FORO TAI
grupotai

Revista digital

FORO TAI

CIBERSEGURIDAD TIC

- Conoce a los patrocinadores
- Descubre todo el contenido
- Accede a los vídeos
- Todo a un *click*

Blindando el Futuro Digital en un Mundo Interconectado

Allied Telesis™ · Cyber Guru · SOPHOS · yubico

IR A PÁGINA SIGUIENTE

Blindando el Futuro Digital en un Mundo Interconectado

Dirigido a responsables de TI y ciberseguridad, Foro TAI se trasladó a Málaga para celebrar el que ha sido su cuarto encuentro para saber qué preocupa a los responsables tecnológicos de las empresas y analizar qué necesitan, sabiendo que garantizar la ciberseguridad se ha convertido en un objetivo primordial.

Rosalía Arroyo

A medida que la tecnología evoluciona, también lo hacen las tendencias de ciberseguridad, y las filtraciones y los ciberataques se vuelven cada vez más comunes. Antes de dar paso al debate poníamos sobre la mesa las tendencias de un mercado que no para de evolucionar, tanto en defensa como en ataque. La inteligencia artificial, el aprendizaje automático y el Internet de las Cosas (IoT) están redefiniendo el panorama de la ciberseguridad. Los atacantes aprovechan

estas tecnologías para desarrollar ataques más sofisticados y personalizados, mientras que las empresas buscan soluciones proactivas para proteger sus activos digitales. El ransomware, los ataques de phishing y las amenazas internas siguen siendo una preocupación constante, pero ahora se ven agravados por la creciente complejidad de los entornos tecnológicos.

El debate reunía a una serie de fabricantes, empezando por Mar Sánchez, responsable de Cyber Guru en la región de Iberia, que dejó clara la importancia de la formación continua en ciberseguridad para todos los empleados; Fabio Cichero, Sales Manager Southern Europe de Yubico, empresa experta en soluciones de autenticación diseñadas para proteger los datos sensibles de las organizaciones; Álvaro Fernández, Sales Manager de Sophos Iberia, empresas relevante en el mercado de ciberseguridad con amplia experiencia en las ciberamenazas que enfrentan las empresas de diferentes tamaños; y Luis González Encuentra, responsables de Allied Telesis en Iberia, compañía experta en asegurar las redes industriales y proteger la continuidad de las operaciones.

> NIS2 es un marco normativo fundamental para garantizar la seguridad de las redes y los sistemas de información en la Unión Europea

Del lado de los clientes nos acompañaron en Foro TAI Málaga Ramón Freire, CTO de Pegasus Aero Group, una empresa que opera en el sector de la aviación ejecutiva; Juan García Galera, Responsable de Seguridad Información Delegado del CEMI (Centro Municipal de Informática) de Málaga, que se encarga de gestionar la seguridad de los sistemas informáticos que sustentan los servicios municipales; Jesús López del Peral, Responsable de Innovación TIC del Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina (IBIMA Plataforma BIONAND), que se configura como un espacio de investigación multidisciplinar en biomedicina y nanomedicina; Laura Guiance, Responsable de Ciberseguridad de Harvong Holding, una empresa dedicada a la adquisición, renta y remodelación de infraestructuras inmobiliarias; Jesús Valverde, CIO/CISO, Isemaren, empresa española especializada en ofrecer soluciones globales para la transición ecológica de empresas con foco en las energías renovables, especialmente en la energía fotovoltaica; Luis Pérez Pau, CISO, Ribera Salud, uno

de los grupos empresariales de gestión sanitaria más importantes de España fundado en 1997; Luis Márquez, Manager IT Andalucía de LHH/ LEE Hecht Harrison, compañía que se dedica a acompañar a personas y organizaciones en sus procesos de transformación, desarrollo del talento y gestión de carreras; y Enrique Cibantos, CTO de Ádivin Beach Flag, marca reconocida en el mercado de las banderas publicitarias, especialmente de las conocidas como fly banners o banderas de playa.

