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*

"La innovación como aliada de la ciberseguridad"

CHECK POINT · ENTHEC · Qualys. · WatchGuard

Foro TAI Madrid.
La innovación como aliada de la ciberseguridad

Dirigido a responsables de TI y ciberseguridad, Foro TAI ha celebrado su tercer encuentro para saber qué preocupa a los responsables tecnológicos de las empresas y analizar qué necesitan sabiendo que garantizar la Seguridad de la Información 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 de que no para de evolucionar, tanto en defensa como en ataque:

- Los ciberataques son más y más sofisticados. El cibercrimen no sólo se ha profesionalizado, sino que los grupos patrocinados por los estados han aumentado.
- Los vectores de ataque han aumentado a medida que se multiplican los dispositivos, las redes (llega 5G), las identidades (también las de las máquinas), las tecnologías... Mención aparte merece la cadena de suministro como vector de ataque. Tal es su importancia, el riesgo que puede generar, que se menciona de manera específica en NIS2.
- Los objetivos somos todos. Los unos por ser infraestructura crítica, los otros por la importancia de los datos que manejan.
- La inteligencia artificial generativa ha irrumpido con demasiada rapidez. Quizá por primera vez la ventaja la tiene el mercado, la tienen los defensores, acostumbrados a trata con IA, el machine learning, el Deep learning... Pero los ciberdelincuentes están aprendiendo y a los buenos nos van a cortar las alas con la Ley de Inteligencia Artificial que se está redactando.

- De manera más específica podemos mencionar la seguridad OT e IoT, la inseguridad de la movilidad, el drama del ransomware, el reto de la autenticación y el passwordless para proteger la identidad, la gestión de las vulnerabilidades, la monitorización de los datos... y todo ello con falta, no tanto de talento, como de profesionales.

Llegaba el momento de arrancar un debate patrocinado por Check Point, Enthec, Qualys y WatchGuard en el que los protagonistas eran los asistentes: Vicent Pastor, COO&CIO de Abaco International Loss Adjusters; Luz Mª Hidalgo, CEO&CoFounder de AIBOT Amazing Intelligent Robots; Israel Díaz Domínguez, CISO de Asitur Asistencia; Esther Muñoz Fuentes, Subdirectora Gral. Ciberseguridad DPD Privacidad de Madrid

> "Los SOC deben acercarse a conocer el negocio, porque lo que es un incidente para una empresa, puede no serlo para mí"
>
> **Vicent Pastor,** COO&CIO,
> **Abaco International Loss Adjusters**

Digital-Ag. Transformación Digital Comunidad de Madrid; Jesús Yáñez Colomo, Socio Risk&-Compliance, Ciberseguridad, Protección Datos de Écija Abogados; Sergio Calvo, Director TI de Envalora; Jaime González, CIO&CISO de Grupo EDP HC Energía; Andrés Romero Sánchez, Re-

> “NIS2 viene a reforzar a los que los estaban haciendo bien, y va a pesar en aquellas que no han hecho nada”
>
> **Israel Díaz Domínguez,**
> CISO de **Asitur Asistencia**

gional Information Security Officer de Mercedes Benz AG; Jesús Abascal Santamaría, CISO de Plenitude España; Santiago Anaya Godoy, Global CTO de Prosegur/Cipher; Mª del Pino González-Junco, Cibersecurity Partnerships Manager de SIEMENS; Félix Rodríguez Cabrera, Director de Seguridad de Triodos Bank; Alejandro Expósito Esteban, experto en Digital Innovation&Business Operation; Max Moreno, responsable de ciberseguridad; Víctor Méndez, CIO; Mario García, Country Manager Spain&Portugal de Check Point; Lola Miravet, Chief Operations Officer de Enthec; Sergio Pedroche, Country Manager Spain&Portugal de Qualys; Carlos Castro, Strategic Account Manager de Watchguard.

