it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Abril 2021 - nº 40

BAS, la simulación de ataque al rescate

‘El cloud no se hace responsable de la seguridad’ (Toni García)

‘Yo protejo a la gente y los productos que protegen a todos los demás’ (Jony Fischbein)

‘Los IDS aún existen por una sola razón, y se llama checkbox’ (ExtraHop)

Monográfico. Tecnología y sanidad, la mejora en la atención al usuario

Revista IT Trends. Cloud, ¿hay opción? Viviendo la nube hibrida

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Directora	**Rosalía Arroyo** rosalia.arroyo@itdmgroup.es
Colaboradores	Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales	Contracorriente
Producción audiovisual	Favorit Comunicación, Alberto Varet
Fotografía	Ania Lewandowska

it Digital MEDIA GROUP

Director General Juan Ramón Melara	juanramon.melara@itdmgroup.es
Director de Contenidos Miguel Ángel Gómez	miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen Arancha Asenjo	arancha.asenjo@itdmgroup.es
Directora División Web Bárbara Madariaga	barbara.madariaga@itdmgroup.es
Director de Operaciones Ángel Porras	angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Las soluciones BAS (Breach and Attack Simulation) impulsan la seguridad proactiva

Con el crecimiento de la complejidad de los entornos empresariales y la naturaleza dinámica del panorama de amenazas, los equipos de seguridad no pueden confiarse. Tener la mejor solución en un entorno cambiante, híbrido, multicloud y deslocalizado no es garantía, ni siquiera tener, como así es, decenas de soluciones que tienen que interactuar y se flexibles. En 2017, Gartner acuñó el término Breach and Attack Simulation (BAS) para describir una nueva ola de tecnologías de prueba de controles de seguridad capaces de automatiza las capacidades de testing. Las soluciones BAS vienen al rescate porque ejecutan ataques simulados para determinar si los controles de seguridad detectan y responden a las amenazas como deberían, y luego informan sobre los resultados, ayudando a encontrar brechas de seguridad en una variedad de fuentes.

Entre los protagonistas de este número de IT Digital Security tenemos a Toni García Estopà, es el CISO y CIO de LETI Pharma, o a Jony Fischbein, el CISO de Check Point, a quien preguntamos qué retos tiene un responsable de ciberseguridad que tiene a su alcance la mayoría de las herramientas que necesita. También hablamos con Pilar Vila, una de las fundadoras de Forensics&Security, una compañía gallega dedicada a la consultoría, auditoría y análisis forense que asegura que a las empresas les interesa saber cuáles son sus puntos débiles.

Os contamos también cómo A10 ha evolucionado del mercado del ADC al de cloud y seguridad; cómo Varonis ha impulsado su negocio hasta desarrollar una de las plataformas de seguridad de datos más completas del mercado o cómo Extrahop está impulsando su propuesta de NDR (Network Detection and Response) como el Next Generation IDS.

Incluimos en este número una revista digital con información sobre cómo queda la nueva WatchGuard tras la compra de Panda Security con Carlos Vieira como protagonista; un monográfico sobre Tecnología y Sanidad y el último número de IT Trends, donde os resumimos lo más destacado del cloud Summit que celebramos a finales de Marzo.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

En Portada

BAS, la simulación al rescate

itds

Sumario

Actualidad

A10 Networks, del ADC on-premise al cloud y la seguridad

“Los IDS aún existen por una sola razón, y se llama checkbox” (ExtraHop)

Varonis lleva la detección y respuesta a la protección del dato

No solo IT

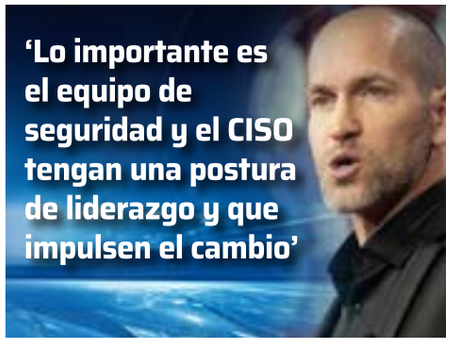
Ciberseguridad y alfabetización digital: El desafío de la diversidad y la inclusión

La realidad del mito del monopolio de las Big Tech

Entrevistas

‘El cloud no se hace responsable de la seguridad’

Toni García,
LETI Pharma



‘Lo importante es el equipo de seguridad y el CISO tengan una postura de liderazgo y que impulsen el cambio’

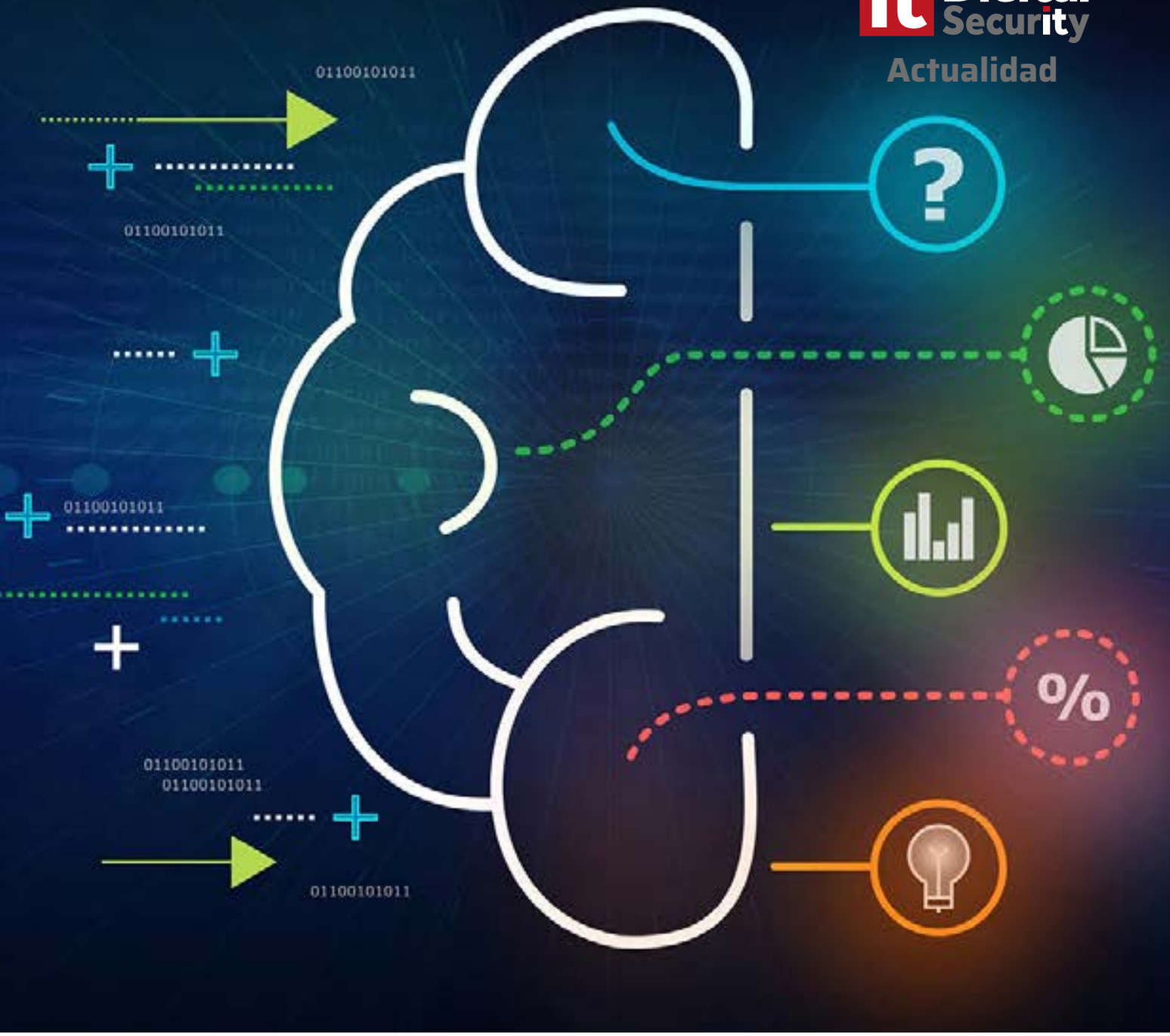
Jony Fischbein,
Check Point

‘Ha habido estafas millonarias con un phishing básico’

Pilar Vila,
Forensics&Security

Índice de anunciantes

Revistas Digitales



‘Los IDS aún existen por una sola razón, y se llama checkbox’

(ExtraHop)

Las redes son cada vez más complejas y distribuidas y por eso la visibilidad, antes importante, ahora es imperativa para poder detectar y detener las amenazas antes de que generen una brecha de seguridad. Aquí es donde entra en juego la detección o respuesta de red, o NDR (Network Detection and Response), una categoría de producto que tiene su origen en la detección de intrusiones en la red, la búsqueda de amenazas basada en la red y la investigación de incidentes; una categoría de producto en la que una empresa, ExtraHop, se abre camino con un mensaje: llega NDR, llega el Next Generation IDS.

ExtraHop es un proveedor de seguridad y monitorización de redes que en 2018 lanzó Reveal (x) una solución NDR, con la que ganó presencia en el mercado rápidamente. Dice también Gartner en su estudio Market Guide for Network Detection and Response que las capacidades de detección de ExtraHop aprovechan una combinación de técnicas, incluidos los controles basados en reglas y en la reputación, pero también combinan el aprendizaje automático supervisado y no supervisado para detectar anomalías y desviaciones de los comportamientos normales de la red.

Christian Buhrow, el responsable de ExtraHop en las regiones de DACH e Iberia, nos cuenta que los ataques avanzados son cada vez más inteligentes y complejos, y esto significa que “las herramientas que necesitas para detenerlos y para detectarlos también tienen que ser más complejas”. Añade el directivo que ha habido un cambio, una evolución tecnológica en las herramientas de seguridad que se utilizan en las empresas. Apunta a que desde hace más de diez años los SIEM han sido la única tecnología capaz de recoger datos de la infraestructura de las empresas, “de recoger esos log files y extraer sentido de ellos”; en cuanto a los antivirus, “no eran muy inteligentes, solamente podían detectar una firma de algún malware que ya era conocido” y no utilizaban análisis de comportamiento o de anomalías; del mismo modo los IPS o los IDS, “que tienen todas las empresas, no valen para mucho porque lo único que hacen es comparar firmas de ataques conocidos. Nunca van a poder detectar un ataque Zero Day”. Asegura Christian Buhrow que se necesita más y que la parte que te permite tener visibilidad total de lo que pasa en una empresa es el análisis de tráfico, “una tecnología que tiene cuatro o cinco años, muy novedosa, que se ha desarrollado mucho en los últimos dos, y que pocas empresas conocen”.

"El mensaje de NDR en España está más avanzado que en otros países como Suiza, Austria o incluso Alemania"

Christian Buhrow, ExtraHop

NDR, ¿sustitutos o complementarios?

Los NDR, ¿sustituyen alguna tecnología de seguridad que tiene las empresas, como los IPS o IDS, eliminando así parte del stack de seguridad que tienen las empresas? Empieza respondiendo

La estrategia a media plazo es que los NDR sustituyan a los IDS

Christian Buhrow que no sustituyen ni a los SIEMS ni a las soluciones de seguridad endpoint.

Las soluciones antivirus han evolucionado hacia lo que se conoce como EDR (Endpoint Detection and Response), soluciones más inteligentes, con conexión a la nube y, lo más importante, “añaden la parte de análisis de comportamiento y anomalías que le faltaban a los antivirus”. El NDR también es una evolución, “podrías denominarlo el Next Generation IDS, porque va mucho más allá”.

En el mundo del EDR, los nuevos jugadores del mercado están evolucionando su oferta de producto para, además de dar la solución de detección y respuesta, aportar también una solución de antivirus, que no por no ser avanzados han dejado de utilizarse porque, como se dice en el mercado “siguen parando mucha morralla”. La complejidad que tienen que afrontar los responsables

de ciberseguridad, que necesitan tanto el AV/AM como el EDR está haciendo que los fabricantes de antivirus tradicionales estén desarrollando EDRs (como es el caso de Bitdefender, Sophos, Trend Micro, Kaspersky, Panda… y tantos otros) y los fabricantes de EDR están añadiendo a su oferte un AV/AV, como es el caso de Crowdstrike. ¿Podemos suponer una evolución parecida en el mercado de visibilidad de red y que ExtraHop incluya en su oferta un IDS?

"Precisamente la compañía está a punto de lanzar una gran campaña hablando de Next Generation IDS", responde Christian Buhrow, añadiendo que "los IDS aún existen por una sola razón, y se llama Checkbox" y que la estrategia a media plazo es que los NDR sustituyan a los IDS.

Zero Trust + NDR = Zero Trust v.2.0

Está de moda ahora hablar de Zero Trust y de SASE (Secure Access Service Edge), un modelo y una arquitectura que buscan dar un nuevo impulso a la ciberseguridad. ¿Cómo encaja NDR en este tipo de conceptos? Dice el directivo de ExtraHop que a primera vista no parece haber relación porque el modelo Zero Trust se basa en dar acceso a la red únicamente a los usuarios, dispositivos o aplicaciones autenticados; "pero la debilidad de Zero Trust es que una vez que estás dentro del castillo te puedes mover y hacer todo lo que quieras", dice haciendo referencia al NIS SP 800-207, una recomendación de esta directiva para ampliar las capacidades de Zero Trust al advertir que "el Zero Trust como lo tenemos montado no es suficiente. Necesitamos también una monitorización continua".