En Pegasus Aero Group se apuesta por el múltiple factor de autenticación “aderezado con acceso condicional y Bring Your Own Device gestionado”

Ramón Freire, CTO de **Pegasus Aero Group**

Autenticación

Durante el debate se trataron diferentes temas. Uno de los primeros en plantearse estuvo relacionado con el múltiple factor de autenticación, o MFA. La importancia de esta tecnología radica en la creciente necesidad de proteger los datos y sistemas digitales de las ciberamenazas. Al exigir múltiples formas de verificación, la MFA dificulta significativamente que los atacantes accedan a cuentas de forma no autorizada, incluso si obtienen una contraseña.

Se planteaba que, en términos de implementación y administración, ¿qué tipo de tecnología de MFA ofrecería la mejor combinación de seguridad, durabilidad y conveniencia en un entorno corporativo? Jesús Valverde, CIO y CISO de Isemaren, dejaba claro que “el segundo, o múltiple, factor de autenticación es necesario y hay que implementarlo”, y que debería haber una capa adicional de forma que no dependa únicamente de que se compruebe la identidad,

En concienciación se apuesta “por píldoras de sensibilización lo menos intrusivas posible que vayan calando en la conciencia de los usuarios”

Juan García Galera,
Responsable de Seguridad Información Delegado del **CEMI (Centro Municipal de Informática) de Málaga**

sino que también se compruebe el dispositivo y el contexto del usuario.

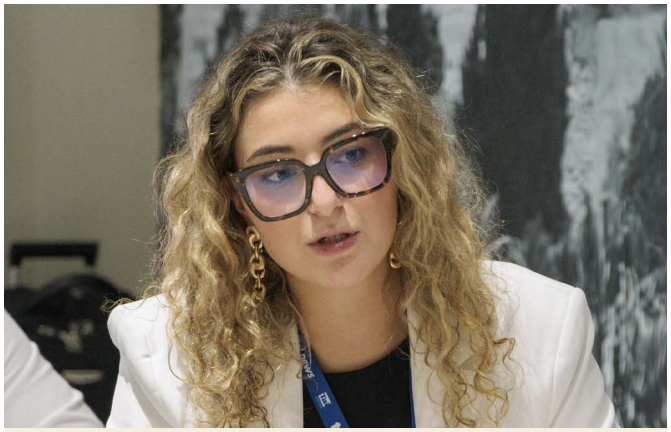
El MFA a través de tokens es una realidad en Harvong Holding, según contaba su responsable de ciberseguridad, Laura Guiance, durante el encuentro mantenido en Málaga. Aseguraba la directiva que es una tecnología cada vez más necesaria, sobre todo ahora que la inteligencia artificial es capaz de elaborar los phishing más sofisticados e incluso hacerse pasar por directivos para realizar delitos de fraude.

"En BIONAND preocupa el uso de Inteligencia Artificial en la investigación de los investigadores"

Jesús López del Peral,
Responsable de Innovación TIC del
Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina (IBIMA Plataforma BIONAND)

En Ribera Salud, donde también se apuesta por la autenticación desde hace años, se busca que el doble factor de autenticación "esté detrás de cualquier web o aplicación que sea accesible de manera pública o a gran número de usuarios, reduciendo también el riesgo al que exponemos nuestra base de empleados", comentaba Luis Pérez, CISO de la compañía, quien añadía que también se realiza un acceso condicional "para proporcionar una capa extra de seguridad".

Contaba Ramón Freire que en Pegasus Aero Group se apuesta por el múltiple factor de autenticación "aderezado con acceso condicional y Bring Your Own Device gestionado, por lo que puedo tener la tranquilidad de que, aunque te lleguen mil alertas, si tu móvil no está autorizado, no va a llegar a entrar al recurso corporativo". Se pedía a Fabio Cichero, responsable Yubico para el sur de Europa, que hiciera una valoración de lo mencionado. Puntualizaba que cuando se trata de un token de hardware, "creemos que la autenticación por aplicación es correcta,



