it Digital Security

Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

Junio 2021

Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

La seguridad proactiva es un enfoque más holístico para proteger los sistemas de TI. Se centra en la prevención más que en la detección y la respuesta y es una aproximación que gana peso en las empresas. Según el informe Cyber Risk Alliance, Cybersecurity Resource Allocation and Efficacy Index (CRAE) del segundo trimestre de 2020 las empresas con 500 o más empleados en América del Norte y Europa enfatizaban las medidas de seguridad proactivas para proteger los activos y detectar infracciones, en contraposición a un enfoque de seguridad puramente reactivo.

Un enfoque de seguridad proactivo consiste en comprender dónde se encuentran las vulnerabilidades para poder mitigarlas. La concienciación de los usuarios es una de las medidas de seguridad proactivas que deben tenerse en cuenta ya que permite adelantarse a una ingeniería social u otros ataques de phishing al garantizar que una base de usuarios sabe cómo detectar los signos y trucos reveladores de los estafadores.

Otras medida proactiva son las pruebas de penetración, la monitorización de endpoints y redes o el uso de tecnologías como el Threat Hunting

LA VISIÓN DE LAS EMPRESAS **LA VISIÓN DE LA INDUSTRIA IT**

itds

Encuentros ITDS

ENCUENTROS ITDS - SEGURIDAD PROACTIVA **CLICAR PARA VER EL VÍDEO**

y la inteligencia de amenazas. Los avances en aprendizaje automático están ayudando a que las medidas reactivas sean más proactivas al reducir los falsos positivos y negativos.

Una cosa importante a tener en cuenta es que las regulaciones de protección de datos a menudo exigen un enfoque proactivo de la seguridad. El RGPD de la UE, por ejemplo, requiere un enfoque de "privacidad por defecto y diseño" para la protección de datos, esperando que la protección de datos se integre en un sistema.

Pero lo más importante es que la seguridad proactiva funciona, ya que según el informe CRAE las organizaciones que apuestan por un enfoque proactivo de la ciberseguridad se sentían más seguras de que las medidas funcionaban.

Con el fin de saber lo que está ocurriendo en la empresa española IT Digital Security ha organizado un nuevo Encuentros ITDS bajo el título "Seguridad Proactiva, ¿hasta dónde estás dispuesto a llegar?", en el que han participado Ignacio Pérez, CISO, Aragonesa de Servicios Telemáticos (AST) (Gobierno de Aragón); Judit Closa Ribalta, CISO de Habitissimo; Joan Massanet, CTO y CISO de Maximice Events Group; Mónica de la Huerga, CISO de Sopra Steria; José Luis Paramio Martínez, CISO de Userlytics; Raül Albuixech Gandia, director de servicios y soporte técnico de ESET España; Raúl Dopazo, Arquitecto de Soluciones de One Identity; Francisco Valencia Arribas, Director General de Secure&IT; Sergio Martínez Hernandez, Country Manager Iberia de SonicWall y Raúl Nuñez Herrero, Ingeniero Preventa de Trend Micro.

LA VISIÓN DE LAS EMPRESAS

AST Gobierno de Aragón. Ignacio Pérez, CISO

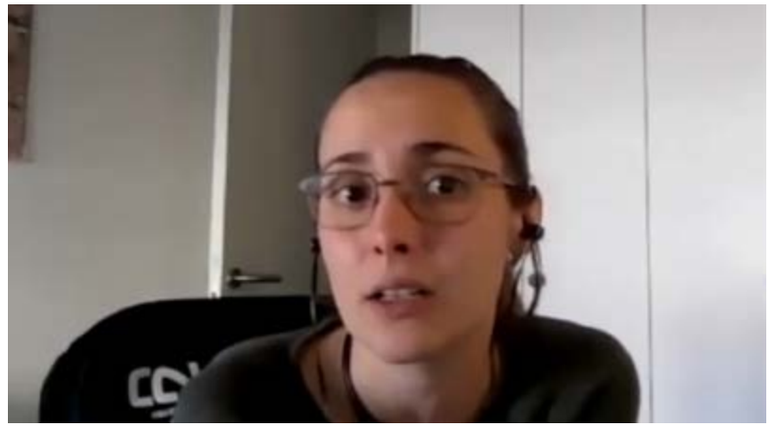
El control de la superficie de exposición es una de las principales preocupaciones de Ignacio Pérez, CISO de AST (Aragonesa de Servicios telemáticos) del Gobierno de Aragón, quien es el responsable de todos los elementos TIC de la región “con un modelo de negocio complicado porque nada tiene que ver un centro de salud con un juzgado o una oficina de empleo” y por lo tanto dónde poner las capas de seguridad en cada momento “es uno de los grandes quebraderos de cabeza” a los que se enfrenta.
Para Ignacio Pérez la proactividad en la seguridad no está tanto en la tecnología como en el proceso. Apuesta por la inteligencia, “tanto en la adquisición, en el Threat Intelligence de donde sacamos nuestras fuentes, como en el análisis que hacemos de ello, y en la respuesta”, y asegura que, en