"El Zero Trust como lo tenemos montado no es suficiente. Necesitamos también una monitorización continua"

Dice Buhrow que hasta ahora saber qué hacen esas identidades, aplicaciones o dispositivos una vez han sido autenticados "no ha sido un parte de Zero Trust", pero que esto es, precisamente, lo que hace ExtraHop: ver cada movimiento, ver exactamente qué hace cada dispositivo, cada usuario, qué hacen en cada momento, con qué aplicaciones trabajan, con quién comunican y qué transacciones se realizan dentro de la red. Es, en opinión del directivo, la versión 2.0 de Zero Trust

CON EXTRAHOP PUEDES SABERLO TODO

CLICAR PARA VER EL VÍDEO

ExtraHop en España

En España ExtraHop opera a través de Ingecom, su mayorista exclusivo con el que se trabaja en dos vías, por un lado educando el mercado, a los clientes, porque el NDR "es una tecnología novedosa", y por otra parte buscando integradores que se comprometan a trabajar con ExtraHop.

A estos integradores se le pide que entiendan que NDR "es una tecnología clave para el futuro", que "somos la mejor opción en este mundo del NDR", y que se comprometan a desarrollar mercado junto con nosotros.

Dice también Buhrow que el mensaje de NDR en España está más avanzado que en otros países como Suiza, Austria o incluso Alemania. La clave está en le red, asegura, añadiendo que las operadoras han hecho un buen trabajo en nuestro país.

Enlaces de interés...

- ExtraHop
- Las soluciones de Detección y Respuesta en la Red son tendencia
- NDR (Network Detection and Response), guía para principiantes

Compartir en RRSS

STORMSHIELD

PROTECCIÓN DE **INSTALACIONES INDUSTRIALES**

De amenazas dirigidas a estaciones de trabajo o provenientes de la red

www.stormshield.com

Varonis lleva la detección y respuesta a la protección del dato

Varonis ha entendido muy bien cuál es la necesidad de los clientes, ofreciendo una visibilidad y un control muy detallado sobre los datos almacenados de forma local y en la nube, monitorizando de forma transparente los sistemas críticos sin agentes de punto final.

De la seguridad reactiva a la proactiva. Esto es lo que ha hecho Varonis. De auditar y analizar a responder. La compañía ha sabido entender lo que necesitan los clientes, visibilidad, hasta desarrollar una de las plataformas de seguridad de datos más completas del mercado capaz de recoger y analizar los datos almacenados en la infraestructura de las compañías, incluidos los endpoints, para priorizar los riesgos en base a la sensibilidad, la exposición y la actividad de acceso. La plataforma protege los datos, detecta amenazas y responde en tiempo real.

La clave está en la visibilidad. Saber lo que pasa en las redes, lo que ocurre en los endpoints, lo que hacen los usuarios y donde están los datos y quién accede. Parece fácil, y obvio, pero no lo es tanto. “Venimos de la parte clásica de auditar una cabina a una plataforma de seguridad capaz de proteger los datos de toda la organización, que es otro paradigma, es otro escenario totalmente diferente”, dice Juan Luis Gosalvez, National Channel Manager de Varonis, una compañía que está evolucionando de proteger los datos a proteger la empresa digital porque “ya no nos basta auditar

Varonis no sólo ofrecen visibilidad de los datos, sino que es capaz de identificar el riesgo y, lo que es más importante, solucionarlo aplicando tecnología y automatización

Se ha pasado del poder que tenían los administradores al poder de compartir información que tienen los usuarios, y esto hay que hacerlo adecuadamente

los recursos, sino que tenemos que monitorizar los eventos que están teniendo lugar en tiempo real en toda la infraestructura de la compañía" para conseguir "la seguridad del propio dato a través de la automatización, la eficiencia y la generación de valor añadido".

Apunta su compañero Julián Domínguez, Sales Engineer de la compañía, que Varonis ha evolucionado para adaptarse a los problemas que tienen los clientes, como es el poder identificar quién puede acceder a una información, poder diferenciar la criticidad de la información en base al contenido o saber si ese acceso es lícito o no. Es más, la compañía cuenta desde hace un tiempo con un equipo de responsables de ciberseguridad que tienen la función "de ayudar a entender mejor cuáles son los ciberataques que están recibiendo nuestros clientes y ayudar a identificar, parar y a mitigar ese tipo de ataques", lo que significa que la compañía es capaz de ofrecer equipo de respuesta ante incidentes "que ayuda a los clientes a proteger mejor la información".

Destaca Juan Luis Gosalvez el concepto de plataforma única de seguridad. Explica que lo que hace Varonis es "monitorizar, controlar y reaccionar" a partir de lo que está sucediendo en todo el contexto para, aplicando machine learning, "entender qué es normal y qué no es normal entre el usuario y el dato en toda la infraestructura de la compañía". Para hacer todo esto, añade, "no basta con recolectar logs, sino que tenemos que monitorizar cada uno de ellos", y además trabajar de manera automática para ser eficientes y poder "quitar el ruido de lo que realmente es el foco importante de los ataques".

Menciona Gosalvez que la plataforma de Varonis es capaz de "controlar el flujo entre el usuario y el dato en los diferentes entornos y entender

2020 CYBER THREATS AND VARONIS INCIDENT RESPONSE

CLICAR PARA VER EL VÍDEO

"Varonis no está aquí para arreglar permisos, sino para reducir los riesgos de ciberseguridad"

Juan Luis Gosalvez, National Channel Manager Iberia, Varonis

cuál es la interacción entre los usuarios o las cuentas y los datos de la compañía". El perímetro de seguridad se desdibujó hace tiempo y parece haber desaparecido definitivamente con la pandemia. Lo que hay que proteger es el propio dato, ¿cómo lo hacemos? "entendiendo lo que está pasando a través del contexto, a través de la monitorización, y aplicando medias en tiempo real con el equipo de respuesta ante incidentes, con el machine learnign y el User Behavior Analytics, con la clasificación por regla, contenido y etiqueta de todos los datos".

Planteamos a los directivos de Varonis cuál es el reto al que se enfrentan las empresas cuando quieres proteger sus datos. ¿Saben qué datos tienen y dónde están? Responde Julián Domínguez que se parte de un modo de gobierno de los datos de hace 20 o 25 años en el cual los administradores de IT eran los que gestionaban los permisos y los accesos a los usuarios; "es decir, si tú no le pedías a un administrador que te diera acceso a una carpeta, no podías acceder a ella. A pesar de ello, más el 94% de las empresas que hemos auditado tienen el problema de no saber, no tener visibilidad, de quién accede a la información y si los permisos de acceso son correctos".

El tema no queda ahí, sino que ha empeorado, porque con la pandemia las exigencias se han relajado ante la necesidad de mantener la operativa de trabajo y el negocio online, y soluciones de colaboración como Teams ofrecen a los usuarios la capacidad que ellos decidan con quien pueden

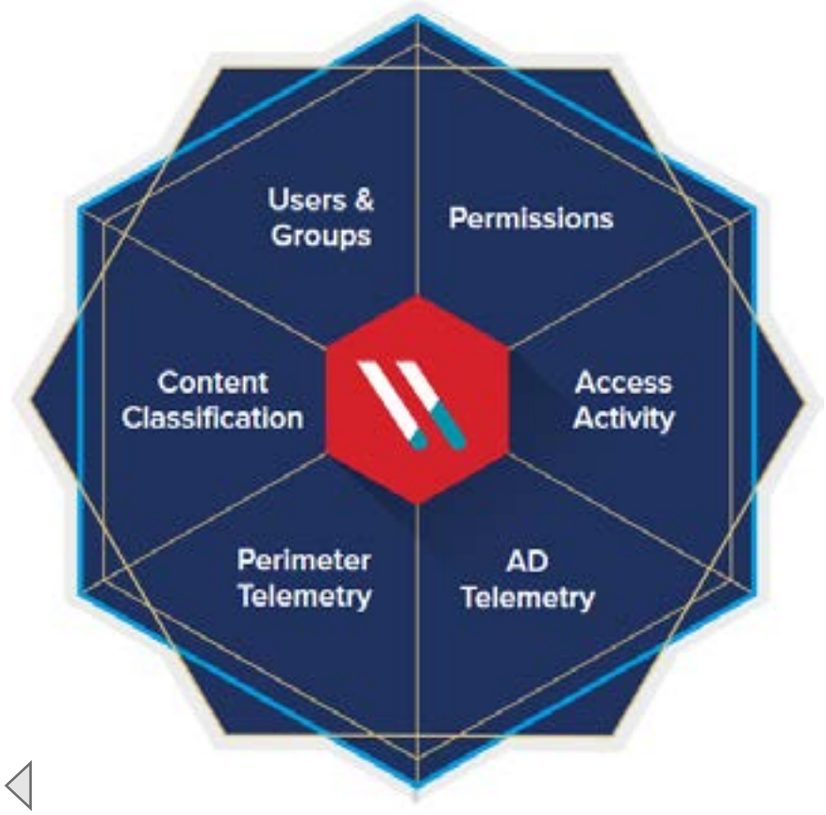
2021 DATA RISK REPORT. FINANTIAL SERVICES

Analizando datos de 4.000 millones de archivos en 56 organizaciones de servicios financieros, este estudio ofrece información sobre la seguridad de los datos de la industria financiera: banca, seguros e inversiones. Entre los datos aportados por el estudio destaca que un empleado de servicios financieros tiene acceso a casi 11 millones de archivos el día que entra por la puerta. Para las grandes organizaciones, el número es el doble: 20 millones de archivos abiertos para todos los empleados.

compartir información sin que tenga que intervenir ningún administrador de mi empresa.

Según Julián Domínguez hemos pasado “del poder que tenían los administradores al poder de compartir información que tienen los usuarios, y esto hay que hacerlo adecuadamente. Lo que hace Varonis es darte esa visibilidad”.

Una visibilidad que implicaría saber dónde está la información sensible en base a contenido, regla y etiqueta, qué grupos tienen acceso a ello y, con toda esa información, poder remediar el riesgo de acceso a esa información sensible. “Varonis no está aquí para arreglar permisos, sino para reducir los riesgos de ciberseguridad”, dice Juan Luis Gosalvez, explicando que si una empresa tienen ocho mil usuarios que tienen acceso a cinco millones de carpetas con información sensible, el riesgo de que una sola cuenta quede comprometida pone en riesgo cinco millones de carpetas con información sensible, y esto “es un riesgo de ciberseguridad que no ayudar a mitigar un PAM, ni un IRM, ni un DLP, ni un SIEM. La ventaja que te da Varonis es esa visibilidad, pero sobretodo la capacidad de arreglar esa situación de riesgo de manera automatizada, sin impactar en producción”.



De forma que la compañía no sólo ofrecen visibilidad, sino que es capaz de identificar el riesgo y, lo que es más importante, solucionarlo aplicando tecnología y automatización. La remediación automática y rápida de los problemas de los clientes es lo que está siendo clave, asegura Julián Domínguez.

Esta evolución tecnológica, ¿cómo ha impactado en el canal? “Lo que estamos buscando en el canal son partners que acompañen al cliente en este viaje de seguridad”, dice el director de canal de Varonis en España, quien añade que también deben capaces de dar el paso de estar de una manera reactiva, monitorizando o auditando una cabina como hace diez años a, de manera proactiva, estar analizando lo que está pasando en tiempo real, mitigando riesgos, dando reactividad en tiempo real sobre ataques a la infraestructura de la compañía. Esto supone contar con un canal más especializado capaz de liderar proyectos de seguridad dando la capa de servicios profesionales.

"La remediación automática y rápida que ofrece Varonis a los problemas de los clientes es lo que está siendo clave"

Julián Domínguez, Sales Engineer, Varonis

Enlaces de interés...

- Las aseguradoras dicen sí a cloud, pero les preocupa la seguridad de los datos
- La seguridad de los datos es la prioridad número uno para la transformación digital
- El mercado de soluciones para blindar big data se duplicará en cinco años

Lo que propone la compañía es dejar de lado las herramientas parciales e integrar todo en una única plataforma que sea eficiente, que sea potente y que sea escalable para responder a una situación que pasa porque los datos no dejan de crecer y las empresas han adoptado la continuidad negocio en una infraestructura híbrida donde cada trabajador es como una oficina que se conecta a diario a los recursos y genera datos.

Sobre la tipología de cliente, aunque el target es la gran cuenta, la compañía también da servicio a las pequeña porque en realidad, como afirma Juan Luis Gosalvez, “el core de negocio es proteger el dato, y hay empresas de cien usuario que manejan datos extremadamente sensibles”.

Sobre las previsiones de la compañía para este año se espera “una adopción masiva de la plataforma de seguridad de Varonis en las corporaciones”, porque si bien es cierto que cuando saltó estalló la pandemia hubo una fuerte inversión en continuidad de negocio, agilización de los puestos de trabajo… “luego se dieron cuenta de que estaban perdiendo el control del propio dato, por lo que creemos que las empresas van a apostar por una política de securización del dato desde el propio dato, lo que significa entender dónde está, entender quién accede, aplicar políticas de seguridad, de automatización y de eficiencia”.

Compartir en RRSS

S21SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

A10 Networks, del ADC on-premise al cloud y la seguridad

Los ADC, o controladores de entrega de aplicaciones, siguen siendo el core del negocio de A10 Networks, que avanza en el mercado de seguridad con una herramienta de inspección de tráfico cifrado y con una reconocida solución DDoS que se ofrecerá en modo SaaS.

En ocasiones resulta curioso bucear en la historia de las compañías, en su evolución, así como en la evolución del mercado, o mercados, en el que se mueve. Es el caso de A10 Networks. Resulta que esta compañía se fundó en 2004 ofreciendo una línea de productos llamada ID Series para la gestión de identidades, según Wikipedia. La compañía evolucionó con dos líneas de negocio, uno orientado a Enterprise centrada en la entrega de aplicaciones, y otra orientada al negocio con operadores. Justo en 2004 la primera generación de controladores de entrega de aplicaciones, o ADC (Application Delivery Controllers) empezaron a llegar al mercado como una evolución de los balanceadores de carga de servidor, convirtiéndose en poco tiempo en elementos críticos de la seguridad empresarial.