"El MFA a través de tokens es una tecnología cada vez más necesaria, sobre todo ahora que la inteligencia artificial es capaz de elaborar los phishing más sofisticados"

Laura Guiance,
Responsable de Ciberseguridad de
Harvong Holding

pero tiene sus limitaciones", como en aquellos casos de uso donde no se puede utilizar un móvil, o donde no existe un móvil corporativo. Desde Yubico se apuesta por acercar al mercado un múltiple factor de autenticación resistente al phishing "y que se pueda utilizar en la mayor parte de casos de uso", comentaba el directivo, explicando que "en casos de uso de usuarios que tienen móvil corporativo, la aproximación es apostar más por la seguridad en sí de los protocolos que se utilizan".

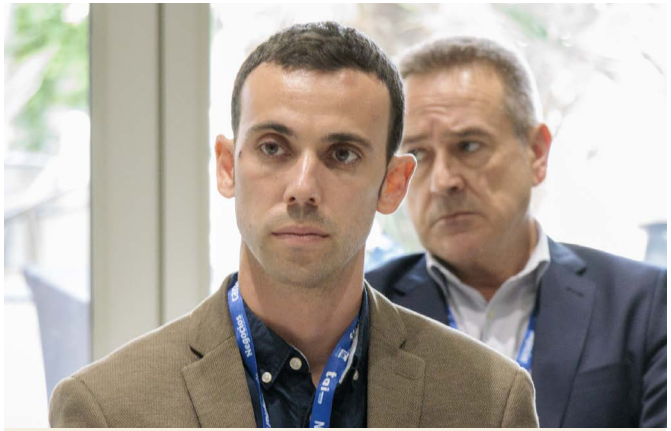
"Para aquellos que ya conocían la directiva NIS y tuvieron contacto con la Ley de Protección de Infraestructura Crítica, NIS2 es un refuerzo"

Jesús Valverde, CIO/CISO, **Isemaren**

Concienciación

La concienciación de los empleados en ciberseguridad se ha vuelto cada vez más importante. Siendo la primera línea de defensa contra las ciberamenazas, que los trabajadores estén capacitados para identificar y reportar posibles amenazas, permite que pueden prevenir incidentes de seguridad antes de que causen daños significativos. Por otra parte, muchos incidentes de ciberseguridad son causados por errores humanos, como hacer clic en enlaces sospechosos o compartir información confidencial. La concienciación ayuda a reducir la probabilidad de estos errores.

En Pegasus Aero Group lo tienen claro, y por eso se lanzan píldoras semanales. Explicaba Ramón Freire, CTO de la compañía que se apuesta por píldoras escuetas y recurrentes que se centran en el phishing, entre otras, que se completan con sesiones de formación de una hora máximo un par de veces al año con especialistas "donde

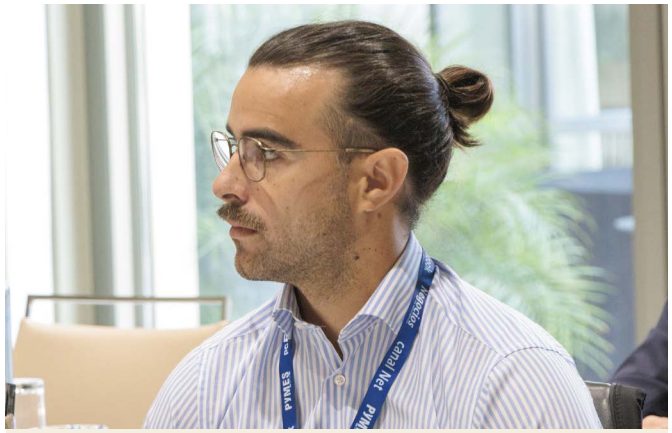


"Las certificaciones como la ISO27001 o el Esquema Nacional de Seguridad tendrán un papel a la hora de ayudar a demostrar el compromiso de cumplimiento de las empresas"

Luis Pérez Pau, CISO, **Ribera Salud**

no solo se habla de ciberseguridad en general, sino de la particularidad de nuestra empresa".