NIS2

NIS2, la actualización de la Directiva sobre Seguridad de las Redes y los Sistemas Informáticos (NIS), entró en vigor el 27 de diciembre de 2022, tras su publicación en el Diario Oficial de la UE. Los estados miembros tienen hasta el 17 de octubre de 2024 para realizar la transposición y publicar las medidas necesarias para cumplir lo establecido por la directiva. Preguntar qué están haciendo los clientes para cumplir con la normativa ocupaba el primer bloque de debate de Foro TAI Madrid

Respondía Félix Rodríguez Cabrera, Director de Seguridad de Triodos Bank, que se valoran cuáles son las diferencias principales en NIS2 respecto a la primera versión de la normativa, o qué implica a otros estamentos dentro de la organización, como puede ser el departamento jurídico o los responsables de riesgos. La percepción, asegura el directivo, es que incide en algunos aspectos, pero que no hay cambios sustanciales “que en el sector financiero no ha-

> “Para hacer frente a la suplantación de identidad de marca, la clave está en el servicio de vigilancia digital”
>
> **Esther Muñoz Fuentes,**
> Subdirectora Gral. Ciberseguridad DPD Privacidad, Madrid Digital-Ag. Transformación Digital
> **Comunidad de Madrid**

yamos regulado ya". En todo caso, destaca que la gestión de la seguridad del tercero es donde se está incidiendo, "y donde estamos poniendo especial atención".

Jaime González, CIO&CISO de Grupo EDP HC Energía, dejaba claro que lo que preocupa en el sector de la energía "son las terceras partes", añadiendo a continuación que es algo que cuesta mucho abordar, y que la carga de trabajo que implica cumplir con NIS2 y otras normativas puede llevar a algunas empresas a perder lo importante.

"Por favor, no dejéis que los contratos que tengáis con prestadores de servicios TIC los negocien los técnicos solos, sin legal"

Jesús Yáñez Colomo,
Socio Risk&Compliance, Ciberseguridad, Protección Datos, **Ecija Abogados**

En opinión de Israel Díaz Domínguez, CISO de Asitur Asistencia, NIS2 viene a "reforzar a los que los estaban haciendo bien, y va a pesar en aquellas que no han hecho nada", además de ayudar a los responsables de seguridad de la información para poder desbloquear algunos proyectos.

En respuesta a los comentarios realizados por los asistentes, decía Mario García, director general de Check Point para España y Portugal, que si bien hay una serie de entidades que tiene un nivel de ciberseguridad muy alto, hay otras empresas mucho menos maduras, y que NIS2 sirve, entre otras cosas, para "tener una foto real" de la situación de cada empresa, "cuál es el análisis de qué hay en cada uno de los elementos para poder aportar las diferentes soluciones de ciberseguridad". Añadí el directivo que el 80 % de las propuestas no serán tecnológicas, "sino procesos y decisiones de cómo se hacen las cosas".

"Siempre hay que complementar las políticas de seguridad de los grandes proveedores de cloud"

Sergio Calvo,
Director TI **Envalora**

Cadena de suministro

Preguntada por cómo se está abordando desde Siemens la seguridad de la cadena de suministro, recuerda Mª del Pino González-Jun-

> “Lo que preocupa en el sector de la energía son las terceras partes”
>
> **Jaime González,** CIO&CISO, **Grupo EDP HC Energía**

co, Cibersecurity Partnerships Manager de la compañía, que hace varios años que se lanzó la iniciativa Charter Of Trust que precisamente recogía, en uno sus puntos, la seguridad de la cadena de suministro. Se apostó por desarrollar, con el resto de las compañías involucradas en la iniciativa, una lista de 17 requisitos básicos para los suministradores no críticos que se incluyeron en los términos y condiciones de los contratos. El siguiente paso, añade la directiva, fue desarrollar unos formularios básicos que ayudan a contrastar que las compañías verdaderamente cumplen con esos requisitos. Ahora, “cualquiera que trabaje en compras, o que esté negociando con proveedores, puede acceder a una base de datos y comprobar si se ha evaluado a un suministrador, y tener una idea de su nivel de madurez”.

Con la cadena de suministro “estamos entre la espada y la pared”, apuntaba Israel Díaz Domínguez, CISO de Asitur Asistencia. Recordaba que, si un proveedor ve vulnerada su cadena de suministro y hay un fraude, el seguro no se hace cargo porque lo que pide es que la cadena entera está segura. “El problema que nos estamos encontrando es que las empresas grandes tienen seguridad, pero cuando empiezas a bajar hay un solar enorme con el que estamos luchando nosotros”, asegura.