Dice Juan Asensio, country manager de A10 Networks para España y Portugal, que la compañía viene del mundo del hardware, “donde desarrolló

A10 Networks ha ido creciendo en el mercado de la seguridad con una solución de interceptación del tráfico SSL, A10 SSLi, que permite a las empresas saber si el tráfico cifrado que circula por su red es legítimo o no

un porfolio de soluciones enterprise centrado en mantener las aplicaciones e infraestructuras de negocio de los cliente siempre disponibles y seguras, mediante las tecnologías de entrega de aplicaciones ADC, de interceptación de tráfico SSLi y de mitigación de ataques DDoS". En cuanto al negocio centrado en los operadores, trataba de facilitarles a los mismos la transición del mundo IPv4 al mundo IPv6.

De forma que A10 Network es, claramente, un jugador destacado del mercado de ADC, pero con la evolución de este mercado a la nube y el declive de las soluciones locales, la empresa se está expandiendo al área de seguridad, donde entra en competencia con otros jugadores mejor posicionados y donde mantiene la rivalidad de otros players del mercado del ADC, como F5 Networks, que por cierto está siguiendo la misma estrategia.

Es en 2012 cuando la compañía aterriza en España sin referencias. Hoy se trabaja con 300 clientes pertenecientes a todos los verticales, "desde administración pública, grandes empresa del IBEX, operadores, hosters, etc.". Explica Juan Asensio que la consolidación de la compañía en el mercado español se ha hecho gracias a los ADC, "donde la propuesta de valor de A10 se asienta en disponer de una solución de altas prestaciones que incluye todas las funcionalidades y sin que haya sorpresas en la renovación de los soportes".

La compañía ha ido creciendo en el mercado de la seguridad con una solución de interceptación del tráfico SSL, A10 SSLi, "que permite a las empresas saber si el tráfico cifrado que circula por su red es legítimo o no". En cuanto a la propuesta anti DDoS, explica el directivo que a partir de 2019 estas soluciones se adaptaron al segmento de empresas "y comenzamos a comercializarlo en modo servicio, orientándolo a la protección tanto de las infraestructuras como a los ataques DDoS de baja intensidad".

Recuerda Juan Asensio que las soluciones anti DDoS surgen en 2016 a partir de un encargo de Microsoft, que es uno de los principales clientes del producto DDoS de A10, para proteger la línea de productos en la nube Azure de la empresa y su producto Office 365. A10 Networks ha ido

evolucionando su producto, muy orientado actualmente a compañías que “quieren dar sus servicios a otros clientes en modo servicio, y muy orientado también a empresas que disponen de recursos online”, siendo clientes de A10 las principales compañías de juegos del mundo. La solución de anti DDoS se ha ido adaptando al mercado Enterprise, se ofrece en modo servicio y el negocio se está desarrollando en la región de Iberia.

Por otra parte, A10 Networks está muy presente en el segmento operador. La compañía participó en las últimas ediciones del Movile World Congress “donde presentamos nuestra evolución de la solución CGN hacia la seguridad convergente de altas prestaciones para entornos 4G y 5G”.

Impacto del cloud

El movimiento hacia el cloud y hacia propuestas de infraestructura como servcicio (IaaS) que adoptaron muchos clientes de A10 Networks, impactó en el negocio de esta última, que supo moverse conforme a las necesidades del mercado para convertir su sistema operativo ACOS (Advanced Core Operating System) en una solución clod ready, lo que permite “que nuestros clientes se puedan moverse a la cloud sin problema y

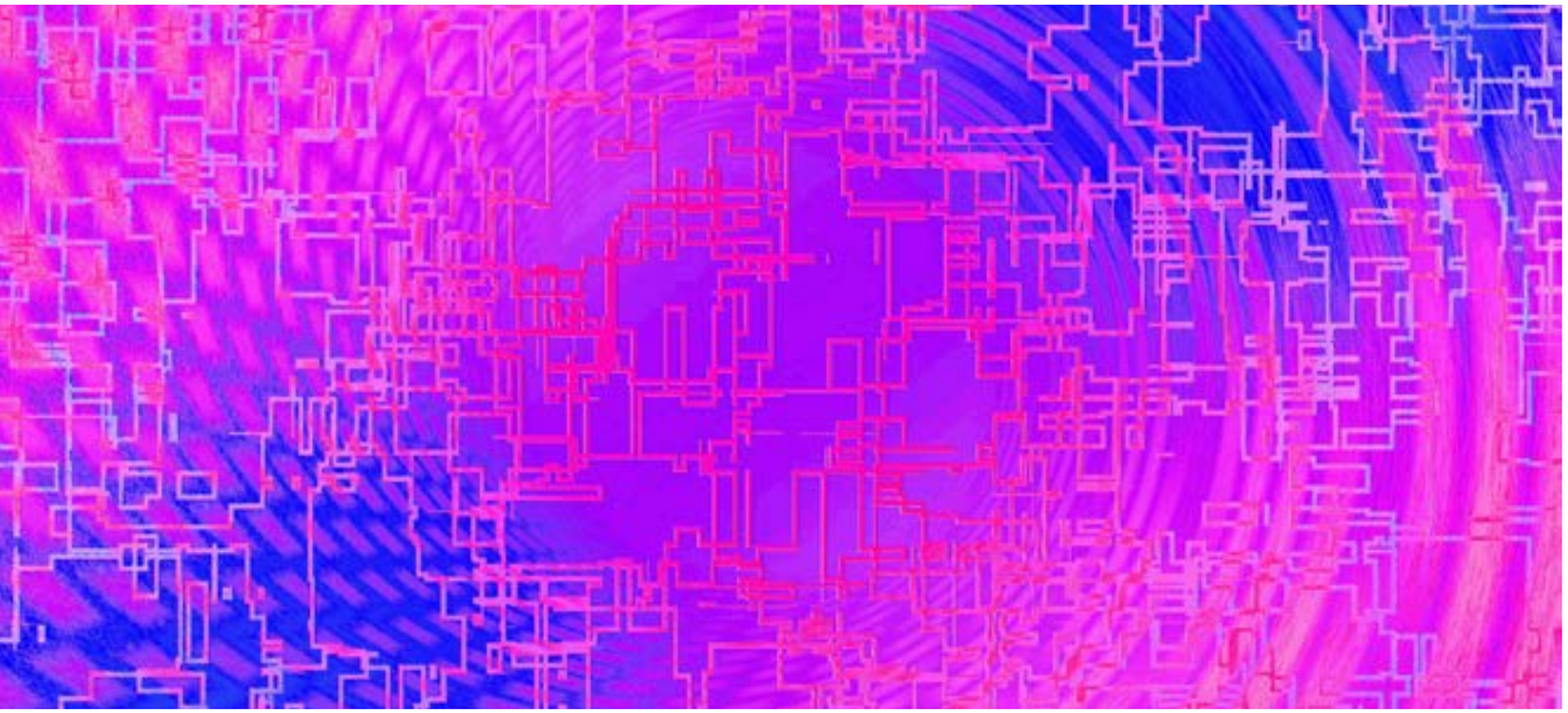
Dhrupad Trivedi, el nuevo CEO de la compañía, está cambiando A10 desde dentro, optimizando procesos para hacer A10 más eficiente y más orientada a la venta de soluciones

tendrían un sistema homogéneo entre todas las clouds que quieran utilizar, de forma que la disponibilidad y entrega de las aplicaciones estaría unificada bajo una plataforma multicloud con disponibilidad para desplegarse en distintos entornos de una forma sencilla". A esto se le suma una gestión basada en este concepto capaz de mostrar "dónde están corriendo las aplicaciones, los tiempos de respuesta en cada una de los cloud… de una forma visual muy gráfica y dándote un valor muy importante a la hora de definir cómo es la experiencia del usuario".

Como muchos otros fabricantes de TI/seguridad, la plataforma se ha convertido en el elemento clave. En un mundo multicloud e híbrido, la plataforma de la compañía evita que los responsables tengan que preocuparse por saber del balanceador, del SSL o de cualquier otro dispositivo de seguridad que tiene en cada una de las nubes, sino que a través de una plataforma homogénea lo puede gestionar todo de manera uniforme. Este se puede hacer, explica Juan Asensio, a dos elementos, por un lado los equipos virtuales, que se pueden desplegar en las nubes que decida el cliente de una manera ágil y después con una herramienta de visibilidad y gestión que es capaz de desplegar de forma automática todos estos todos estos servicios en las cloud que designe el cliente.

Nuevo CEO

En noviembre de 2019 se anuncia el nombramiento de Dhrupad Trivedi como nuevo CEO de la compañía en sustitución de Lee Chen, fundador de A10 Networks y CEO de la misma desde sus inicios. La noticia es muy bien recibida por un mercado en el que algunos analistas aseguraron en su momento



"Queremos que el canal siga siendo el motor del crecimiento y consolidación de la compañía en la región"

Juan Asensio, Country Manager Iberia, A10 Networks

que “la compañía tiene productos de primera categoría” pero que no “había tenido una estrategia clara de comercialización bajo Lee Chen”, sobre el que también se ha comentado que si bien es un excelente innovador de productos, no estaba orientado a las ventas y las operaciones. Dhrupad Trivedi llegaba a A10 con una gran experiencia en Belden, con una facturación de dos mil millones de dólares anuales, o JDS Uniphase.

Sin entrar en comentarios, asegura Juan Asensio que “sin duda alguna Dhrupad está cambiando A10 desde dentro, optimizando procesos para hacer A10 más eficiente, y más orientada a la venta de soluciones”. Bajo el liderazgo de Dhrupad se han impulsado dos acuerdos importantes con Ericsson y Dell Technologies. El primero convierte a A10 en el firewall de Ericsson para su packet core para impulsar la seguridad en redes 5G en el segmento de operadores; con Dell se firma un acuerdo de

Appcito, el poder del ‘cloud native’

Durante su larga carrera A10 Networks solo ha realizado una adquisición, la de Appcito en julio de 2016. Sin desvelar los detalles financieros del acuerdo, la compra permitía a la compañía cumplir con su visión de convertirse en un proveedor de controladores de entrega de aplicaciones (ADC) nativo de la nube.

El servicio Cloud Application Front End (CAFE) nativo de la nube de Appcito, que se integraría en la arquitectura Harmony de A10, unificaba los servicios de entrega de aplicaciones, incluido el equilibrio de carga, la seguridad de las aplicaciones, la implementación continua, la optimización del rendimiento y los análisis de aplicaciones necesarios para entregar aplicaciones tradicionales y basadas en microservicios.

partnership que permite a Dell revender toda la línea de productos se seguridad para multi-cloud y 5G,incluidos los Application Delivery Controllers (ADCs), Carrier-Grade Networking (CGN), Convergent Firewall (CFW), SSL Insight (SSLi) y A10 Harmony Controller. Ambas, tanto Ericsson como Dell Technologies, ajustaron sus productos para desarrollar una solución final sólida, lo que ha puesto de manifiesto el compromiso con la relación.

A10 Networks y en canal

En España A10 Networks trabaja "por y para el canal", asegura Juan Asensio, añadiendo que con la ayuda de V-Valley, su mayorista, "queremos que el canal siga siendo el motor del crecimiento y consolidación de la compañía en la región". La relación con el canal se basa en tres pilares básicos, como es "la cercanía y apoyo al canal para que todas las oportunidades de negocio que llegan se conviertan en proyectos con un buen margen"; añade Asensio que otro pilar importante es "la formación continua, tanto de las soluciones de A10 como de las herramientas que permitan tener el conocimiento más profundo de la tecnología de A10 y desarrollar servicios entorno a las soluciones la compañía"; por último, aboga el directivo por "la cercanía al cliente final para proporcionar la mejor experiencia de uso posible con la tecnología de A10".

Para este año las previsiones son "seguir creciendo tanto en nuevos clientes como con nuestros clientes mediante la continua capacitación de nuestro canal", asegura juan Asensio, que también prevé un crecimiento de nuevos productos, como puede ser en DDoS as a Service o la proyección a entornos hibridos multi-cloud con nuestras solucines cloud-ready de ADC y seguridad.

Enlaces de interés...

- La seguridad se convierte en requisito previo dentro de las estrategias de TI
- INCIBE gestionó más de 133.000 ciberincidentes en 2020

Compartir en RRSS

SECURE ACADEMY

TU CENTRO AVANZADO DE FORMACIÓN EN CIBERSEGURIDAD

www.secureacademy.es

Secure&IT

Toni García Estopà es el CISO y CIO de LETI Pharma, una empresa con más de cien años de historia; antes lo fue de Damm, otra empresa centenaria que tenía las mismas necesidades: poner freno a los ciberdelincuentes. Tiene este directivo las ideas claras cuando dice que estandarizar los problemas es una buena manera para poder solucionarlo; que hay un abismo entre un EDR y un antivirus; que es importante que aparezcan palabras, como SASE, que definan conceptos y los estandaricen, o que el servicio gestionado es el modelo de revolución industrial dentro de la seguridad que se vivió a principios del siglo anterior.