A la hora de medir los resultados de estas acciones, explicaba también Ramón Freire que, mientras que dos terceras partes de los empleados son ofimáticos, el otro tercio no lo es y



"Cada vez son más los CISO que solicitan ayuda de agencias para nutrir a las propias empresas del mejor talento"

Luis Márquez, Manager IT Andalucía de **LHH/ LEE Hecht Harrison**

que "ha costado mucha comunicación, mucha formación interna, que entendieran que no le íbamos a sacar las fotos de su dispositivo, que lo que se buscaba era la seguridad de la información y la privacidad de sus datos, y que además se le abrían un abanico de posibilidades enormes al poder acceder a un serie de aplicaciones corporativas que facilitan su día a día".

Experiencia similar aseguraba tener Enrique Cibantos, CTO de Adivin Beach Flag. La compañía, una fábrica de textiles y banderas, cuenta con una plantilla variada, donde hay desde tecnólogos hasta operarios base, y donde trasladar la importancia de la concienciación "a esa variada cantidad de perfiles es muy complejo".

A pesar de ello, se ofrece "una formación muy exhaustiva a nuestros empleados", comentaba Enrique Cibantos añadiendo que el mayor reto al que se enfrentan es "cómo le vamos a trasladar todo esto a nuestros empleados para que se sientan cómodos, y cómo le vamos a trasladar todo eso a la dirección para que no lo vean como un impacto negativo en el trabajo".

Preguntado por cómo se está abordando en el Centro Municipal de Informática de Málaga

"Hemos de ser muy proactivos a la hora de poner todas las herramientas posibles para prevenir problemas"

Enrique Cibantos, CTO de **Ádivin Beach Flag**

la formación y concienciación, explicaba Juan García, responsable de Seguridad de la Información del CEMI, que "lo tenemos bien separado". En concienciación se apuesta "por píldoras de sensibilización lo menos intrusivas posible que vayan calando en la conciencia de los usuarios",

y se apuesta por identificar el tipo de usuario, lo que lleva a enviar tres boletines mensuales a tres públicos objetivos diferentes, desde el usuario más básico, al que trasladamos nociones de qué es el phishing a otro boletín más técnico "donde se incluye información de las últimas vulnerabilidades". El tercer boletín, que Juan García Galera considera el más importante, está enfocado a la alta dirección "para concienciar de los riesgos del mundo digital". Explicaba que este último boletín recoge "todos los ataques que está sufriendo la administración pública mes a mes, de forma que, ese gota a gota vaya calando en la capa directiva y entiendan que todos estamos expuestos a un ciberataque".

Luis Márquez Pérez, Manager IT Division – Andalucía & Extremadura, de LHH Recuitment Solutions, aseguraba haber notado un aumento significativo de peticiones de perfiles cualificados y específicos en las diferentes áreas de la ciberseguridad; "cada vez son más los CISO que solicitan a los equipos de recursos humanos internos que cuenten con ayuda externa y especializada de agencias con expertos en selección de perfiles de ciberseguridad, con el objetivo de nutrir a las propias empresas del mejor talento", lo que ha llevado a la compañía a abrir nuevas sub-divisiones dentro de IT para la búsqueda de talento de Ciberseguridad.

"Nuestro objetivo es cambiar el comportamiento", aseguraba Mar Sánchez, responsable de Cyber Guru para la región de Iberia. La compañía, dedicada única y exclusivamente a la concienciación y formación a empleados, apuesta por tecnologías disruptivas para que, cuando el usuario cuando perciba una amenaza se comporte de una determinada manera. El más de millón de usuarios que acceden a la plataforma de la compañía en Italia validan una forma de aproximación diferente que trabaja tres planos de manera simultánea.