Poniéndose en el lugar de una tienda pequeña, Alejandro Expósito Esteban, experto en Digital Innovation&Business Operation, explica que las empresas pequeñas tienen pocos medios, pocos recursos y pocos conocimientos, y que lo que

> “Para obtener la máxima visibilidad, deben hacerse barridos a nivel de red para descubrir los dispositivos que están fuera del ámbito de nuestro trabajo”
>
> **Andrés Romero Sánchez,** Regional Information Security Officer, **Mercedes Benz AG**

agradecerían es que el mercado, los fabricantes “desarrollen algo que sea lo suficientemente accesible, entendible y manejable para ellos”. Habla de indefensión “porque al final estas perso-

nas se sienten, primero, amenazadas por lo que viene de fuera, por esas ciberamenazas, y luego, presionadas por los grandes, porque tienen que cumplir con cosas que no son capaces".

Como experto en ciberseguridad que ha tenido que lidiar con una cadena de suministro plagada de empresas pequeñas, incluso autónomos, habla Max Moreno de un modelo de responsabilidad compartida en el que se invierta en mejorar la seguridad a las empresas suministradoras, "porque al final es salvaguardar tu propia empresa".

"El principal reto es el acceso de los empleados a servicios o aplicaciones vía web"

Jesús Abascal Santamaría, CISO, **Plenitude España**

Le llamaba la atención a Lola Miravet, Chief Operations Officer de Enthec, que cuando se habla de NIS2 se termine hablando de las terceras partes, y comentaba que, acostumbrados a que los procesos estén muy automatizados, cuando una empresa tiene que hacer el análisis de la cadena de valor se recurre a formularios, validaciones, certificaciones varias... "y se trata de un proceso complicado". El secreto, aseguraba "es poder ser capaces de automatizar la validación de todos esos formularios a un coste muy reducido para que las empresas pequeñas puedan afrontarlo y meterlo dentro de los procesos de seguridad de las empresas grandes para que eso esté automatizado".

Visibilidad

Aunque tener una visibilidad total de los activos de la empresa es prácticamente imposible, es algo que persiguen todos los responsables de IT y ciberseguridad. Bajo la idea de que no se puede proteger lo que no se puede ver, las empresas apuestan por la visibilidad. Durante el debate comentaba Andrés Romero Sánchez, Regional Information Security Officer de Mercedes Benz AG, que tienen bien gestionados los activos, elementos de red, endpoint... inclusive los de terceras partes. A través de un siste-

"La revolución del EDR hacia el XDR es fundamental "sobre todo en el tema de la identidad, que es muy importante"

Santiago Anaya Godoy, Global CTO, **Prosegur/Cipher**

"Aunque estén en la nube, tú eres el responsable frente a tus usuarios, tus clientes y el regulador"

Mª del Pino González-Junco, Cibersecurity Partnerships Manager, **SIEMENS**

ma de VDI se han clasificado los activos o las empresas que se conectan, y a través de una CMBD (Configuration Management Database) de Qualys se realizan "barridos a nivel de red para descubrir los dispositivos que están fuera del ámbito de nuestro trabajo".

Durante su intervención, aseguraba Jesús Abascal Santamaría, CISO de Plenitude España, que en su compañía también tienen controlados los activos principales, al tiempo que destacaba que el principal reto de monitorización al que se enfrentan actualmente es el acceso no controlado de los empleados a servicios vía web ya que para la empresa son desconocidos. Por ejemplo, aplicaciones como ChatGPT porque "hay bastante intercambio de información no controlado que puede generar un impacto de seguridad".

Planteado durante el debate cómo se hace frente a las aplicaciones low code propone Alejandro Expósito Esteban colocarlas en un área militarizada, "en un entorno controlado del que no puedan salir y desde no puedan conectarse con ninguna aplicación externa a la compañía".

Hablando de activos, asegura Vicent Pastor, COO&CIO de Abaco International Loss Adjusters, que "todo lo que depende del usuario es lo que realmente nos preocupa". Se hace frente a la situación no solo mediante un control permanente, sino sensibilizando de la seguridad para que "realmente sean conscientes de lo que sus acciones particulares pueden hacer en la empresa". Respecto a las terceras partes, la cadena de suministro, se invierte en que sean conocedores de la ciberseguridad y en ayudarles a la hora de "implementar lo básico en seguridad".