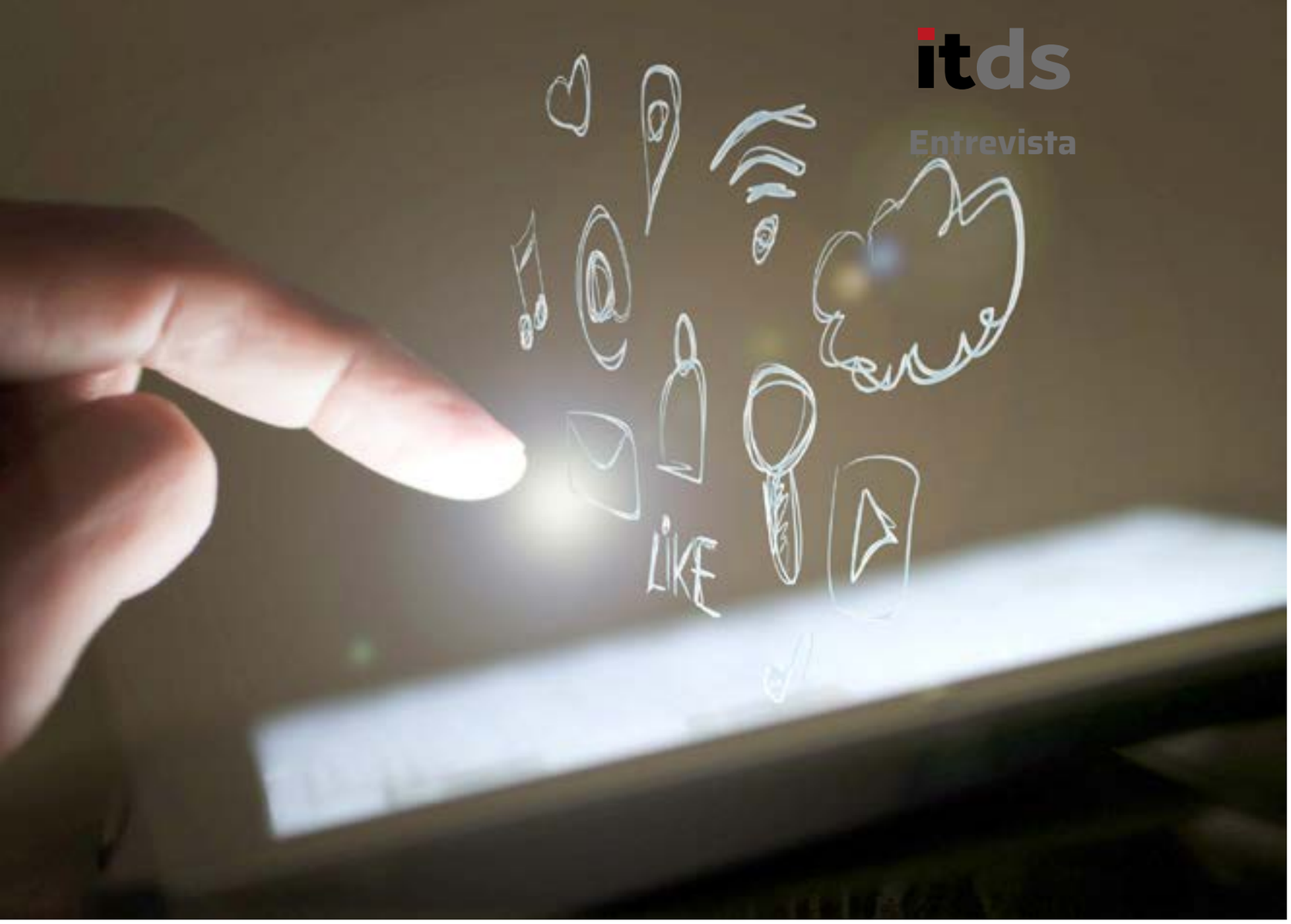
Rosalía Arroyo

‘El cloud no se hace responsable de la seguridad’

(Toni García, LETI Pharma)

La figura del CISO ha evolucionado muchísimo, asegura Toni García. “Hemos pasado de ser una figura que estaba muchas veces dentro del departamento de redes, debajo del de sistemas o dependiendo de finanzas”, a ser una figura que está en el comité de dirección y reporta directamente a la presidencia de la compañía. Esta nueva situación, que es una realidad para el CISO de LETI Pharma, no es lo habitual. Asegura el directivo que los responsables de ciberseguridad de las empresas “estamos cogiendo más peso” y que algunos cambios, como el Real Decreto 43/2021 sobre la seguridad de las redes y sistemas de información que especifica que es necesaria la figura del CISO, o responsable de seguridad, en las infraestructuras críticas o proveedores esenciales, están también ayudando. Por otra parte, si bien el papel del CISO ha evolucionado mucho en los últimos 15 años, aún le queda mucho por evolucionar.

La pandemia también ha sido un impulsor de la figura y el valor del CISO. Explica Toni García que una de las cosas que normalmente la gente de seguridad suele estructurar/plantearse es que no sólo hay que tener en cuenta los problemas del día a día, sino hay que tener una visión amplia de cosas que pueden pasar “y el de la pandemia es un escenario que yo había planteado en muchas



"La ciberseguridad es un problema que no vamos a poder solucionar si no puedes ir a otros países a buscar a los ciberdelincuentes"

ocasiones, aunque no con este alcance. Esto ha hecho ver a los CEOs que hay una cierta preparación a riesgos del que no eran conscientes". Continúa diciendo el CISO de LETI Pharma que esta percepción ha llevado a que muchos de los planes que se habían hecho con anterioridad "estén ganando peso e importancia".

La empresa española está más sensibilizada hacia la ciberseguridad, "pero no del todo", dice Toni García, añadiendo que se sigue viendo como un gasto y que esto tiene mucho que ver con el desconocimiento; "no es fácil pedirle a alguien que visualice una arquitectura de red, o un modelo de gestión de aplicaciones y que se den cuenta de que, igual que debe haber un control de acceso a la entrada del edificio, tiene que haber controles de acceso a la red", asegura.

Tiene que ver esto con el cambio del discurso que hace años que se le pide a los CISOs. Reconoce Toni García que "nuestro lenguaje ha tenido que cambiar", pero que al mismo tiempo se ha tenido que aceptar "porque es un lenguaje que ahora hablan los hijos de los CEOs". Añade que el cambio importante ha sido el hecho de que no sólo los responsables de seguridad han tenido que modular su lenguaje y acercarlo más a negocio, sino que negocio también tiene que entender un poco el lenguaje de seguridad "porque ya no es un tema solo mío, es un tema de gestión de riesgos corporativos. A lo mejor no saben utilizar las palabras concretas, pero saben que estas palabras son importantes".

Siglas para estandarizar

En un mercado tan saturado de fabricantes, de soluciones y de propuestas, ¿cómo se puede escoger? "Básicamente hay un factor que es que es crítico, que es el de toda la vida, y es el boca a boca. No es ninguna novedad que hablamos entre nosotros y evidentemente las experiencias, buenas y malas, son muy importantes, porque si no es imposible verlas todas, hablar con todo el mundo y entender la realidad de cada una de las herramientas", dice Toni García.

"A todos nos gustaría tener un SOC, pero es un servicio caro y complejo porque necesitas a alguien que lo gestione"

Otra peculiaridad de este mercado, no exclusiva del mismo, es la pasión por las siglas. Si hace unos años se hablaba del NGFW, ahora es el EDR, o el XDR, o SASE. ¿Os lo tomáis con humor, preocupación o con ganas de aprender algo nuevo? Asegurando que "muchas veces no es un modelo nuevo" dice este directivo que "es importante que aparezcan palabras que definan conceptos y los estandaricen". Añade que muchas veces las consultoras han visto que en muchas empresas la preocupación era la misma y cada uno lo abordaba de una manera distinta y le ponía un nombre distinto, "y cuando hablaban entre ellas no eran capaces de darse cuenta de que estaban hablando del mismo problema. Estandarizar los problemas es una buena manera para poder solucionarlos", dice Toni García.

Servicios gestionados y cloud

"Para mí son imprescindibles los servicios gestionados porque no todos somos grandes compañías con presupuestos muy grandes", asegura el CISO de LETI Pharma. Añade que "el servicio gestionado es el modelo de revolución industrial dentro de la seguridad que se vivió a principios del siglo anterior. Es decir, tú no puedes ser una empresa que lo haga todo, no puedes tener todo el expertise dentro de tu casa" y eso significa que necesitas externalizar, sobre todo en un entorno que cambia muy rápido, en el que las tecnologías se mueven muy rápido. Dice también Toni García que lo importante es saber "qué tiene sentido externalizar y cómo juegas con la pérdida de conocimiento que esto puede suponer".

A la hora de elegir un proveedor de servicios gestionados, ¿también funciona el boca a boca o se espera algo más? Evidentemente hay un proceso, dice el directivo de LETI Pharm; explica que ese 'boca a boca' te ayuda a decidir a quién metes en la coctelera, pero que es importante que los proveedores de servicio de seguridad gestionados "aterricen los temas" y "se profesionalicen".

¿Cómo se afronta el riesgo de seguridad que generan los empleados? Para Toni García lo más importante es la formación y concienciación de los usuarios, "pero es verdad que esperamos que hagan las cosas de una cierta manera, y eso no es siempre posible". Dice que los usuarios utilizan la tecnología de la manera que creen conveniente y, "o les has marcado un camino muy cerrado, que eso no es adecuado porque encorsetas mucho la organización, o tienes que asumir que lo pueden hacer de una manera que tú no habías planteado" y lo que debe hacerse es formar a esos usuarios lo máximo posible y estructurar las herramientas a su alrededor. "No podemos asumir que sepan lo mismo que nosotros", asegura el directivo.

Sobre el cloud comienza diciendo Toni García que "migrar al cloud es más fácil de lo que parece", pero que si esa migración no está bien definida de partida "cuando vas allí, todo el mundo se olvida de la seguridad", y que lo hay que tener claro es que "el cloud no se hace responsable de la seguridad". Llegados a este punto plantea el directivo que, si eres una empresa tardía, que has visto lo que le ha pasado a los demás, la seguridad se plantee de base; si has sido de las que han migrado al cloud sin ese

conocimiento previo, seguramente seas de las que están teniendo un problema con la adopción de la seguridad en el cloud “porque no se gestiona de la misma manera”.

Tecnologías imprescindibles

Preguntamos a Toni García qué tecnologías o servicios cree que deben ser imprescindibles para la seguridad de una empresa. Comienza señalando que al conocer las amenazas lo primero que se necesita es una monitorización y respuesta; “a todos nos gustaría tener un SOC, pero es un servicio caro y complejo porque necesitas a alguien que lo gestione”.

Metiéndonos de lleno en las tecnologías menciona que hay algunas “fantásticas”, como UBA (User Behavior Analytics), o el EDR; “hay un abismo entre un antivirus y el EDR”, asegura. Pero advierte al mismo tiempo que no se debe asumir que “como tengo un EDR no me hace falta nada más”.

Sin identificarla como importante o imprescindible, pone foco Toni García en “una tecnología que realmente estuviese basada en la identidad y no tanto el concepto de perfilado. Es decir, que me diera igual si estás en un ordenador, un móvil o una Tablet, que me diera igual dónde estés… que cuanto yo sepa que tú eres tú pueda asegurarme de que te aplico toda la seguridad que necesitas”.

Añade que el cloud nos va a llevar hacia este concepto “porque eso cambia mucho la manera en consumir servicios”. Si la clave es la identidad el usuario tendrá una capacidad infinita de acceder a

"No puedes tener todo el expertise dentro de tu casa y eso significa que necesitas externalizar, sobre todo en un entorno que cambia muy rápido"

sus servicios, “y la única manera que tengo de restringirlo es asegurando que quien accede es quien dice ser, y a partir de ahí da igual si lo hace desde un dispositivo u otro, siempre con las medidas adecuadas”.

Apurando los últimos minutos de la entrevista con Toni García le pregunto si espera algún cambio significativo en 2021. Comenta que la ley es obsoleta desde el punto de vista de que la tecnología no tiene fronteras, y la seguridad que hay que aplicar a esa tecnología no tiene fronteras; la ley, asegura, no se ajusta a la realidad. Y lo que espera este directivo es que, en algún momento, alguien encuentre la fórmula para adaptar esas normas obsoletas. La ciberseguridad, dice, es un problema que no vamos a poder solucionar si no puedes ir a otros países a buscar a los ciberdelincuentes que siempre atacan desde los mismos sitios.

Enlaces de interés...

- ‘El IoT es el principal dolor de cabeza en el sector sanitario’ (Josep Bardallo, CISO Recoletas Red Hospitalaria)
- ‘SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección’ (Carlos Manchado, Naturgy)
- ‘El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad’ (Elena García, Indra)
- ‘En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar’ (Jesús Alonso Murillo, Ferrovial Servicios)

Compartir en RRSS

Descarga este **documento ejecutivo** de itRESEARCH

NUEVO INFORME

‘Lo importante es que equipo de seguridad y el CISO tengan una postura de liderazgo y que impulsen el cambio’

(Jony Fischbein, Check Point)

Los responsables de ciberserguridad de las empresas no solo tienen que hacer frente a los ciberdelincuentes o a las amenazas internas de una compañía. También tienen que pelear por una partida presupuestaria que les permita hacer su trabajo lo mejor posible, y tener que decidir entre las, literalmente, decenas de soluciones y propuestas que hay en el mercado, y eso por cada una de las capas de seguridad que se quieran aplicar. Estos no son precisamente los retos a los que se enfrenta Jony Fischbein, quien lleva 18 años en Check Point, los últimos dos como CISO, a cargo de todos los activos digitales de la compañía, combatiendo los ataques avanzados, y como Jefe de Privacidad de los clientes, partners y empleados de la compañía. ¿Cuáles son los retos del CISO de una compañía que fabrica productos de seguridad?

Reconoce Fischbein que para un CISO común el tema del presupuesto y las herramientas supone "un gran desafío porque el presupuesto no crece cada año y con la misma dinámica que crecen y cambian los ciberataques cibernéticos", a lo que se añade el desafío de la falta de profesionales que limita las opciones de este sector pero que al mismo tiempo está impulsando la automatización y todo lo relacionado con el machine learning.

El 85% de las soluciones que utiliza Jony Fischbein son de la marcha Check Point, pero no considera este directivo que esto signifique que se eliminen los problemas. El coste es alto si se tiene en cuenta la gran responsabilidad que conlleva la complicada labor de testear en producción los últimos productos y versiones de las soluciones que la compañía lanza al mercado. Es algo que, reconoce, "hay que saber manejar, especialmente con la gente de desarrollo y con la de Quality Assurance", que son los encargados de comprobar que se cumplen las expectativas del usuario que va a utilizar dicho producto.

"Lo más importante es que los CISOs tienen un gran poder para hacer cosas buenas, para hacer cambios y revoluciones internas"

Tener a su disposición una amplia oferta que cubre desde el endpoint a la red o la seguridad del cloud no significa que Jony Fischbein no tenga que hacer frente a un presupuesto; “cuando yo pido más personal, la compañía me da más productos”, reconoce sonriendo.