"El Threat Hunting nunca va a ser un producto"

Ignacio Pérez, CISO, AST

la medida en que somos capaces de automatizar alguna de estas fases, ganamos en rapidez, “pero al mismo tiempo no puedes quitar el factor humano del que está indagando”.
Asegura este CISO que es tanto la capa tecnológica que te facilita una respuesta mucho más rápida de lo que podrías hacerlo con humanos, como la capacidad de tus procesos que te permiten detectar esos problemas
“El Threat Hunting nunca va a ser un producto. No puede serlo por su naturaleza”, dice Ignacio Pérez, quien asegura que el coste de llevar la securización a todas las superficies de exposición es inasumible; “para que sea viable hay que adecuar el nivel de securización al ámbito que quieres proteger, no es lo mismo un centro de educación secundaria que el centro de protección civil 112”.
Al final se pone el foco en dos cosas: la información y los servicios esenciales; “y para mí la información es muy importante, pero que no se me caiga la monitorización de las UCIs también, y ahí no hay ningún dato especialmente relevante”.

“Yo pediría sobre todo sinceridad”, dice Ignacio cuando se le plantea qué pediría a los fabricantes o proveedores de servicios; “dime lo que hace y cómo lo hace”. Menciona también la orquestación unificada como un Santo Grial y “el compromiso, el soporte, el acompañamiento”.



HABITISSIMO. Judit Closa, CISO

“Siempre habrá nuevas amenazas y superficies de exposición no controladas, y el poder priorizar, el poder escalar el riesgo para que la situación se asuma a nivel de negocio es el paso principal”, dice Judit Closa, CISO de habitissimo, añadiendo que amenazas concretas como el ransomware, o el phishing más básico, son algunos de los retos a los que se enfrentan los responsables de ciberseguridad de las empresas.

"La monitorización es lo que te ayuda a tener una postura de seguridad más proactiva"

Judit Closa, CISO, HABITISSIMO

Para Judit Closa, "todas las tecnologías que tengan que ver con la monitorización de tu red, de tus activos", son las que ayudan adoptar una postura de seguridad más proactiva. Añade la directiva de habitissimo que "tener tu superficie de exposición más controlada implica que la tengas bajo monitorización, con un centro de operaciones que te responda en unos tiempos adecuados para tus requerimientos de negocio".

Sobre el Threat Hunting y la Deception, que son tecnologías que buscan cazar y poner trampas al ciberdelincuente, dice Judit Closa que no es que la empresa española no esté preparada para su uso, sino que se incluye dentro de actividades de inteligencia, o que son parte de los servicios de monitorización que te puede dar un SOC, y no algo que habitualmente se haga de forma aislada.

Destaca Judit la importancia de la comunicación, tanto con los usuarios como con las juntas directivas y los propios proveedores mencionando que debe quedar muy claro lo que se está incluyendo en un servicio, a veces saturado de añadidos que te van dando funciones diferentes. "Hay que fortalecer la comunicación, tanto pre-venta como post-venta, y los lazos que hay con los servicios de soporte, que deben ser próximos", dice la CISO de habitissimo, añadiendo que siempre cuesta conseguir que un proyecto llave en mano realmente se acabe implementando bien, porque cada empresa se organiza de una forma diferente.

"La comunicación es básica para cualquier tipo de relación, así como asegurar unas buenas implementaciones", concluye Judit Closa.

MAXIMICE EVENTS GROUP. Joan Massanet, CISO y CTO

"Los ataques de ransomware están siendo nuestra gran preocupación", dice Joan Massanet, CTO y CISO, Maximice Events Group. Apunta dos motivos: el cifrado de datos en sí mismo y la denegación de servicios que conlleva.