En opinión de Sergio Pedroche, Country Manager Spain&Portugal de Qualys, desde el punto

"Hoy no puedes tener la certeza de que tu dato está en Europa, por mucho que se le exija a los grandes proveedore de nube"

Félix Rodríguez Cabrera, Director de Seguridad, **Triodos Bank**

de vista de los riesgos, “la visibilidad es un pilar fundamental desde el que construir cualquier

> “Las empresas pequeñas tienen pocos medios, pocos recursos y pocos conocimientos, y agradecerían que el mercado desarrolle algo que sea lo suficientemente accesible, entendible y manejable para ellos”

Alejandro Expósito Esteba,
Digital Innovation&Business Operation Director

servicio”. Comentaba que, a pesar de que se cree que se tiene control de todos los activos, es habitual encontrarse con activos nos controlados, lo que “difumina mucho la superficie de ataque”. Añadía el directivo de Qualys que, “si tenemos visibilidad de todos los activos que tenemos, independientemente de donde estén, vamos a ser capaces de poder tener los procesos y capacidades de monitorización más adecuadas”.

Managed, Detection and Response (MDR)

Asegurando que todo el mundo quiere recuperar la máxima información, meterla en el mismo saco y tener visibilidad de lo que está ocurriendo en una empresa, explicaba Santiago Anaya Godoy, Global CTO de Prosegur/Cipher, que la revolución del EDR hacia el XDR es fundamental “sobre todo en el tema de la identidad, que es muy importante”. Definía los servicios MDR como un “must” que se unen a otros servicies capaces de englobar toda la trazabilidad de información posible para poder tener más seguridad.

Esther Muñoz Fuentes, Subdirectora General de Ciberseguridad DPD Privacidad de la Comunidad de Madrid, se refería a los EDR como “el Santo Grial”. Explica que, cuando diariamente se ingestan 3TB de datos, no solo se disfruta del producto, sino del servicio, porque “lo más importante son las personas y los equipos humanos”. Mencionaba que en organizaciones muy grandes la respuesta automatiza no siempre es posible y que, aspirando a un MDR, lo que se tiene ahora son “herramientas distintas y procesos que intentan que la respuesta se lle-

> “Hay que proteger el dato más allá de la nube”

Max Moreno, ,
responsable de ciberseguridad

> La inteligencia artificial generativa ha irrumpido con demasiada rapidez y quizá, por primera vez, la ventaja la tenga el mercado, la tengan los defensores, acostumbrados a trata con IA desde hace años

ve más allá del puesto, las redes del perímetro y algunas redes".

En respuesta a la intervención de Esther Muñoz, explicaba Carlos Castro, Strategic Account Manager de WatchGuard, que la automatización "es un reto al que estamos yendo todos", pero que ofrecer una respuesta automatizada "es algo que aún está lejos" porque se tendría que conocer al cliente mejor que él mismo.

Sobre el MDR, que Gartner plantea como un servicio que da un tercero de forma remota con funcionalidades de SOC, comentaba Carlos Castro que el peso está en las funcionalidades que se ofrecen, que puede ser una o varias para saber no solo lo que pasa con el endoint, sino con los accesos e identidades, con las redes... y, sobre todo, en el equipo de personas, de expertos, que están detrás.

De todas las funcionalidades SOC que dice Gartner, el EDR, el NDR, la identidad, el SIEM... ¿Qué es lo que más os preocupa a vosotros?, preguntaba el directivo de WatchGuard. Cogía el testigo Esther Muñoz Fuentes para asegurar que, en caso de crisis "lo más importante es la telemetría que aporta, así como el contexto", para añadir que tiene muchas esperanzas en esos Copilot for Security, "que nos van a ayudar a todos, y que es lo que yo echo de menos cuando hay un incidente".

Apuntaba Vicent Pastor que la tecnología es un facilitado y que los SOC deben "acercarse a conocer el negocio, porque lo que es un incidente para una empresa, puede no serlo para mí".