Explica Mar Sánchez que se trabaja un primer plano cognitivo, "en el que estamos enseñando al usuario determinadas píldoras mes a mes, cuáles son las amenazas, cuáles son los posibles riesgos y qué es lo que deben hacer

"Nuestro objetivo es cambiar el comportamiento"

Mar Sánchez, country manager, **Cyber Gurú**

para evitarlos". También se trabaja la parte emocional, para lo que la compañía cuenta con un programa específico que forma al usuario sin que se dé cuenta de que está siendo formado", para lo que, de una manera muy amena, se van a enseñar diferentes casos reales de incidencias; "y donde el usuario ve las consecuencias que tiene realizar una determinada acción". El último plano es la práctica: se lanzan pruebas a los usuarios todos los meses para ver si el comportamiento está alineado con la parte emocional con la que se está trabajando.

Inteligencia Artificial

La inteligencia artificial (IA) ha revolucionado la forma en que las empresas operan, generando un impacto profundo en diversos aspectos de sus negocios. No sólo ha permitido automatizar tareas repetitivas y rutinarias, liberando a los empleados para que se enfoquen en actividades de mayor valor, sino que además pueden procesar grandes cantidades de datos con una precisión mucho mayor que los humanos, lo que reduce significativamente los errores. Lo ciento es que, al automatizar procesos, las empresas pueden optimizar el uso de sus recursos, como tiempo y materiales.

Explicaba durante su intervención Jesús López del Peral, responsable de Innovación TIC del IBIMA Plataforma BIONAND de Málaga que en su empresa preocupa el uso de Inteligencia Artificial "en la investigación de los investigadores". De manera más genérica habla de cómo la IA está permitiendo que personas que casi no tienen formación puedan realizar ataques sofisticados y elogia lo que hacen en Ayuntamiento de Málaga desde el punto de vista de formación en ciberseguridad "porque entiendo que se han preocupado de dotar de infraestructura y de personal para hacerlo". Comentaba tam-

"Apostamos por un MFA resistente al phishing y que se pueda utilizar en la mayor parte de casos de uso"

Fabio Cichero, Sales Manager Southern Europe, **Yubico**

bién que cada vez es más habitual que haya una mayor mentalización sobre ciberseguridad en la parte directiva y que hay que aprovechar el impacto de un ciberataque para concienciar y se invierta algo más.

Respecto a la IA "estamos viendo cómo va evolucionando", reconoce Enrique Cibantos. Explica que además de formar y concienciar, el departamento tecnológico de Ádivin Beach Flag tiene que ser "muy proactivo a la hora de poner todas las herramientas posibles para prevenir problemas, y tener el backup suficiente como para poder resolver el problema que nos va a venir sí o sí". El reto de la IA es el tener que hacer frente a más problemas y más complejos.

Deja claro Ramón Freire que lo que está consiguiendo la inteligencia artificial es que los ataques de phishing sean cada vez más sofisticados. El punto de partida, aseguraba el CTO de Pegasus Aero Group, es que "el usuario picará antes o después", por lo que "yo tengo que montar mis barreras y mis defensas asumiendo que llegará el correo que se cuele y llevará un enlace malicioso que el usuario terminará pinchando" y, partiendo de esa base "es como construir esa seguridad por capas".

> La IA ha revolucionado la forma en que las empresas operan, generando un impacto profundo en diversos aspectos de sus negocios

Recuerda Juan García Galera que, cuando se habla de inteligencia artificial, "hay que tener en cuenta la parte de cumplimiento" y que, según el Reglamento de Inteligencia Artificial, "tenemos que saber qué podemos hacer y qué no podemos hacer pues existen prácticas prohibidas para el uso de la IA", añadiendo que el desconocimiento de los riesgos de la IA está provocando la llagada del "Shadow IA" de manera similar al ya existente "Shadow IT".

En Allied Telesis la inteligencia artificial se utiliza en la automatización de procesos. Así lo aseguraba durante su intervención Luis González Encuentra, director de la compañía para la región e Iberia, "un fabricante de networking que está migrando hacia la parte de cíber". Explicaba que, con el objetivo de ser muy proactivos y muy predictivos, "utilizamos la IA para saber los estados de la red, para que sepas en qué estado está la red en cada momento y, con un sistema de gestión automatizada, saber cuándo te va a fallar o cuáles son los puntos a revisar". La compañía también ha trabajado en la integración IT/OT, comentaba el directivo añadiendo que el problema en torno al mundo OT "es que, si paras una línea de producción OT, la pérdida es incalculable".