"Es el soporte lo que aporta el valor a la solución"

Joan Massanet, CTO y CISO, Maximice Events Group

"La herramienta perfecta para los CISO sería una calculadora de ROI que nos diera siempre positivo porque al final todo se basa en el beneficio que va a generar y no es los gastos", asegura Joan Massanet, añadiendo que a nivel tecnológico y como herramienta diaria apuesta por los IRM (Information Rights Management) para la gestión de los datos y los documentos. Hablando de datos, "la extorsión es una de las cosas más graves que nos puede pasar porque si el cliente pierde confianza en ti, ahí ya no puedes tener ingresos de ningún tipo".

Otras tecnologías que destaca Massanet son las herramientas de parcheado virtual de vulnerabilidades y "el XDR para poder visibilizar los ataques dentro de nuestra propia red".

Apunta también el CISO de Maximice Events Group que le preocupa el uso de la inteligencia artificial en los ciberataques y la computación cuántica "capaz de romper cualquier cifrado en cuestión de segundos", con la consiguiente pérdida de confidencialidad.

Ahora lo que importante es el dato y creo que la arquitectura Zero Trust es algo que deberíamos implementar todos

La interoperabilidad es algo que hace muchísima falta, “sobre todo cuando hablamos de recoger toda esa información, juntarla y saber qué está pasando”, dice Joan Massanet, quien pediría a los fabricantes reducir la cantidad de información para poder ir al grano de lo que hace un producto. Menciona también el tema de los costes de las soluciones y los presupuestos con los que se trabajan en las empresas puntualizando que no cree que haya un producto mejor que otro y que “es el soporte lo que aporta el valor a la solución”.

SOPRA STERIA. Mónica de la Huerga, CISO

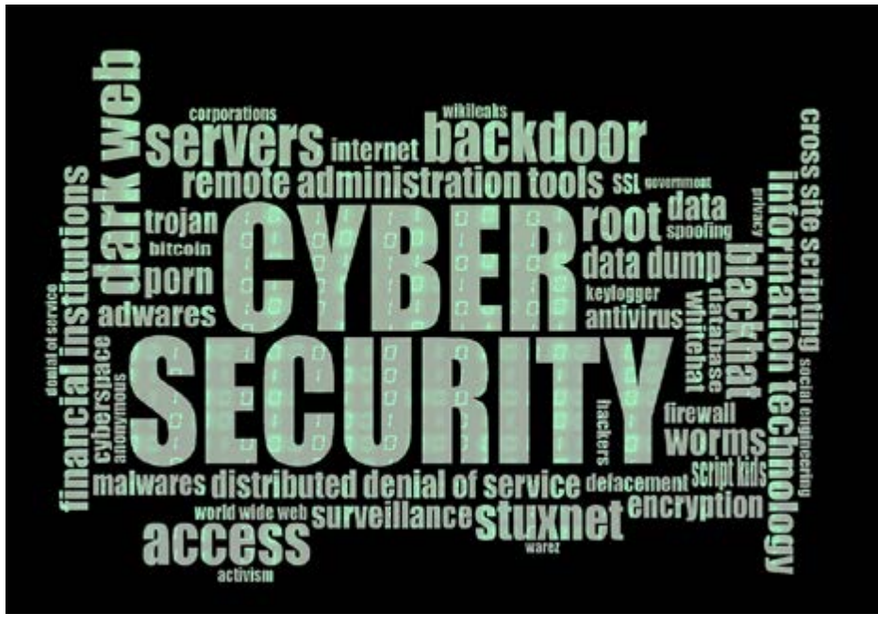
Además de prevenir los ataques de ransomware “lo importante es proteger el dato, que es el objetivo”, dice Mónica de la Huerga, CISO de Sopra Steria,

"En España estamos en la fase del EDR"

Mónica de la Huerga, CISO, SOPRA STERIA

cuando preguntamos cuáles son los retos a los que se enfrentan los responsables de ciberseguridad. Haciendo referencia a la pandemia, “que pensábamos que eran 15 días y llevamos ya año y medio”, también se ha convertido en un reto el control de los accesos “porque el perímetro que antes teníamos bien acotado se ha ido a las casas de nuestros colaboradores y proveedores, y es un poco más difícil de controlar, gestionar y verificar”. Añade Mónica de la Huerga que el control de la cadena de suministro es otro de los aspectos que los responsables de ciberseguridad de las empresas deben tener muy en cuenta.

