Servicios gestionados

El despliegue de servicios gestionados marca el futuro, y el presente, del canal.

Calcula IDC que el 25 % de la inversión en materia de seguridad ya se canaliza a través de un modelo de servicio gestionado. "Es la panacea para el canal que tiene la capacidad de gestionar desde cualquier lugar la ciberseguridad, con una capacidad de llegada a los clientes que antes no tenía", razona Carlos Galdón.

Para Ángel de la Encarnación el ecosistema de *partners* aporta el valor añadido, complemento a las soluciones. "Es esencial también su labor de integración entre los diferentes fabricantes y la posibilidad de negocio que se le abre con el *upselling*".

> "El tráfico encriptado es una autopista para la entrada de todo tipo de *malware*"

Aunque aún no es una fórmula extendida hasta el último rincón del ecosistema, Sergio Martínez asegura que los distribuidores están empezando a adaptarse a este nuevo entorno, promovido por la oferta de los fabricantes, que se ha adaptado a esta fórmula, y también por la falta de talento y por la compleja situación a la que deben enfrentarse las empresas. "La única respuesta de cualquier organización es construir una defensa por capas, que exige visibilidad y control de lo que está sucediendo en la organización y en la infraestructura", insiste. A su juicio, queda mucho camino por recorrer en el terreno de la interoperabilidad. "Además de la necesaria conexión a múltiples sensores para recoger y tratar los datos, hay que identificar los indicios que señalan un ataque. Sin una inteligencia artificial que lo gestione es prácticamente una labor titánica saber qué está pasando".

Es esencial que el canal construya un catálogo de servicios gestionados. "Es importante que el distribuidor o el proveedor de servicios esté alineado con las necesidades de las distintas organizaciones y extender esos catálogos para cubrirlas, permitiendo que la organización esté tranquila subcontratando esa capa de seguridad", completa Juan Denia. "Aunque las empresas cuenten con departamentos específicos para gestionar la seguridad es imposible abarcarlo todo, con lo cual contar con servicios profesionales reputados que consigan mejoras y eficiencias, es una herramienta que cualquier organización se tiene que plantear".

Enorme oportunidad

Según la consultora IDC, el mercado de la se-

guridad en España está mostrando este año un crecimiento respecto del año pasado del 9,2%, alcanzando los 2.130 millones de euros. Para 2026 podría superar la barrera de los 2.995 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito (9,9 %).

La oportunidad se extiende a todos los ámbitos. Ángel de la Encarnación señala la falta de madurez de las redes empresariales como una fuente de oportunidad para analizarlas y ver cuál es la mejor configuración. Además, a su juicio, el negocio va más allá de la nube. "También es importante observar quién, cómo y de qué manera accede, en cualquier campus".

Galdón insiste en la seguridad como servicio. "Para un *partner* un servicio como MDR es un catalizador de sus ventas". La seguridad, recuerda, es compleja. "Con un MDR el canal puede ofrecer a una pyme, que no cuenta con recursos suficientes para gestionarla, la misma capacidad de defensa de la que disfruta una gran compañía".

La protección de la red sigue siendo esencial. "El *firewall* sigue siendo el elemento central en la ciberdefensa de todas las compañías", recuerda Martínez. En la construcción de la defensa por capas, el *endpoint* es área esencial. "Es posible desplegar políticas desde el propio *firewall* y ayudar en la gestión de los certificados, por ejemplo, para poder descifrar el tráfico encriptado".

Juan Denia defiende la enorme oportunidad que exhibe el área de la gestión de identidades; un sector que crece por encima del 20 %, un baremo superior al que marca el mercado de la seguridad. "Hemos detectado que hay una falta de madurez importante en el ámbito de la seguridad de la identidad. Hay muchas compañías que aún no tienen sistemas para gestionar sus cuentas privilegiadas", explica. Unas cuentas, críticas, que

son atacadas y pueden provocar enormes daños en las empresas. "Tenemos que ser capaces de protegerlas y dotar a los usuarios de los procedimientos adecuados para una eficaz protección".

> "Es esencial que las empresas disfruten de una visibilidad para observar qué sucede en la red"

Seguridad en la nube

También se celebró una mesa dedicada a la seguridad en la nube en la que se debatió acerca de los retos en este entorno, quién tiene la responsabilidad de la gestión y de la protección de los datos; la soberanía, la madurez que presentan las empresas españolas en este terreno o los riesgos a los que se enfrentan las empresas.

Javier Soto, *distributor account manager* de Acronis, se refirió a los riesgos reputacionales a los que se enfrentan las empresas en este ámbito. "Es clave llevar a cabo una monitorización constante de la red, con alertas tempranas, siendo proactivos", señaló. "Hay que construir una resiliencia". El responsable apeló al *disaster recovery* como un área esencial, con aplicaciones críticas para las empresas, "que hay que trasladar a la pyme".

En este entorno de la nube, maduro en la adopción de las empresas españolas, los riesgos, identificó Antonio Anchustegui, *channel manager* de Barracuda, tienen que ver con la gestión y la suplantación de las identidades. "Hay que introducir la nube en la estrategia general de seguridad de las compañías".

Pau Canales, responsable de canal de HornetSecurity, recordó que la seguridad, en un entorno *cloud*, es constante. "La actualización es continua y la empresa disfruta de la redundancia en diferentes localizaciones. Un modelo *cloud* es el adecuado para la seguridad de las empresas". En relación a los datos, Canales recordó que el usuario es el responsable de los datos y de su movimiento. "Debe ser consciente de la seguridad, por lo que la concienciación es esencial".

Ángel Ortiz recordó que si la transformación digital es *cloud*, la ciberseguridad también debe serlo. "Debe estar pegada a ella". El responsable de seguridad de Cisco abogó por las plataformas únicas y abiertas, transversales a los grandes proveedores *cloud*, donde "converjan las funciones de conectividad y las funciones de seguridad; y que simplifiquen su gestión".

Carlos Manchado, responsable de seguridad, *compliance* e identidad de Microsoft, recordó que dependiendo del sabor de la nube (IaaS, Paas o Saas), el enfoque de la seguridad es diferente, con más o menos complejidad. "Hay soluciones para mitigar todos los riesgos".