La apuesta de Allied Telesis es por redes coherentes con protocolos industriales sobre equipamiento no industrial, "para que realmente sea una única red la que esté manejando todo. Además, hemos añadido elementos de seguridad de forma automática que sean capaces de estar hablando con los firewalls independientemente de quién sea el fabricante para que le transmita la información, no solo de entrada-salida, o norte-sur, sino de este-oeste que detecta movimientos laterales", explicaba Luis González Encuentra.

Añadía el directivo que la propia herramienta es un controlador SDN que habla con los switches, o con los puntos de acceso, es capaz de detectar una amenaza y actuar de forma automática. Teniendo en cuenta que el 95% de los problemas ocurren en redes, “si somos capaces de poder automatizar esos procesos, estamos eliminando un 95 % de problemas”.

“La mayoría de las 300 empresas que están sujetas ahora mismo a NIS2 no tienen planes de respuesta ante incidentes”

Álvaro Fernández,
Sales Manager de **Sophos Iberia**

NIS2

La normativa NIS2 es un marco normativo fundamental para garantizar la seguridad de las redes y los sistemas de información en la Unión Europea. Al establecer requisitos claros y exigentes, contribuye a fortalecer la resiliencia de las organizaciones y a proteger a la sociedad en su conjunto frente a las amenazas cibernéticas. ¿Cómo se está abordando? ¿cuáles son los principales retos que tienen las empresas?

Para Juan García Galera NIS2 es una “una vuelta de tuerca más a las múltiples normas existentes tales como el ENS, DORA o el RGPD”. Estas normativas tienen una esencia similar a la hora de proteger la la información, cada una en su ámbito de actuación, tratando temas comunes tales como la importancia de la gobernanza de la seguridad de la información y la gestión de incidentes, teniendo como denominador común a todas ellas la gestión de la seguridad de la información basada en riesgos, la resiliencia y la necesidad de ser proactivos.

Durante su intervención comenta Jesús Valverde que, para aquellos que ya conocían la directiva NIS y tuvieron contacto con la Ley de Protección de Infraestructura Crítica, “NIS2 es un refuerzo”. Por otro lado, hay todavía una parte del mercado expectante de una transposición que aún no se había producido a fecha de celebración de este encuentro.

“El problema en torno al mundo OT es que, si paras una línea de producción OT, la pérdida es incalculable”

Luis González Encuentra,
responsable de **Allied Telesis en Iberia**

Que los trabajadores estén capacitados para identificar y reportar posibles amenazas permite que pueden prevenir incidentes de seguridad

Ribera Salud es entidad esencial, explicaba su CISO, Luis Pérez Pau. Al respecto del alcance de la normativa comenta que se pasa de unas 300 empresas sujetas a NIS, a unas 20.000 afectadas por NIS2, por lo que el perímetro que tendrán que controlar los organismos de control es mayor, “las certificaciones como la ISO27001 o el Esquema Nacional de Seguridad tendrán un papel a la hora de ayudar a demostrar el compromiso de cumplimiento de las empresas”, comentaba. Mencionaba que todo lo relacionado con los métodos de autenticación, la política de contraseñas o el de acceso a los sistemas corporativos puede ser la asignatura pendiente de muchas empresas.

La mayoría de las 300 empresas que están sujetas ahora mismo a NIS2 “no tienen planes de respuesta ante incidentes, no han realizado un análisis de riesgos, no se han comparado con la 27001, no tienen capacidad para monitorizar los comportamientos de los usuarios y equipos,

ni de detectar y responder” aseguraba Álvaro Fernández, asegurando que Sophos cuenta con una plataforma con la que “podemos ayudar a las compañías que realmente están faltas de recursos”.