Que el 85% de los productos de seguridad que utilizas sean de la misma marca también le ahorra al CISO de Check Point el tener que buscar y probar soluciones de diferentes colores y sabores. Pero el reto sigue estando, e incluso acrecentado, porque hay que dar el doble de explicaciones, a favor y en contra, cuando se propone la adquisición de una solución de seguridad externa.

El reto más grande, dice, es que un problema de seguridad impacte en Check Point. “Yo protejo a la gente y los productos que protegen a todos los demás”, exclama el directivo en un momento en que las empresas de seguridad se han convertido en el foco de los ciberdelincuentes. Asegura Fischbein que durante la crisis de SolarWinds a consecuencia del ataque de suministro sufrido, se ha visto cómo los grupos que trabajan para agencias de inteligencia que están detrás de los estados nación están

invirtiendo en lanzar ofensivas contra empresas que tienen como clientes a agencias o empresas importantes de Estados Unidos. Son ya unas cuantas las empresas de seguridad que se han visto afectadas por el ataque de SolarWindows, un problema que ha despertado tanto recelo que en Check Point “hemos levantado cada baldosa para comprobar que no hay nada problemático”.

Un año después de la pandemia, ¿qué han aprendido los CISOs? “Lo más importante es que los CISOs tiene un gran poder para hacer cosas buenas, para hacer cambios y revoluciones internas, para mejorar las normas de trabajo implementando políticas y tecnología”, asegura Jony Fischbein, añadiendo que, en todo caso, el que ha liderado la transformación digital durante el último año no ha sido el CISO, ni el CIO, ni el CEO, sino COVID-19. “Lo importante es el equipo de seguridad y el CISO tengan una postura de liderazgo y que impulsen el cambio, como es el trabajo remoto de forma segura, acceso remoto y seguro a activos críticos de la empresa, o temas de soluciones de colaboración”, explica.

"Yo protejo a la gente y los productos que protegen a todos los demás"

Seguimos hablando de la situación sanitaria y de su impacto. Dice Jony Fischbein que, sin entrar en el debate de si el CISO tiene que reportar el CIO, o al CTO… “el CISO tiene que estar más cerca del CEO; el CISO es un aliado del CEO”. Añade que la pandemia sanitaria ha puesto en valor el papel de los equipos de seguridad para sobrevivir a este entorno “y el poder que tienen para mejorar y para cambiar cosas”.

Al margen del impacto directo que ha tenido en el trabajo de los responsables de TI y seguridad, la pandemia ha cambiado muchas otras cosas. Cambió nuestra forma de vivir y nuestra forma de trabajar, y los ciberdelincuentes pronto se hicieron cargo de este cambio que provocaba el acceso a las empresas desde redes WiFi no seguras, que los equipos se compartieran con diferentes miembros

"Cuando yo pido más personal, la compañía me da más productos"

de la familia, que el BYOD se disparara o que se perdiera visibilidad ante la dificultad de monitorizar las redes que utilizaban los empleados.

En todos estos procesos, muchos de los cuales ocurrieron casi de la noche a la mañana, pudieron cometerse errores y es ahora, recuerda el CISO de Check Pint, es cuando se está comprobando que los cambios que se hicieron, se hayan hecho de una manera efectiva desde el punto de vista de la seguridad. Otro impacto de la pandemia fue en la tipología de los ataques. Apunta Jony Fischbein que la compañía arrancó el 2020 pensando en unos tipos de ataques, "y de repente cambiaron", y hubo que hacer frente a un incremento de los ataques de phishing o de ransomware.

¿Cuáles crees que deben ser las medidas de seguridad mínimas que debe tener una empresa? Empieza diciendo el CISO de Check Point que hoy en día no es suficiente tener seguridad con un único producto; "es una unificación entre seguridad endpoint, Gateway network, mobile y cloud. Son muchas piezas de ajedrez que van juntas y tenemos que asegurarnos que trabajan en un ecosistema".

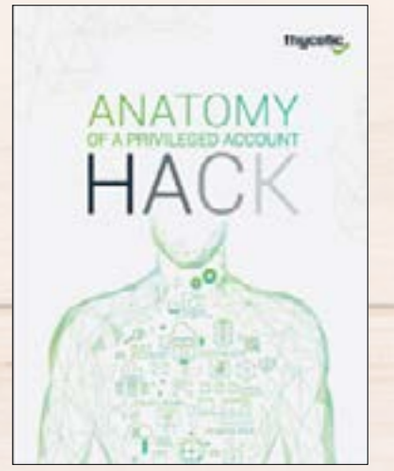
Enlaces de interés...

- 'El IoT es el principal dolor de cabeza en el sector sanitario' (Josep Bardallo, CISO Recoletas Red Hospitalaria)
- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)
- 'En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar' (Jesús Alonso Murillo, Ferrovial Servicios)

Compartir en RRSS

La documentación TIC, a un solo clic

Anatomía del ataque a una cuenta privilegiada



Este documento técnico realizado por Thycotic describe un ataque a una cuenta privilegiada; explica cómo los atacantes externos o los internos malintencionados pueden explotar las vulnerabilidades utilizando ejemplos como la contraseña de una cuenta de correo electrónico comprometida que se convierte en una violación total de la seguridad de la red.

7 consejos para proteger los datos de tu empresa y vencer al ransomware

La pérdida de datos no es una broma. Los ataques de ransomware y malware van en aumento, pero ése no es el único riesgo. Con demasiada frecuencia, las empresas piensan que sus datos están bien respaldados, pero en realidad no lo están. Este documento de Commvault muestra siete razones comunes por las que las empresas pierden datos, a menudo porque nunca estuvieron realmente protegidos, junto con consejos para ayudarte a evitar que te ocurra lo mismo.

Cloud Migration: Apuesta por el futuro de tu organización en la nube

En tiempos de incertidumbre, la migración a cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y lugar. Este documento de Making Science recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

Guía para implementar una CDN moderna

Este documento de Fastly señala la evolución de la relación de los desarrolladores con la CDN (Red de Distribución de Contenidos) y explica por qué las CDNs tradicionales están obsoletas. El texto también detalla los beneficios que pueden aportar las CDNs modernas, que van desde una mejor visibilidad de los patrones de tráfico hasta el diseño de APIs que potencian una experiencia de usuario personalizada.

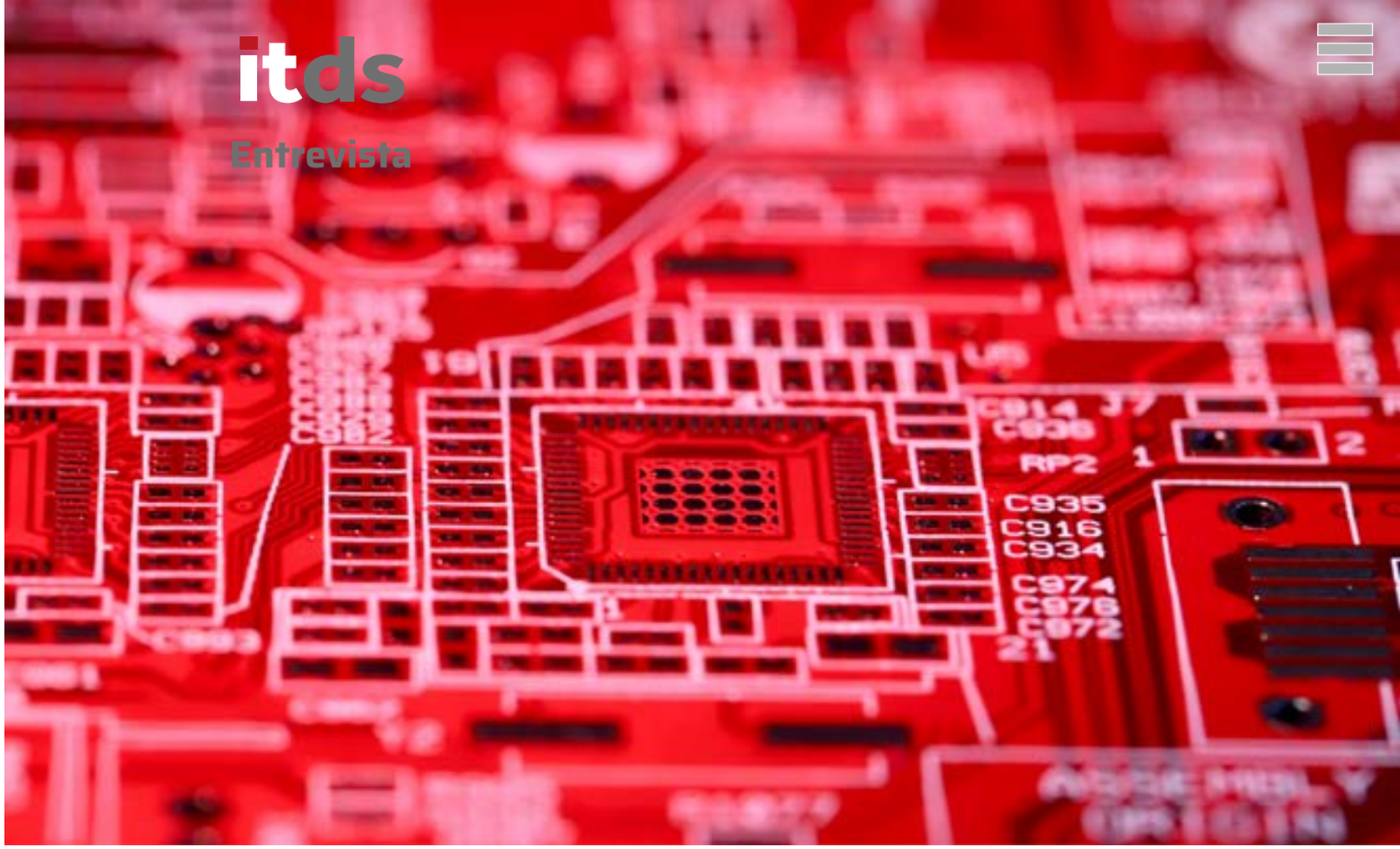
“Ha habido estafas millonarias con un phishing básico”

(Forensics&Security)

Pilar Vila es una de las fundadoras de Forensics&Security, una compañía gallega dedicada a la consultoría, auditoría y análisis forense que asegura que a la empresa le interesa saber cuáles son sus puntos débiles; que las empresas siguen siendo reactivas, y no proactivas, frente a la seguridad; que el profesional tiene mucha responsabilidad en su aprendizaje; que hay determinadas empresas que no se pueden permitir no tener un EDR y que incluso las empresas más pequeñas tiene que empezar a separar presupuesto para seguridad.

Rosalía Arroyo

Los avances en las tecnologías han intensificado la sofisticación de los ataques a dispositivos digitales. La mayoría de las actividades de transacciones comerciales y personales se realizan de forma electrónica, en las que las transacciones se realizan a través de correos electrónicos y los datos confidenciales se guardan en libretas de direcciones personales y discos duros. La identificación, preservación, recopilación, análisis y presentación de informes sobre las pruebas encontradas en dichos dispositivos se denominan análisis forense informático, un mercado que según la firma de investigación MarketsandMarkets crecerá una media anual del 15,9% hasta 2022, cuando se espera que genere 9.680 millones de dólares de ingresos. Forensics&Security es una compañía gallega que dedica gran parte de su tiempo a hacer “mucho forense en incidentes de seguridad”. Nos lo cuenta Pilar Vila, CEO y con-fundadora de la compañía junto con Ignacio Díaz, CTO, y Jaime Vila, que ocupa el cargo de CIO.



"La clave es mantener la cadena de custodia por si hay que ir a juicio"

Explica Pilar Vila que entre otras cosas su compañía realiza las tareas de respuesta al incidente y el forense posterior para investigar cómo se produjo el incidente, "porque a la empresa le interesa saber cómo entraron para ver sus puntos débiles, si siguen dentro y si exfiltraron datos". Insiste Pilar Vila en que lo principal es saber si hubo exfiltración de datos porque ahora "extorsionan mucho"; extorsionar está de moda entre los ciberdelincuentes, quienes desde hace un tiempo han dado una vuelta de tuerca a sus demandas amenazando con publicar la información robada, lo que no sólo puede generar un duro impacto de cara al cumplimiento de GDRP, sino también en las estrategias empresariales al quedar sus planes o investigaciones a disposición de quien las quiera ver. De forma que saber a ciencia cierta si ha habido una exfiltración de datos se convierte en algo fundamental.

"Llevamos tiempo haciendo respuesta ante incidentes, pero no tanto como tenemos ahora", dice Pilar Vila, añadiendo que desde que empezó el COVID los incidentes y las estafas se han disparado, así como asuntos de competencia desleal a nivel empresarial. El teletrabajo ha reducido el control sobre los empleados y eso ha hecho que este tipo de asuntos se haya disparado. "Siempre hemos llevado mucha competencia desleal en empresa. Quizá el 90% de nuestras peticiones de empresas es competencia desleal, casi siempre de un empleado de dentro, normalmente de confianza porque son los que tienen capacidad de hacer gestiones y tratar con determinados clientes", asegura la CEO de Forensics&Security.

La compañía empezó estudiando estafas de cantidades importantes, "pero empezamos a ver estafas a pymes, a empresas pequeñas que a lo mejor tienen facturas de 20.000 euros; el caso es que "ha habido estafas millonarias con un phishing básico, y la persona que pagaba no se ha dado cuenta", asegura Pilar Vila, añadiendo que el COVID ha impactado de forma total en nuestra forma de vida, en nuestra forma de trabajo, "y eso esta generando una gran cantidad de problemas".

Tiene mucho que ver la falta de cultura en tecnología, acrecentada cuando se trata de seguridad.