Cada uno debe saber muy bien cuáles son los riesgos, alinearlos con los objetivos de negocio y adecuarse a los presupuestos, dice Mónica de la Huerga. Añade la CISO de Sopra Steria que se debe evitar caer en una avalancha de datos que te impidan hacer tu trabajo y encontrar la aguja en el pajar. Coincide con el resto de ponentes en el que el factor humano se debe tener en cuenta, porque por muchas medias tecnológicas que tengas “si al



final me llega un intento de phishing y hago clic en el enlace porque voy con prisa, ya han superado una de las capas de seguridad”.

“El Threat Hunting lo hacemos modularizando en función del análisis de riesgos, de ese presupuesto que nos validan, etc.”, dice Mónica de la Huerga. Añade que no sólo hay que tener en cuenta la búsqueda de vulnerabilidades, sino el poder desplegar todas las soluciones para corregirlas, el poder detectar una vía de ataque y eliminarla, “y eso como tal no lo estamos haciendo en España. Estamos en la fase de EDR”.

Un dashboard unificado y simplificado, “que casi sea como un semáforo de rojo, verde y porque tenemos muchas soluciones de diferentes fabricantes y la interoperabilidad no es tan simple” es algo

que pediría a los fabricantes. Añade que analizar qué información es importante o no es complicado cuando tienes un entorno complejo, y que lo que diferencia un producto de otro es el soporte; “no digo que todos sean exactamente iguales pero el diferencial es el soporte que te dan, ese acompañamiento para poder aprender a sacar el máximo partido a esas soluciones que has comprado”.

USERLYTICS CORPORATION. José Luis Paramio, CISO

Además del del phishing, el ransomware..., “cambiar los usos y costumbres de algunos empleados es uno de los retos a los que yo, por lo menos personalmente, me enfrento”, dice José Luis Paramio, CISO de Userlytics Corporation. Dice también que seguridad es la palabra de moda y está en boca de todos, “aunque cuando la pronuncien no sepan la carga que lleva detrás” y que “la cantidad ingente de oferta en herramientas y en soluciones de seguridad” es otro de los retos a los que deben enfrentarse los responsables de ciberseguridad. El presupuesto, asegura, es importante, tanto como acertar con la herramienta que necesita la empresa.

Para una empresa como Userlytics Corporation, con presencia en Miami, Tejas, Portugal, Madrid, Taiwán... “la mejor tecnología es la nube”, dice José Luis Paramio. Trabajar en la cloud “nos permite acotar bastante la superficie por la que podemos ser atacados, y además el tipo de alertas al que tenemos que estar pendiente”. Se añade que la compañía que protege realiza cursos y pruebas sobre ciberseguridad de manera periódicos, porque más que la tecnología a veces son las personas las que tienen que ayudar.

Ante la pregunta de qué le pediría a un fabricante o proveedor de servicios, hace referencia José Luis Paramio a la cantidad de información que se aporta asegurando que “un exceso de información es absolutamente inservible”. Afirma que una cuantiosa información te vale cuando ya tienes una experiencia con el producto en sí y menciona también curvas de aprendizaje algo elevadas. El resultado

es que las empresas contratan el producto que ya conocen y con el que ya tienen experiencia sus empleados, “o bien contratan al empleado que tiene experiencia con el producto que han contratado, o lo subcontratan todo a un tercero”.

Finaliza pidiendo más capas de abstracción, el hacer más sencillas las soluciones y el que se puedan hablar entre ellas, “porque yo abro cada mañana mi navegador y tengo 14 pestañas en lugar de un solo dashboard con toda la información”. Resumiendo: compatibilidad entre las soluciones, servicios unificados y más capa de abstracción.

"La mejor tecnología de seguridad es la nube"

José Luis Paramio, CISO, Userlytics Corporation

LA VISIÓN DE LA INDUSTRIA IT

ESET ESPAÑA. Raül Albuixech, director de servicios y soporte técnico

"Los fabricantes llevamos tiempo trabajando en la creación de soluciones y herramientas para ser algo más que un simple antivirus basado en firmas", dice el director de servicios y soporte técnico de ESET España. Añade que las empresas son cada vez más conscientes de que hace falta adoptar medidas de seguridad adicionales y que, además de visibilidad e inteligencia, la seguridad proactiva necesita la educación del usuario final, una educación "que solucionaría la gran mayoría de incidencias habituales.

Menciona el problema del presupuesto asegurando que, aunque los fabricantes ofrezcan mejores herramientas y mejores soluciones a un mejor precio, "hay tantos frentes de batalla que es imposible llegar a cubrirlos todos y hay que priorizar". El último punto para adoptar una seguridad más proactiva es la educación del usuario final; "educar en una buena praxis a la hora de trabajar con datos e información sensible".