Queriendo hacer una reflexión de todo lo que se había ido diciendo, Jaime González, CIO&-CISO de Grupo EDP HC Energía, comentaba

> “La gente se piensa que poner las cosas en la nube es como llevarlo a la caja de seguridad de un banco. Y no es cierto”
>
> **Mario García,**
> Country Manager Spain&Portugal, **Check Point Software**

que el SOC “tiene que ser algo que nos ayude todavía a ser más precisos a la hora de proteger nuestra infraestructura y nuestro servicio dependiendo del foco de negocio que tenga cada uno”, al tiempo que añadía que también es importante saber lo que están haciendo los ciberdelincuentes.

Adopción de la nube

Planteado cómo está yendo la evolución hacia el cloud y dónde se están poniendo las prioridades a nivel de ciberseguridad, comentaba Sergio Calvo, Director TI de Envalora, varias experiencias que le han llevado a confiar en las políticas de seguridad de los grandes proveedores de cloud, pero siempre complementadas con las suyas.

Alejandro Expósito Esteban ha vivido no solo una migración hacia la nube y sino una vuelta atrás, una migración de la nube al on-premise. El experto en Digital Innovation&Business Operation asegura que la mejor política es no fiarnos nunca de las políticas de seguridad de esas nubes, “porque los responsables somos nosotras, no ellos. Para nosotros son un medio, que está genial, pero la responsabilidad última siempre es nuestra”, algo en lo que se muestra de acuerdo Mª del Pino González-Junco, de Siemens, al asegurar que “tú eres el responsable frente a tus usuarios, tus clientes y el regulador”.

Hablando de nube y seguridad se pregunta Félix Rodríguez Cabrera, de Triodos Bank, cómo se va a gestionar Dora con Azure, Google, o

> “Cuando se habla de suplantación de identidad, tanto en redes sociales como en páginas web, uno de los temas importantes es saber qué se pretende con esa suplantación de identidad”
>
> **Lola Miravet,**
> Chief Operations Officer, **Enthec**

Amazon, un trío que define como “un monopolio”. Plantea también que se pasó del ‘todo cloud’ de la pandemia a un modelo híbrido por-

que “hay ciertos servicios, cierta información, ciertos procesos que no queremos que estén por ahí, precisamente por el monopolio”. Comenta también que se trabaja con multinacionales cuyos on-premises están fuera de Europa, “y no es lo mismo tener en dato en Europa que fuera. Hoy no puedes tener la certeza de que tu dato está en Europa, por mucho que se le exija a los grandes del monopolio”.

“La visibilidad es un pilar fundamental desde el que construir cualquier servicio”

Sergio Pedroche,
Country Manager Spain&Portugal, **Qualys**

Jesús Yáñez Colomo, Socio Risk&Compliance, Ciberseguridad y Protección Datos de Ecija Abogados, intervenía para recordar las guías de la Autoridad Bancaria Europea (EBA), “han exigido a las entidades financieras batallar en temas de ciberseguridad con sus proveedores antes de la llegada de NIS2 o DORA”, y que desde de Ecija Abogados se lleva batallando contra los grandes proveedores de cloud desde hace años. Asegurando que los abogados empiezan a entender de tecnología, pide a los compañeros de debate: “Por favor, no dejéis que los contratos que tengáis con prestadores de servicios TIC los negocien los técnicos solos” porque, conociendo toda la parte técnica, “hay tretas legales que se les puede escapar”, y destaca al mismo tiempo lo importante que es que haya colaboración entre el equipo legal y el equipo técnico en cuestiones de ciberseguridad.

“La gente se piensa que poner las cosas en la nube es como llevarlo a la caja de seguridad de un banco. Y no es cierto”, decía Mario García durante su intervención, añadiendo que los

“El doble factor de autenticación es la tecnología más sencilla que existe para proteger más”

Carlos Castro,
Strategic Account Manager, **Watchguard**

datos pueden estar aquí o en cualquier parte del mundo, “pero te los roban igual”. Habló no solo de aumentar las medidas de seguridad más allá de las que ofrecen los proveedores de nube sino de tener una capa de gestión independiente que permita cambiar de un proveedor a otro.