Salir en las noticias es uno de los mayores impulsores de un mercado que crece a pesar de la crisis. Hace años que se espera un cambio de actitud por parte de las empresas, sobre todo pymes, sin que tengan que sufrir un incidente de seguridad porque, como asegura Pilar Vila. “los clientes que tenemos sensibilizados son los que han pasado por el incidente”.

Hay que ver la seguridad como una inversión, y no como un gasto, porque a veces es lo que salva a la empresa de un cierre. “Hay que empezar a separar presupuesto para seguridad”, aconseja la CEO de Forensics&Security que reconoce que cuando el negocio de los clientes empieza a crecer “quieren hacer auditoría de sus sistemas para ver si sería fácil o no exfiltrar datos de sus sistemas”.

La micro pyme es, asegura, un mundo aparte. Explica Pilar Vila que estas empresas muy pequeñas buscan la supervivencia en su economía y la informática la colocan en el último lugar, lo que es un error porque tienen menos capacidad para soportar un impacto. “Para mí lo importante es contar con una informática robusta y un departamento financiero fuerte. El marketing puede traerte clientes, pero tienes que poder soportarlos, y para eso necesitas tecnología y finanzas, o contar con una empresa informática que tenga un buen servicio”, dice Pila Vila. Y a la falta de concienciación se une el problema de no saber distinguir un buen técnico de otro que no lo es; “creemos que un técnico tiene que saber de todo, incluida la seguridad. Ir tanto a la supervivencia al final nos perjudica”.

Añade esta directiva que estamos en un punto donde la tecnología se ha especializado tanto que no es posible controlarlo todo; “Nosotros, siendo de la rama de la ciberseguridad hay algunas cosas

"En una respuesta ante incidentes nosotros tenemos que desplegar el EDR para ir levantando equipos"

"Las empresas nos están pidiendo mucho testing y mucho análisis de vulnerabilidades porque quieren saber cómo están y cómo mejorar, y eso antes no pasaba"

que hacemos, pero otras no". En el tema de la profesionalización y la especialización, hay cursos, másteres y certificaciones "que te pueden dar una aproximación, un acercamiento a este mundo para que comiences también a cacharrear, porque también es mucho de investigación propia. Añade por último que el profesional tiene mucha responsabilidad en su aprendizaje".

Un caso de uso

Cuando un cliente sufre un incidente de seguridad Forensics&Security le recomienda que ponga una denuncia. Normalmente ahí acaba todo, porque, como explica Pilar Vila, "llegamos aciertas direcciones IP que normalmente son de fuera y ahí suele acabar todo".

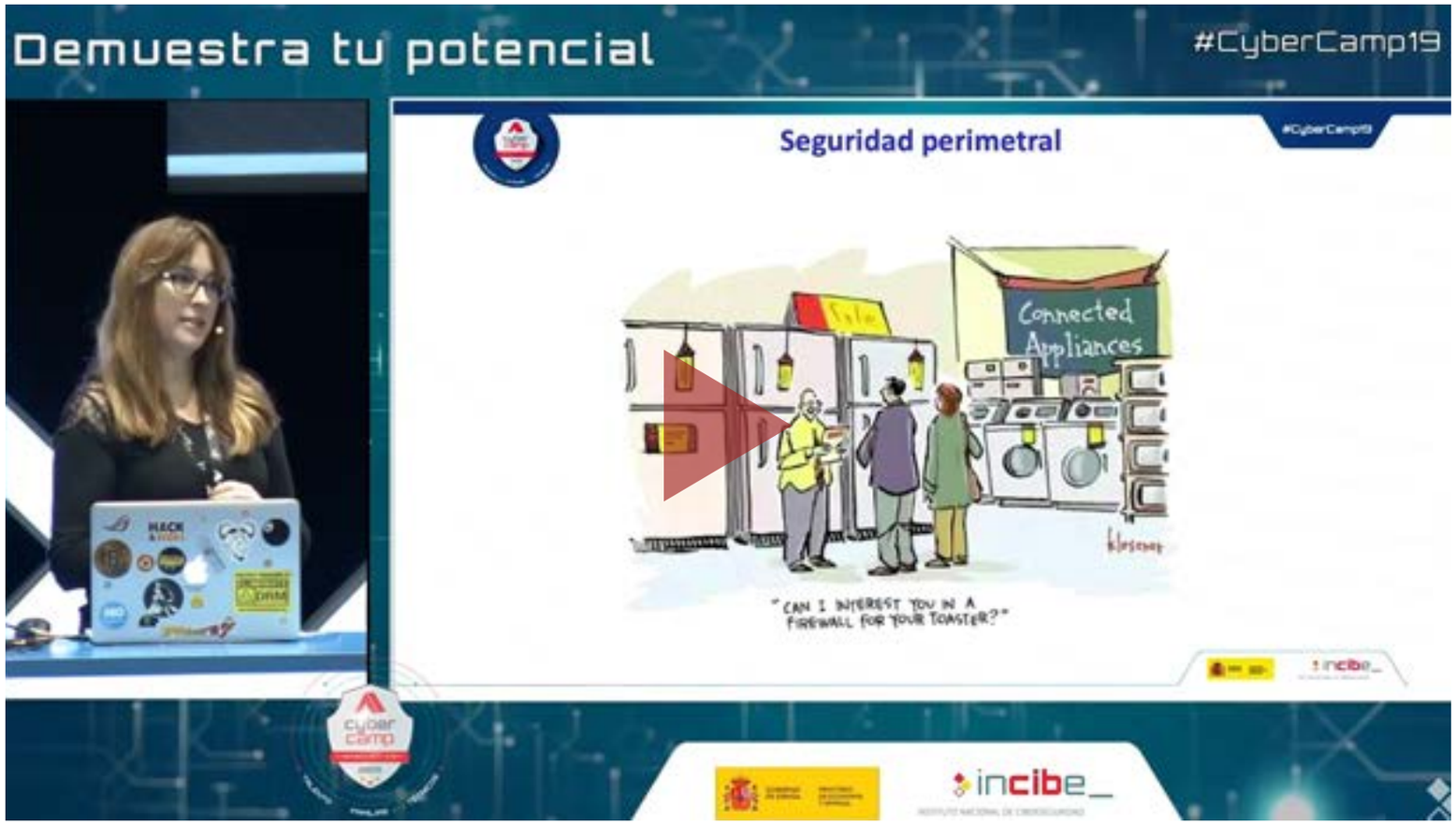
En lo que se refiere a temas periciales y cuando se trata de competencia desleal, normalmente se inicia con una sospecha y lo que hace Forensics&Security es ir, acompañado de un notario, a la empresa del cliente, donde se recoge todo el equipo, que se traslada a la notaría, donde se dejan los originales depositados tras hacer una copia exacta de los mismos. La clave, explica Pilar Vila, es mantener la cadena de custodia por si hay que ir a un juicio.

Los expertos de Forensics&Security estudian las pruebas y elaboran un informe que determina si ha habido competencia desleal. "Se intenta ser muy garantista en los procesos penales", apunta Pilar Vila.

También se puede intervenir en temas relacionados con despidos, en casos relacionados con un bajo rendimiento del empleado, para lo que puede tener que demostrarse que estaba todo el día metido en YouTube o leyendo el periódico.

En temas relacionados con conflictos con las empresas, para lo cual puede tener que estudiar el equipo del trabajador, o el WhatsApp, el correo electrónico, etc.

Dice Pilar Vila que casuísticas para aplicar la tecnología pericial hay muchas, pero que lo más habitual en empresas es competencia desleal y estafas, y en particulares temas de separaciones de pareja y despidos. Respecto a las estafas, cuando una empresa paga pero el dinero no llega porque ha sido interceptado, el llamado fraude al CEO, se tiene que saber de quién es la culpa, quién tiene la



CÓMO ENCONTRAR SISTEMAS VULNERABLES USANDO METABUSCADORES - PILAR VILA

CLICAR PARA VER EL VÍDEO

responsabilidad cuando el dinero se queda en manos de los ciberdelincuentes.

Mercado en ciernes

Además de la pandemia, la mayor visibilidad que se da a la seguridad en los medios de comunicación está impulsando el mercado de análisis forense. MarketsandMarkets menciona también su informe Digital Forensics Market que se espera que el uso masivo de dispositivos de IoT incrementará la demanda de soluciones y servicios de forénsica digital, que además tendrá nuevas oportunidades de mercado en verticales regulados y por el incremento del uso de criptodivisas. Entre los retos menciona la falta de planificación de este tipo de actividades entre las empresas y una "inadecuada" experiencia técnica entre los investigadores digitales.

Apunta Pilar Vila que ha habido un cambio cultural, que los usuarios ya saben que cuando sufren un incidente se puede hacer algo más, que hay opciones, y que eso está impulsando este mercado. "Sabe que hay profesionales a los que puede acudir, pero aún funcionamos por reacción, no somos proactivos", señada. Lo habitual, asegura, es que les llamen cuando algo ha pasado, pero que una vez que se realiza la respuesta al incidente pidan más cosas; "nos están pidiendo mucho testing y mucho análisis de vulnerabilidades porque quieren saber cómo están y cómo mejorar, y eso antes no pasaba", dice la directiva, aclarando que esta proactividad se da más en pymes de cierto tamaño y que la micro pyme sigue sin dar el paso.

Preguntamos a Pilar Vila qué impacto tienen tecnologías como EDR (Endpoint, Detection and Response), o NDR (Network Detection and Response), en el mercado de analítica forense. "En

una respuesta ante incidentes nosotros tenemos que desplegar el EDR para ir levantando equipos", dice pilar Vila.

Las soluciones EDR llegaron al mercado hace unos años para añadir inteligencia a los antivirus tradicionales, que si bien siguen teniendo cierto valor para la protección del endpoint, no son suficientes. Estas soluciones se van imponiendo, pero no tan rápido como se esperaba. Entiende Pilar Vila que la capacidad económica de la pyme es un factor importante para no tener un EDR, pero que "hay determinadas empresas que no se pueden permitir no tener un EDR, al menos en sus servidores".

Como consultora ¿qué recomendaciones son las que hacéis para que la empresa sea segura? "Depende del nivel de la empresa", dice la CEO de Forensics&Security, añadiendo que mínimo sería contar con antivirus y EDRs en los servidores, o tener regulados a los empleados mediante un documento sobre el uso de medios de la empresa; "y de ahí, para arriba". it

Enlaces de interés...

- Forensics&Security
- IA y Forénsica digital
- El mercado de Servicios forenses digital en 2021 y más allá

Compartir en RRSS

8
ABRIL
11:00 CET

REGISTRO

Sophos ZTNA:
securizando el acceso a organizaciones en cualquier lugar

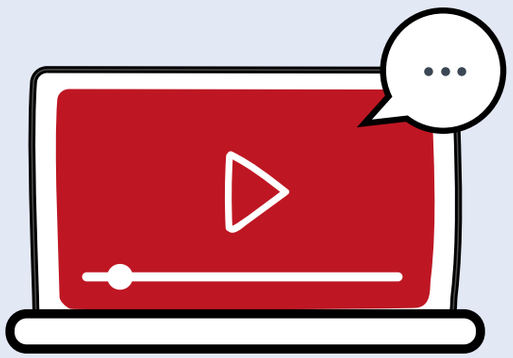
ON DEMAND

Sophos aborda la problemática actual de seguridad a la que se enfrentan las empresas, con un mayor volumen de ataques y la necesidad de extender las medidas de protección a una organización dispersa. Explica, además, qué es Sophos ZTNA (Zero Trust Network Access).

REGISTRO

Operaciones y Kubernetes
Infraestructura para cargas nativas en Cloud

La adopción de Kubernetes está permitiendo a las empresas implementar y administrar contenedores y, al mismo tiempo, administrar aplicaciones heredadas obteniendo ventaja competitiva, capacidad de innovación y productividad en sus entornos de desarrollo.



#ITWEBINARS

Aplicaciones,
¿cómo desarrollo y entrego mi mejor software?

6
MAYO
11:00 CET

Porque las aplicaciones son hoy -más que nunca- la cara del negocio...
Únete a este Encuentro IT Trends con expertos y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlos en producción y administrarlos.

22
ABRIL
11:00 CET

REGISTRO

Cómo hacer avanzar y proteger la empresa digital

El mercado de la ciberseguridad está adoptando nuevos o renovados planteamientos para obtener visibilidad de lo que ocurre en la red. En este webinar abordaremos los principios de las tecnologías de EDR, NDR, SIEM y SASE y sus capacidades para proporcionar la seguridad que toda empresa digital necesita.

REGISTRO

Una estrategia global única y grandes oportunidades para partners y clientes, así queda WatchGuard

(Carlos Vieira, Country Manager WatchGuard Iberia)

Una estrategia global única y grandes oportunidades para partners y clientes, así queda WatchGuard

(Carlos Vieira, Country Manager WatchGuard Iberia)

En marzo de 2020 se anunciaba la compra de Panda Security por parte de WatchGuard. El acuerdo, cerrado en junio, crea una empresa de seguridad con una oferta para la red, el cloud, el endpoint y los accesos que, bien asentada en el midmarket, busca sumar nuevas oportunidades en la parte alta del mercado. Apostando por el canal y una oferta gestionada centralmente a través de la plataforma WatchGuard Cloud, la compañía afronta un año lleno de oportunidades para los clientes y el canal de distribución.

Los últimos han sido los meses de transición que toda adquisición requiere, algo en lo que WatchGuard tiene experiencia tras haber comprado en los últimos diez años un total de siete empresas, permitiéndole evolucionar su oferta desde los UTMs a la seguridad de las redes WiFi, el cloud, la autenticación multifactor y, gracias a Panda Security, adentrarse en el mercado de seguridad endpoint y los servicios de threat hunting. “El balance de la operación es positivo y la evolución de la integración muy buena. En menos de un año del anuncio de la compra de Panda, hemos logrado importantes hitos, pues desde el pasado 1 de julio ya hay una aproximación al mercado conjunta de ambas compañías y desde octubre los partners de las dos pueden ofertar los productos de WatchGuard, incluidos los de Panda”, explica Carlos Vieira,

"Nos sentimos orgullosos del pasado que hemos heredado de Panda Security"

'NOS SENTIMOS ORGULLOSOS DEL PASADO QUE HEMOS HEREDADO DE PANDA SECURITY' (WATCHGUARD)

CLICAR PARA VER EL VÍDEO

Country Manager de WatchGuard para España y Portugal.