Para Raül Albuixech, tan importante es crear herramientas o soluciones que te brinden toda la información posible como piezas herramientas estén bien optimizadas y bien configuradas para que puedas extraer el 100% de los datos que tienes. Añade que los fabricantes deben crear soluciones

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE ESET

CLICAR PARA VER EL VÍDEO

"Además de visibilidad e inteligencia, la seguridad proactiva necesita la educación del usuario final"

Raül Albuixech, director de servicios y soporte técnico, ESET España

de inteligencia, “pero sobre todo crear soluciones que puedan extraer la aguja en un pajar de manera automatizada”.

Por otra parte, de poco vale implementar una solución y olvidarse de ella, por lo que destaca la importancia de los servicios que se ofrecen durante la vigencia del contrato o licencia, no sólo relacionados con la configuración, puesta en marcha y optimización, sino en lo que se refiere a la monitorización y comprobar que todo está funcionando bien.

En opinión de Raül Albuixech el Threat Hunting no ha empezado a despegar en España, donde la palabra de moda es EDR. Añade que le quedan algunos años para que su uso esté más generalizado y que habrá diferentes formas de consumirlo, ya sea en un modelo directo o a través de un servicio

ONE IDENTITY. Raúl D’Opazo, Arquitecto de Soluciones, consultor de Ventas EMEA

Confirma el portavoz de One Identity que sí se está viendo una seguridad más proactiva en las empresas al tiempo que asegura que el discurso debe ir por hablar de prioridades y aplicar estrategias de seguridad, “y no tanto de comprar una solución, implementarla en tres meses y olvidarte”. Menciona algunas de las barreras que frenan esa proactividad, como es no involucrar al negocio o a recursos humanos, “o a cualquier departamento que realmente sea el propietario de los datos que nosotros queremos proteger desde el punto de vista tecnológico”.

También comenta Raúl D’Opazo durante su intervención que en ocasiones los proyectos se quedan en unas capas tan básicas que “esa idea de crear algo más proactivo es muy

"No involucrar al negocio o a recursos humanos frena la proactividad"

Raúl D'Opazo, Arquitecto de Soluciones One Identity

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE ONE IDENTITY

CLICAR PARA VER EL VÍDEO

itds

Encuentros ITDS

LA VISIÓN DE LAS EMPRESAS | **LA VISIÓN DE LA INDUSTRIA IT**

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE SECURE&IT

CLICAR PARA VER EL VÍDEO

"La tecnología que más ayuda a la prevención es la visibilidad"

Francisco Valencia, CEO, Secure&IT

complicado, aunque después tecnológicamente tengas la capacidad e incluso tu estrategia sea la correcta".

A la hora de hablar de las soluciones que pueden ayudar a la adopción de una postura más ofensiva señala Raúl D'Opazo que hay dos vectores de los que preocuparse: la identidad y el dato, que ahora mismo están deslocalizados. Menciona

el directivo de One Identity el machine learning como el elemento al que cualquier fabricante de cualquier segmento de mercado de seguridad está dando mucha consistencia, así como la importancia de construir aplicaciones que pueden hablarse con el resto del ecosistema para intentar ser un poco proactivo.

SECURE&IT. Francisco Valencia, CEO

"Muchas veces el CISO no sabe qué es lo que está pasando y no hay herramientas que le arrojen una visibilidad global de lo que está sucediendo en la infraestructura, en casa de las personas, en sus móviles, en la nube…", asegura Francisco

Valencia, Director general de Secure&IT, apuntando un segundo reto al que se enfrentan los responsables de ciberseguridad: la socialización del riesgo.

Dice también este directivo que la protección de la información “va mucho más allá de la informática” y que es importante “conseguir socializar el riesgo y que todos los departamentos sean conscientes de los riesgos y sean partícipes en la solución”.

Respecto a si se está adoptando una seguridad más proactiva, no tiene claro Francisco Valencia si se está produciendo desde el punto de vista del fabricantes o desde la organización “por el miedo y el compromiso que ahora empiezan a adquirirlos los órganos directivos, consejos de administración y comités de dirección”.