Aseguró también que la nube “ni es gratis, ni es barata, ni es fácil, ni es segura” y apuesta por entornos híbridos en los que se aprovecha el potencial de la nube cuando se necesita crecer, expandir o reducir, pero no cuando los procesos son siempre los mismos y funcionan de la misma manera.

Proponía durante el debate Max Moreno no confiar en la nube y proteger el dato más allá de la nube. Es decir, subir los datos a través de un proceso que acaba criptografiando el dato. “Eso es tecnología y proceso”, respondía Esther Muñoz, añadiendo: “Me falta la capa de negocio, quién decide qué dato es importante para el negocio”.

Ponía sobre la mesa Sergio Pedroche un dato importante: el 65 % de los ataques cloud se generan por malas configuraciones, al tiempo que aseguraba que los servicios de cloud dentro de las empresas están aislados, que las personas que llevan la cloud no suelen saber de seguridad. Coincidía la Esther Muñoz, de la Comunidad de Madrid asegurando que la responsabilidad de todo el diseño de seguridad y de toda la supervisión de seguridad no puede caer en el CISO, y que “los de desarrollo, sistemas, comunicaciones, cloud... tienen que saber de seguridad, y nosotros hacemos una labor de supervisar”.

> NIS2 entró en vigor el 27 de diciembre de 2022. Los estados miembros tienen hasta el 17 de octubre de 2024 para realizar la transposición y publicar las medidas necesarias para cumplir lo establecido por la directiva

Suplantación de identidad

La suplantación de identidad de marca en redes sociales o en páginas web ha aumentado drásticamente. ¿Cómo se está gestionando? Para Esther Muñoz la clave está en el servicio de vigilancia digital, un servicio para el que cuenta con el apoyo de partners tanto en el inventariado y monitorización de dominios como de las cuentas en redes sociales.

Comentaba Jesús Abascal, con experiencia en conseguir el cierre, o take down, de los dominios, que la mayoría de dominios falsificados se generan desde el extranjero, y que la manera más rápida de acabar con ellos es realizar un cierre técnico, que es la desactivación temporal o permanente de un sitio web o servicio online por parte de las autoridades o proveedor de alojamiento web.

Mencionando casos de suplantación de páginas web, dejó claro Jaime González, de Grupo eDP HC Energía, que “a veces las cosas tienen que pasar” para que se tome conciencia de ellas y se pueda avanzar con la ciberseguridad.

Comentaba Lola Miravet que el problema de la suplantación de identidades de marca “al CISO le queda un poco lejos, porque está dentro del ámbito de marketing y comunicación, que muchas veces, además, lo tienen externalizado”.

Mencionaba que la conversación se ha centrado en la resolución de problemas, en el take down, pero que “muchas veces la clave está en detectarlo cuanto antes”, al tiempo que añadía que cuando se habla de suplantación de identidad, tanto en redes sociales como en páginas

web, “uno de los temas importantes es saber qué se pretende con esa suplantación de identidad: daño reputacional, robo de credenciales…”, y que cuanto más rápido y más claramente se identifique cuál es el problema, de quién depende y quién pueda ayudar en una resolución rápida, mejor.

Gestión de identidades y accesos

Las empresas de hoy en día enfrentan numerosos retos a la hora de gestionar las identidades y accesos (IAM). Estos retos se ven agravados por la creciente complejidad del entorno de TI, el aumento del número de usuarios y dispositivos, y la sofisticación de las ciberamenazas.

Se planteba al término de nuestro debate qué medidas están implementando las empresas a la hora de proteger la identidad y los accesos de los empleados de manera efectiva, y enseguida se menciona el múltiple factor de autenticación. Max Moreno habló de condicionales de acceso por país, ciudad o IP, como una propuesta que funciona muy bien “y acota bastante el ámbito”.

Respecto al doble factor salió a colación el problema que a veces surge cuando los empleados no quieren utilizar sus dispositivos para hacer esa doble, o triple, autenticación. El planteamiento general es que si el empleado quiere acceder a recursos de la empresa en su móvil “hay ciertas cosas que tiene que aprobar”; y si quiere teletrabajar y se requiere un MFA en su móvil, “o lo autoriza o no teletrabaja”.