Dice además el directivo, que los partners de la compañía demandaban una solución de seguridad endpoint, "y nos hemos decantado por Panda Security porque consideramos que es la mejor opción".

La adquisición de Panda Security permite a WatchGuard, una empresa que cumple 25 años de recorrido, dar respuesta a la creciente demanda de seguridad para el punto final, una seguridad impulsada además por el teletrabajo y porque la pérdida del perímetro ha vuelto a colocar a los puntos finales, (ordenadores, portátiles, móviles y tablets,) en el centro de la seguridad.

Esta pérdida de perímetro que impulsó a muchos fabricantes de firewalls a buscar más allá de la seguridad de la red, no ha llevado a una merma en la venta de este tipo de dispositivos. Asegura Carlos Vieira que "los negocios siguen necesitando una solución de firewall". Reconoce el directivo que cuando se deja de trabajar en una oficina, donde hay un perímetro bien controlado, y se trabaja desde casa, las empresas pasan a tener centenares o miles de oficinas remotas y se debe securizar ese entorno y esos endpoints porque "esos dispositivos personales son potenciales medios de transporte de malware que pueden acabar en la red de la empresa".

Lo que es seguro es que la pérdida de perímetro, el teletrabajo o el incremento de los ataques está generando una mayor concienciación en materia de seguridad. Los altos directivos son más receptivos, "y esto se está traduciendo en un incremento en el presupuesto de seguridad". El puesto de trabajo también ha generado

Cytomic, elemento estratégico

“Cytomic es estratégico y lo seguirá siendo para WatchGuard”, asegura Carlos Vieira cuando le preguntamos por la unidad de negocio creada por Panda Security en 2019 para centrarse en el segmento de proveedores de servicios con un paquete de soluciones de protección avanzada para endpoints y servicios de threat hunting.

Miguel Carrero, nombrado recientemente Vicepresidente de Cuentas Estratégicas, será el encargado de liderar el crecimiento y la expansión global de la compañía para dirigirse, incorporar y gestionar alianzas con cuentas estratégicas, incluyendo proveedores de servicios de seguridad gestionada (MSSP).

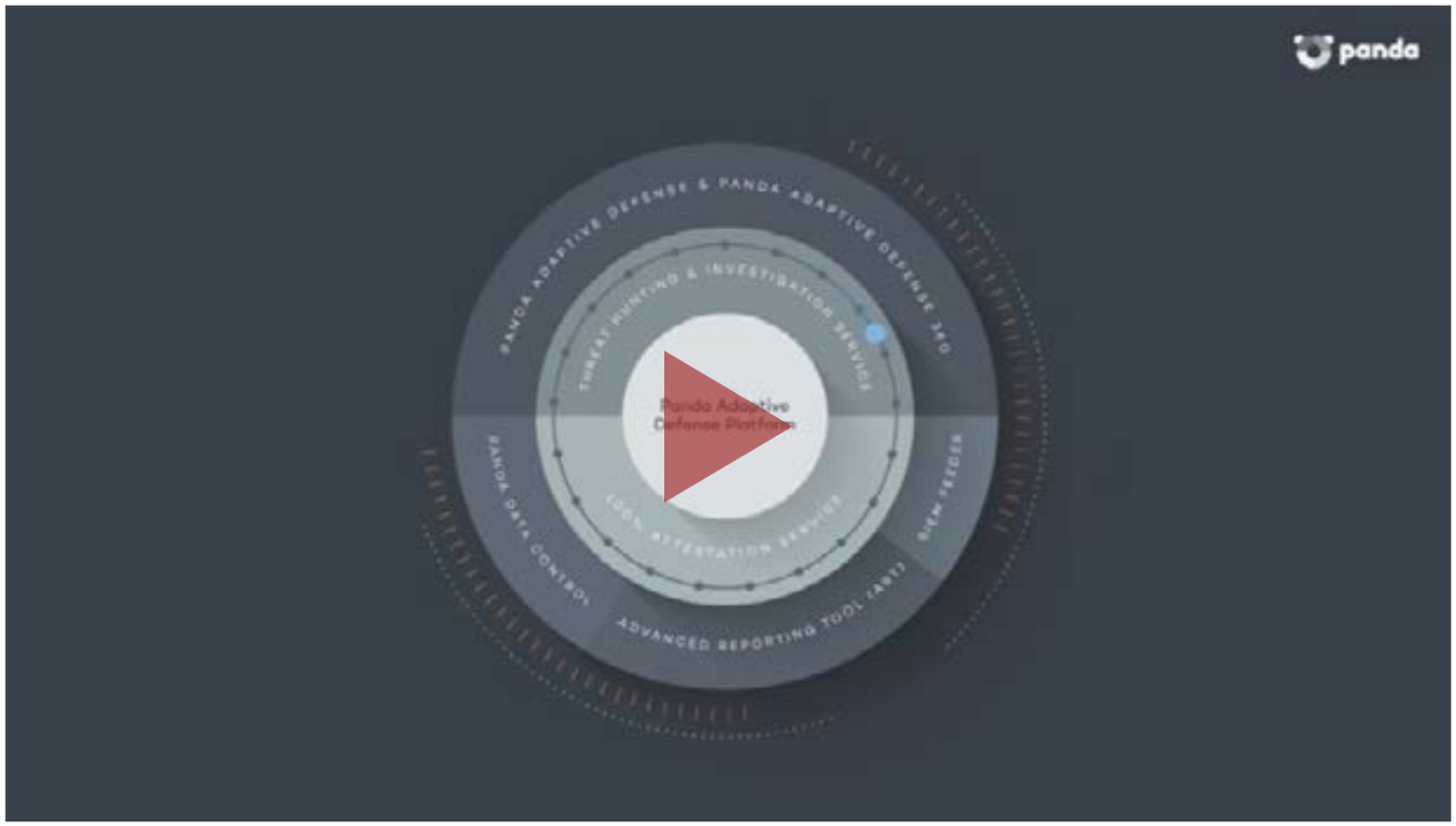
El enfoque de Miguel en WatchGuard es llevar a este segmento una cartera ampliada de productos y servicios, que incluyen seguridad de red, autenticación multifactor y Wi-Fi, y escalar la cobertura de Cytomic a nivel global.

“Las grandes cuentas siguen siendo estratégicas para nosotros”, asegura Vieira, añadiendo que se tiene el portfolio adecuado para darles servicio. Menciona que la compañía cuenta con clientes de más de 25.000 usuarios que utilizan sus soluciones autenticación mutifactor; clientes con más de 3.000 puntos de acceso o grandes clientes a nivel mundial con millares de dispositivos desplegados. Se mantiene, además, el compromiso con el roadmap previamente establecido.

"Queremos ser la solución de seguridad para nuestros clientes, y esto significa que estaremos integrando, adquiriendo y desarrollando nuevas soluciones para poder enriquecer nuestro portfolio"

tecnologías “next gen”, algo que ya ocurrió hace años en el mercado de firewalls, cuando se acuñó un término que aún persiste: el de Next Generation Firewall, o NGFW.

En el mundo del endpoint ha habido una revolución y ya no se habla de antivirus (AV) o antimalware (AM). Ahora se habla de EDR, de Endpoint Detection and Response, un segmento al que han llegado un puñado de empresas entre las que se encuentra Panda Security gracias a su tecnología Adaptive Defense, una solución presente en el catálogo del CCN y que utilizan muchas empresas de diferentes sectores, desde operadores a compañías del sector bancario, seguros o de viajes. Adaptive



ADAPTIVE DEFENSE 360 **CLICAR PARA VER EL VÍDEO**

Las oportunidades de cross-selling permitirán a los partners de "network security" entrar en el mundo del endpoint y a los del mundo endpoint entrar en el del UTM

Defense 360 presenta muchísimas opciones para WatchGuard, cuyo Country Manager asegura que “es nuestro trabajo seguir evangelizando” porque los clientes necesitan dar el salto a este tipo de soluciones que combinan capacidades EPP y EDR para estar más seguros.

Nadie dijo que las integraciones y la toma de decisiones fueran fáciles. En el caso que nos ocupa

No habrá una estrategia de marcas en España distinta a las demás regiones

hay dos grandes marcas, Panda Security y WatchGuard, que se complementan a la perfección y que cuentan con una cultura similar. Se está trabajando en un proceso de integración de las marcas que conoceremos en los próximos meses, pero lo que sí parece claro es que "solo habrá una estrategia global. No habrá una estrategia de marcas en España distinta a las demás regiones".

Comenta también Carlos Vieira que "nos sentimos orgullosos del pasado que hemos heredado de Panda Security" y "la demostrada experiencia que tenemos en operaciones de adquisición e integración de tecnologías que luego convertimos en productos muy sólidos y rentables para el ecosistema de partners". Asegura, además, que la compra de Panda Security permitirá que "nuestros clientes estén más protegidos, que nuestros partners tengan una oferta completa que cubra todo el ciclo de seguridad desde la red al endpoint y que WatchGuard disponga de un portfolio más amplio de soluciones para ofrecer".

Impacto en el canal

En una adquisición tan importante hay que tener en cuenta tanto la integración de productos como el impacto que tendrá en el canal. La palabra cross-selling es la clave y el mensaje para el canal de distribución de ambas compañías es: "Se abre un abanico de oportunidades muy grande en nuestros partners para hacer cross-selling y en nuestros clientes para tener una mejor seguridad, pues hablamos de una oferta completa y unificada que simplifica las tareas de despliegue, gestión y mantenimiento, entre otras cosas", asegura Carlos Vieira.

Del lado de los mayoristas habrá una consolidación de un número determinado de ellos que darán soporte comercial y técnico a sus partners. Para el directivo de WatchGuard, la única opción es para los mayoristas de valor añadido, lo que está generando un proceso de transformación en esta figura.

Dice el directivo que la seguridad es cada vez más compleja y que los clientes lo que buscan son soluciones que sean fáciles de gestionar, "y lo que estamos permitiendo y queremos incentivar es la adecuación y complementariedad del portfolio de soluciones, la sencillez y la eficacia de las mismas y un modelo de negocio que entiende y promueve la colaboración con nuestros partners de una manera estratégica y sostenida para dar la mejor solución al cliente final", subraya Carlos Vieira.

Estas oportunidades de cross-selling permitirán a los partners de "network security" entrar en el mundo del endpoint y a los del mundo endpoint entrar en el del UTM, y "estamos trabajando y realizando un gran esfuerzo en la parte de marketing, en la parte comercial, de gestión de producto, para mostrar a nuestros partners que somos la mejor solución para sus clientes porque, efectivamente, tenemos un portfolio que cubre Cloud, Network, Wireless, Multifactor Authentication y Endpoint".

La corporación trabaja en un ambicioso roadmap de producto que verá la integración de todas las

Enlaces de interés...

- WatchGuard nombra a Miguel Carrero vicepresidente de Cuentas Estratégicas
- Los partners de WatchGuard y Panda ya pueden beneficiarse de la adquisición y ofrecer el portfolio combinado
- La compra de Panda Security por WatchGuard tiene todo el sentido

soluciones. WatchGuard Cloud, la plataforma de la compañía para la gestión de servicios de seguridad y en la que ya se integran las soluciones de UTM, WiFi seguro o MFA, ya está haciendo pruebas con la solución endpoint, "el propósito es tener en los próximos meses un portafolio que cree sinergias y aporte un valor añadido más allá de lo que aporta cada una de las partes de forma independiente" añade Vieira.

Lógicamente, no solo se trabaja en la integración. "Interesante" es como Carlos Vieira define el roadmap de la compañía; "queremos ser la solución de seguridad para nuestros clientes, y esto significa que estaremos integrando, adquiriendo y desarrollando nuevas soluciones para poder enriquecer nuestro portfolio". Pero además WatchGuard aspira a ser el proveedor de seguridad para toda la comunidad MSP, y "creemos que hay tres inversiones principales que nos ayudarán a aumentar nuestra presencia en la comunidad de MSP más amplia: la expansión de la cartera, la evolución del modelo de negocio y un esfuerzo de ventas dedicado".

Tipología de cliente

Antes del acuerdo de compra, tanto WatchGuard como Panda Security compartían tipología de cliente: el mercado de la pyme. Una vez cerrada la compra: "Seguimos siendo la solución de seguridad para las pymes y la empresa distribuida", pero con la oportunidad hacia la gran cuenta que abre la propuesta EDR de Panda Security. Asegura Vieira que habrá una gran oportunidad en muchos grandes clientes.

En cuanto a las previsiones, se mantiene el crecimiento de doble dígito que según el country manager de WatchGuard para España y Portugal," es lo habitual en la compañía".

Compartir en RRSS

SMART SECURITY, SIMPLY DONE.

SEGURIDAD DE RED • AUTENTICACIÓN MULTIFACTOR • WI-FI SEGURO • SEGURIDAD DE ENDPOINTS

900 90 70 80

spain@watchguard.com

PROTECCIÓN INTELIGENTE

Múltiples servicios trabajan juntos de manera inteligente para prevenir, detectar y responder instantáneamente a los ciberataques con políticas automatizadas, así como supervisar e informar sobre el estado de tu infraestructura de TI.

VISIBILIDAD ACCIONABLE

Las herramientas de visibilidad accionable te permiten identificar amenazas de manera proactiva, al tiempo que proporcionan acciones correctivas contra los problemas conocidos.

GESTIÓN SIMPLIFICADA

Nuestra plataforma de gestión basada en la nube despliega, configura y mantiene tu seguridad de forma rápida y sencilla en múltiples productos de seguridad, empresas y sitios.