El reto al que se enfrenta Secure&IT no es lo que detecta y para la solución del fabricante, “sino lo que no es capaz de parar”. El SOC de la compañía recibe 600 millones de eventos cada día y tiene unas 10.000 alarmas diarias, y aunque se consiguen automatizar parte de las alarmas, “hay otra gran parte que se tienen que analizar a mano”. Explica el directivo que la tecnología que más ayuda a la prevención es la visibilidad, “y para conseguirlo lo ideal es tener una buena herramienta capaz de integrarlo todo, con un dashboard facilito en el que pueda verse todo lo que está pasando en la compañía y, en función de los que se vea, se puedan tomar acciones”.

Para Francisco Valencia el Threat Hunting es una pieza de un servicio o producto que está más cerca de los SOCs que de las empresas. “Un cliente no compra directamente y de forma aislada un Threat Hunting, sino que forma parte de un producto/servicio”.

En relación a los reducidos presupuestos de las administraciones públicas, del que es representante Ignacio Pérez, compañero de debate, dice Francisco Valencia que “el problema viene derivado de una de una grave falta de conocimiento por parte de la alta dirección”, que muchas veces no saben determinar cuánto vale la información que manejan”.

SONICWALL. Sergio Martínez, Country Manager Iberia

Según datos aportadas por Sergio Martínez en este debate, el 70% de los CISOs no se sienten

cómodos con las herramientas de seguridad que tienen desplegadas, y cerca de 60% se sienten preocupados por los usuarios que están al otro lado de la pantalla, lo que demuestra que “la formación es un aspecto muy importante”. Por otra parte, el Cyber Threat Report de Sonicwall señala que el ransomware se ha incrementado un 62% a nivel mundial, y un 20% los intentos del intrusión, “lo que nos lleva a plantearnos si se ha desplegado el modelo correcto de seguridad y si estamos en la fase de reducir riesgos”, unos riesgos que se han multiplicado con el teletrabajo y a los que solo podemos enfrentarnos con una defensa proactiva que vaya de extremo a extremo, que detecte lo desconocido, nos ofrezca visibilidad sobre lo que está ocurriendo, verifique la identidad de los usuarios… “y todo esto con un TCO adecuado para que salgan los números”.

“Nuestra estrategia es una defensa por capas, encima de la cual tiene que haber una monitorización que te de una visibilidad única de todo lo

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE SONICWALL

CLICAR PARA VER EL VÍDEO

> "Más que una tecnología, el Threat Hunting es un proceso"
>
> Sergio Martínez, Country Manager Iberia, SonicWall

que está ocurriendo en tu infraestructura”, explica Sergio Martínez cuando preguntamos qué tipo de tecnologías ayudan a generar una postura de seguridad más proactiva. Añade el directivo de SonicWall la capacidad de la compañía de detectar lo desconocido gracias a la inteligencia artificial y a una tecnología de sanboxing con tres motores que permite a los clientes “detectar y reaccionar a las ciberamenazas en tiempo real y de una forma casi automática”.

Sobre el Threat Hunting apunta Sergio Martínez que más que una tecnología es “un proceso de búsqueda de malware y de amenazas dentro de nuestras infraestructuras”.

SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE TREND MICRO

CLICAR PARA VER EL VÍDEO

"Hay que dar visibilidad, y cuanto más unificada mejor"

Raúl Núñez, Ingeniero Preventa, Trend Micro

TREND MICRO. Raúl Núñez, Ingeniero Preventa

Explica el portavoz de Trend Micro que en los primeros tiempos los fabricantes de seguridad se centraron en parar lo malo, pero que "actualmente con esta aproximación no vas a ningún sitio y tenemos que dar visibilidad y saber si un comportamiento es anómalo", que es hacia donde los fabricantes desarrollan su estrategia en pro de una seguridad más proactiva.

Destaca Raúl Núñez tres elementos que ayudan a conseguir una ciberseguridad más proactiva, empezando por la concienciación porque "por mucho dinero que gastes en producto tienes que concienciar a tus empleados entrenándolos"; un segundo elemento que considera esencial es la compartición de inteligencia de la manera más sencilla posible; el tercer elemento importante es la monitorización a través del SIEM y el XDR, "que no deja de ser un SIEM por detrás pero desarrollado por cada uno de los fabricantes".

Como conclusiones señala que "hay que dar visibilidad, y cuanto más unificada mejor", que los fabricantes deben acompañar al cliente no sólo en la venta sino a posteriori ya que "podemos tener el mejor producto, pero mal instalado no sirve para nada" y que hay que fomentar la interoperabilidad entre fabricantes para que sea mucho más fácil la búsqueda de amenazas.