En opinión de Carlos Castro, de WatchGuard, el doble factor de autenticación es “la tecnología más sencilla que existe para proteger más. No hay una cosa en la que puedas invertir poco dinero y sacar un nivel de protección tan alto”, añadía, asegurando que, siendo cierto que causa rechazo, cada vez están más concienciados.

Mencionaba también Carlos Castro que no solo hay que aplicar el doble factor a los empleados,

sino a los proveedores, a los terceros, y que debe cubrir todos los casos de uso, no solo al acceso prioritario de ciertos tipos de sistemas.

Intervenía Andrés Romero Sánchez, de Mercedes Benz para hablar de un piloto en el que al usuario que quiere utilizar su teléfono móvil se le está proporcionando el passwordless a través de reconocimiento facial o huella.

“Tenemos toneladas de tecnología, y la gente con el conocimiento para que esa tecnología os sirva para algo”

La nube, la inteligencia artificial, NIS2 han sido algunos de los temas tratados en el Foro TAI Madrid, recuerda Mario García, Country Manager Spain&Portugal de Check Point, para explicar que la manera que tiene la compañía de ayudar a los clientes “es con conocimiento”.

“Sabemos de NIS 2, de cloud, y cómo os impacta y qué pasa cuando los datos van de un sitio a otro...”, dice el directivo, añadiendo que en es la parte de abordar la ciberseguridad de una forma completa y cómo impacta en mi empresa “donde os podemos ayudar”. Check Point, comenta también Mario García, tiene toneladas de tecnología, “pero sobre todo la gente con el conocimiento para que esa tecnología os sirva para algo”.

Mario García, Country Manager Spain&Portugal, **Check Point Software**

CHECK POINT™

“Enthec es una empresa española y lo que hacemos es ciberinteligencia de amenazas”

“Somos capaces de ver exactamente lo mismo que ven los cibercriminales cuando quieren plantear un ataque a una compañía”, dice Lola Miravet, Chief Operations Officer de Enthec, una empresa española que hace ciberinteligencia de amenazas a través de un ejército de robots que busca en internet, DeepWeb, Dark Web y redes sociales.

Entre las ventajas de la compañía destaca el funcionar de manera continua y no intrusiva, “lo que nos permite monitorizar la cadena de valor de una manera muy sencilla”. Se suma el hecho de que la plataforma es muy fácil de configurar a partir del nombre del dominio para “obtener un montón de información de la compañía”.

Lola Miravet, Chief Operations Officer, **Enthec**

ENTHEC

“Nuestra misión es poder medir el riesgo, poder comunicarlo y proponer una solución”

Qualys nació en el ‘99 con el objetivo fundamental de establecer una plataforma de gestión de riesgo global para sus clientes. Nos lo cuenta Sergio Pedroche, Country Manager Spain&Portugal de Qualys en este video en que explica que la mission fundamental de la compañía es “poder medir el riesgo, poder comunicarlo adecuadamente y poder proponer una solución, asegura el directivo añadiendo que, siendo esto último lo importante, no es suficiente. “Poder poner contramedidas y acciones para la solución de esos problemas es fundamental para nosotros”, comenta Sergio Pedroche.

Recientemente la compañía ha presentado TotalCloud 2.0, una actualización de la plataforma de protección de aplicaciones nativas de la nube (CNAPP) impulsada por IA de Qualys.

Sergio Pedroche, Country Manager Spain&Portugal, **Qualys**

Qualys®

“El MFA permite proteger el acceso a mis datos de la mejor forma posible y no disruptiva”

Asegura en este video Carlos Castro, Strategic Account Manager de Watchguard, que la sencillez es la mejor aproximación para poder controlar la seguridad de la cadena de suministro, que ha demostrado ser un tema de interés para los participantes del foro.

A la hora de proteger la seguridad de la gente que se conecta desde fuera, plantea la compañía plantea “soluciones del tipo de múltiples factores de autenticación”, que permiten proteger el acceso a mis datos “de la mejor forma posible y no disruptiva contra el usuario”.

Respecto a los servicios gestionados de seguridad, o MDR, WatchGuard apuesta por servicios personalizados que hagan “foco donde cada organización realmente tiene sus problemas y necesidades”.

Carlos Castro, Strategic Account Manager, **Watchguard**