La experiencia de la compañía con una gran cantidad de clientes lleva al directivo a enumerar algunos de los retos a los que se enfrentan los clientes, no sólo cumplir con las diferentes legislaciones, sino falta de recursos que lleva a tener equipos sobresaturados de alertas. “Podemos ayudar no sólo con nuestros productos, sino con

una capa de servicios de detección y respuesta que son necesarios para cumplir con una parte muy importante de NIS2”, aseguraba.

“Nuestro producto estrella es la gestión”

Donde más está creciendo Allied Telesis es en el mercado de equipamiento industrial para soluciones de IT, integraciones IT-OT, y generando soluciones de gestión automatizadas “para facilitar el uso del networking, que al fin y al cabo es algo básico para cualquier servicio”, dice Luis González Encuentra, responsable de Allied Telesis en Iberia.

Explica que el foco de la compañía es apostar por incluir protocolos industriales en equipamiento estándar para hacer una red completamente homogénea y que no haya problemas luego de interoperabilidad o de convergencia”.

Vista Manager es, en opinión de Luis González Encuentra, uno de los productos estrella de la compañía. Se trata de “un visor y concentrador de todas las aplicaciones que estás utilizando desde un único punto de referencia”.

Luis González Encuentra, responsable de **Allied Telesis en Iberia**

Allied Telesis™

“La concienciación y formación a los empleados está dirigida a cualquier empresa que tenga email”

Para Mar Sánchez, country manager de Cyber Guru para la región de Iberia, la concienciación y formación de los empleados está dirigida “a cualquier empresa que tenga un correo electrónico o un escaparate en internet”. Deja claro que lo que van a conseguir las empresas es, sobre todo, “tener a sus empleados más despiertos para que, cuando se produzca una amenaza, sepan detectarla, sepan reportarla y sepan reaccionar”.

La oferta de Ciber Guru consiste en una plataforma SaaS con un programa triple: concienciar la parte más cognitiva explicando cuáles son las amenazas; impactar en la parte emocional, “porque es muy importante que el empleado no solo no sepa qué es lo que tiene que hacer, sino que esté convencido de que tiene que hacerlo así”; y una parte de entrenamiento práctico.

Mar Sánchez, country manager de **Cyber Guru**

Cyber Guru

“Somos capaces de hacer sencillo lo complicado”

Tiene claro Álvaro Fernández, Sales Manager de Sophos Iberia, que “somos capaces de hacer sencillo lo complicado”. Añade que Sophos lleva 40 años en el mercado “porque prestamos mucha atención a los clientes, sus necesidades, y a las amenazas”, y que han modificado la manera de entregar la seguridad; “ahora se entrega como un servicio respetando las inversiones que ya están hechas por parte de los clientes”.

“Nos hemos propuesto es devolver el control y la visibilidad a los responsables de ciberseguridad”, comenta Ávaro Fernández cuando le preguntamos por la aproximación de Sophos respecto a la seguridad en la nube. Sophos Cloud Optix monitoriza la infraestructura que esté en los hiperescalares, avisando no sólo de comportamientos anómalos sino de fallos de configuración, además de “ayudar a cumplir con las normativas”.

Álvaro Fernández, Sales Manager de **Sophos Iberia**

SOPHOS

“El aumento de los ciberataques impulsa la adopción masiva de la autenticación multifactor”

El aumento de los ciberataques es “uno de los principales motores detrás de la adopción masiva de la autenticación multifactor basada en hardware”, explica Fabio Cichero, Sales Manager Southern Europe de Yubico, añadiendo que las empresas están buscando soluciones que ofrezcan una mayor protección y que “llaves físicas han demostrado ser increíblemente eficaces en este aspecto”.

“Estamos viendo un interés creciente en el uso de YubiKey en entornos donde los usuarios necesitan tener un método de autenticación robusta, resistente al phishing y que no dependa de un dispositivo móvil” asegura el directivo, añadiendo que están “diseñadas para ser extremadamente fáciles de implementar y utilizar tanto para las empresas como para usuarios finales, lo que reduce la fricción en el proceso de autenticación”.

Fabio Cichero, Sales Manager Southern Europe de **Yubico**

yubico