PIONEROS EN CIBERSEGURIDAD DURANTE 25 AÑOS.

25 ANNIVERSARY WatchGuard®

IT TRENDS

ABRIL 2021

Cloud, ¿hay opción? Viviendo en la nube híbrida

UNA PUBLICACIÓN DE IT Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Directora de IT Digital Security
Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Director de IT User e IT Reseller
Pablo García pablo.garcia@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es
Redacción y colaboradores Ricardo Gómez, Alberto Varet, Hilda Gómez, Arantxa Herranz, Reyes Alonso, Belén Juárez
Diseño revistas digitales Eva Herrero
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska
Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Cloud = Aceleración digital

2020 fue el año en el que la inversión en cloud superó al gasto en data centers propios, según Synergy Research: el año pasado, el gasto en infraestructura en la nube aumentó un 35% rozando los 130.000 millones de dólares, mientras que el gasto en TI empresarial on-premise se contrajo un 6%, quedando en unos 90.000 millones.

El cambio de tendencia comenzó a percibirse en 2019, cuando ambas categorías estaban al mismo nivel. Pero si ya se veía claro que la nube superaría a la TI local, la pandemia ha impulsado este salto en todo el mundo. Cada vez más, las organizaciones se apoyan en servicios cloud para sostener el negocio y avanzar en la transformación digital.

Además, el aumento en las capacidades computacionales, las aplicaciones más sofisticadas y la explosión de los datos están acrecentando la necesidad de servidores, que no terminan instalados en los centros de datos propios, sino en los de los proveedores cloud.

Desde la firma de análisis indican que en los próximos años no se espera ver ya una reducción drástica del gasto en CPD propio, pero sí prevén un aumento rápido en la inversión en la nube, que servirá para sostener la mayor parte del crecimiento digital de las empresas.

Y es que, cuando una compañía necesita más capacidad, puede optar por invertir en su propio data center –espacio ideal para ciertas cargas–, o contar con las posibilidades de flexibilidad, seguridad y crecimiento que ofrece la nube pública; es más, no tiene que casarse solo con una, puede favorecer a su negocio y a su arquitectura de TI con las propuestas de diferentes proveedores y generar un entorno multinube. En la oferta está la opción.

Pero ¿qué supone un entorno híbrido y multicloud desde el punto de vista de la administración de TI? Esto es lo que abordamos en el **Encuentro IT Trends** celebrado este trimestre, y en el que trece compañías nos han ofrecido su visión para la gestión y protección de estas arquitecturas cloud mixtas y múltiples. Gracias a Barracuda, Check Point Software, Commvault, Crayon, Dell Technologies, Entrust, Ikusi, Making Science, Micro Focus, NFON, SonicWall, Sothis y Thales Digital Identity & Security, por haber participado en este evento online que podéis ver aquí y leer su resumen en las siguientes páginas, y a Maica Aguilar Carneros (W4C Spain) y Víctor Escudero Rubio, por aportarnos su visión como expertos tecnológicos.

También en este número de IT Trends descubrimos esas **tendencias tecnológicas que están apuntalando la transformación digital** que se aceleró en muchas organizaciones el pasado año; cómo se está investigando y llevando a cabo proyectos tecnológicos en el entorno universitario de la mano de **Andrés Prado, director TIC de la Universidad de Castilla La Mancha** y miembro de la sectorial TIC de la Conferencia de Rectores de las Universidades Españolas (Crue), y los avances en **computación cuántica** que están haciendo empresas y países. Y ya tenéis disponible el informe IT Trends 2021. Asimilando la aceleración digital, en el que se recoge el estado de las iniciativas TI e intenciones de desarrollo para este año.

Continuemos innovando. ■

Arancha Asenjo
Directora de IT Televisión y Lead Gen Programs

Descarga este documento ejecutivo de itRESEARCH

NUEVO INFORME

2021: tendencias tecnológicas para la maduración digital

Aunque la pandemia ha afectado mucho a la economía mundial, ha tenido un efecto impulsor de la transformación digital para muchos sectores que estaban retrasando este cambio. Una vez superada la primera etapa de esta crisis, las compañías están consolidando sus estrategias de digitalización, lo que acelerará el desarrollo de ciertas áreas en las que la tecnología está evolucionando para proporcionar soluciones de cara al futuro.

Como todo el mundo espera, 2021 será el año en el que vaya estabilizándose la situación sanitaria, aunque las dificultades económicas propiciadas por la irrupción de la pandemia en el devenir global se prolongarán durante varios años. La tecnología ha demostrado su papel salvador en muchas de las situaciones que se plantearon en 2020 y continuará ejerciendo su rol como transformador. En este año seguiremos viendo cómo una serie de tendencias tecnológicas que comenzaron a ganar fuerza el año pasado, están madurando a medida que la situación se va controlando. Cada sector tiene unos objetivos y está siguiendo un camino propio, pero todos tienen como eje principal la transformación

digital. Y también la transición a modelos de negocio digital y la adopción de nuevas estrategias operativas, que aportan flexibilidad y permiten seguir trabajando en situaciones de crisis.

LAS EMPRESAS PRIORIZAN EL TELETRABAJO

Después de que los gobiernos adoptasen medidas de confinamiento, muchas empresas siguieron sus recomendaciones y adoptaron estrategias de teletrabajo para limitar la exposición de sus empleados a posibles contagios. Este es uno de los cambios que se implementaron de forma más apresurada, debido a la urgencia de la situación, pero ha demostrado ser una de las estrategias más inteligentes.

Las restricciones de movilidad han seguir un patrón fluctuante desde la primera oleada de la pandemia, pero la mayoría de las empresas que cuentan con oficinas ha decidido que sus empleados sigan trabajando desde casa, lo que ha sido un acierto. Según los expertos, el éxito que ha tenido esta estrategia en términos generales ha llevado a las empresas de muchos sectores a replantearse su modelo operativo de cara al futuro. Por ello, a partir de este año muchas adoptarán como prioridad el teletrabajo o las modalidades mixtas, que combinan el trabajo remoto y presencial.

Esto tendrá una influencia importante en diferentes mercados vinculados a la tecnología usada en el trabajo desde casa, que verán un aumento importante de la demanda por parte de empresas, instituciones gubernamentales y consumidores. Un ejemplo son las soluciones de comunicaciones unificadas y colaboración, que se han convertido en imprescindibles para muchas empresas.

Aunque las empresas reanuden el gasto en su TI local, seguirán apoyándose en la nube pública para seguir avanzando y para proteger su negocio

Otro es el mercado de ordenadores portátiles, que se ha enfrentado a una demanda muy difícil de cubrir y ha dado nueva fuerza a categorías antes minoritarias como los Chromebooks, que el año pasado registraron ventas sin precedentes y seguirán capturando buena parte del mercado vinculado al teletrabajo. Además, los requisitos que impone esta modalidad laboral están imponiendo nuevos requisitos técnicos que los fabricantes están adoptando para ofrecer equipos más competitivos.

EL MERCADO DE LA NUBE CRECE Y SE CONSOLIDA

Si hay una industria que ha salido reforzada de la crisis causada por la pandemia es la de servicios en la nube. Desde principios de 2020 las empresas han tenido que recortar al máximo el gasto previsto en sus instalaciones y en otras tecnologías, destinándolo a áreas vitales para mantener el negocio en marcha. Esto incluye los servicios cloud, que se han convertido en un apoyo fundamental para garantizar los servicios a sus clientes y la capacidad de sus empleados para trabajar desde sus hogares.

Según los expertos, aunque las empresas reanuden el gasto en su TI local, seguirán apoyándose en la nube pública para seguir avanzando y para proteger su negocio. Esto impulsará el crecimiento del mercado de la nube en los próximos años, generando oportunidades para los proveedores de diferente nivel, que tratarán de capturar cuota en un mercado dominado por unas pocas empresas tecnológicas de gran envergadura. Por ahora, el líder del ranking mantiene un dominio absoluto del mercado y, aunque sus competidores principales están ganando terreno poco a poco, los operadores más pequeños están perdiendo terreno.

LOS CENTROS DE DATOS SE EXPANDEN A NUEVOS MERCADOS

El año pasado las empresas recurrieron más que nunca a las aplicaciones digitales para superar la crisis, generando una gran demanda de tráfico y computación en los centros de datos. A esto se sumó el crecimiento exponencial de los principales segmentos del ocio digital, como los juegos online y los servicios de streaming de contenido

multimedia, que también aumentaron la presión en los centros de datos. Esto obligó a los operadores a incrementar el gasto en infraestructura en sus instalaciones, especialmente en los centros de datos de la nube, una tendencia que continuará a lo largo de este año.

Aunque los expertos afirman que muchos operadores centraron sus inversiones estrictamente en cubrir las necesidades del momento, y los proyectos de construcción y ampliación de centros de datos se vieron ralentizado o paralizados, por lo que el crecimiento del sector fue menor de lo esperado en términos generales. Pero este año la mayoría volverá a ponerse en marcha, y se sumarán otros nuevos proyectos en los principales mercados, que servirán para apoyar la transformación digital en todo el mundo. Además, los expertos destacan que a partir de este año la industria de centros de datos experimentará una rápida evolución, siguiendo tendencias que no se podían anticipar antes de la crisis.

Por otro lado, cabe destacar que no solo se está acelerando la inversión en los grandes mercados de centros de datos, sino que comienzan a ganar peso nuevas localizaciones emergentes en regiones como Asia o Europa, con lugares de gran crecimiento como Madrid, donde se están concentrando nuevas inversiones de la industria. Esta diversificación de la infraestructura global de centros de datos va a continuar en los próximos años, aprovechando la expansión de los nuevos mercados, lo que generará grandes oportunidades para los proveedores de infraestructura y para mercados como el de colocación.

AUMENTAN LOS PRESUPUESTOS DESTINADOS A TECNOLOGÍA

Desde principios de 2020 las empresas han tenido que recortar el gasto al máximo para poder superar la crisis, lo que ha incluido los presupuestos destinados a modernizar y ampliar la TI local. Pero, tras el impacto inicial de la crisis, están volviendo a incrementar el gasto en tecnología para acelerar la transformación digital y mantener su competitividad, una tendencia que continuará este año.

Aunque la pandemia no se ha contenido todavía, y la economía global seguirá sufriendo problemas este año, las empresas de muchos sectores se han dado cuenda de que el futuro de muchos negocios es digital. Para sobrevivir necesitarán invertir recursos en la adopción de nuevas tecnologías, modelos operativos y de negocio basados en lo digital. Esto supone replantear las prioridades de gasto e incrementar los presupuestos destinados a tecnología, algo que los líderes de TI deberán planificar cuidadosamente, en coordinación con otras áreas del negocio que también puedan beneficiarse de estas tecnologías.

LA CADENA DE SUMINISTRO SE MODERNIZA

La pandemia ha puesto de relieve la gran debilidad de la anticuada cadena de suministro global ante situaciones de crisis, ya que el año pasado se produjeron interrupciones graves en el flujo de muchas mercancías fundamentales. Las estrate-

gias tradicionales no permiten anticipar los problemas que se pueden producir ante situaciones complejas en las que confluyen muchas incidencias de forma casi simultánea. Debido a esta rigidez, los integrantes de la cadena no están bien coordinados, por lo que en muchos casos no son capaces de adoptar estrategias que mitiguen posibles interrupciones en el suministro.

Esto está llevando a las empresas vinculadas con toda la cadena de suministro a adoptar tecnologías que les permitan estar más interconectados y poder trabajar en común de forma más flexible e inteligente. Esto abarca desde el seguimiento de activos a través de IoT y 5G a la adopción de sistemas basados en inteligencia artificial para automatizar muchos de los procesos y contar con mejor información de lo que ocurre a lo largo de toda la cadena. Gracias a ello tanto los fabricantes como los distribuidores a lo largo de toda la cadena pueden anticipar las posibles debilidades de la red y los riesgos potenciales de interrupción, pudiendo desplegar a tiempo las estrategias necesarias.

Con el progreso de la digitalización, las organizaciones están capturando y acumulando más activos digitales de alto valor que deben ser protegidos

Especial mención merece el sector de la logística, en el que las principales empresas están adoptando nuevas tecnologías para optimizar las operaciones en diferentes ámbitos. Por un lado, están adoptando sistemas robóticos para automatizar los almacenes y acelerar la gestión de mercancías. Por otro, están desarrollando nuevas plataformas digitales que facilitan el trabajo de los repartidores, optimizando las rutas de reparto y mejorando la conexión con los clientes finales. Además, algunas empresas pioneras están dando los primeros pasos en el desarrollo de los primeros sistemas de reparto de mercancías mediante vehículos autónomos.

NUEVAS TECNOLOGÍAS PARA UNA FABRICACIÓN INTELIGENTE

Hasta el año pasado, la industria manufacturera ha ido adoptando las tecnologías que forman parte del concepto de industria 4.0, pero a un ritmo desahogado. Pero con la pandemia muchas las fábricas han sufrido problemas por la escasez de personal y por los bloqueos de la cadena de suministro. Ante esta situación la industria manufacturera en su conjunto está acelerando la transformación digital, aprovechando los nuevos avances en campos de la tecnología industrial como IIoT, la automatización, la robótica o la inteligencia artificial.

Proteja su experiencia en la nube de Azure.

Soluciones para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad »

Más información:
iberia_team@barracuda.com
barracuda.com

Barracuda Microsoft

STRENGTH IN SECURITY™

Según los expertos, a partir de este año va a acelerarse la adopción de estas tecnologías en la industria de fabricación, especialmente en sectores como la automoción o la electrónica, en los que las cadenas de producción van a seguir automatizándose. Esto permitirá a los fabricantes optimizar todos los procesos de producción, mejorar la calidad de sus productos y ser más eficientes, ahorrando costes una vez que se haya amortizado la inversión inicial.

Aunque, en opinión de los expertos, la automatización de la industria manufacturera todavía tardará unos años y no será completo al 100%, ya que por ahora no hay máquinas capaces de sustituir capacidades superiores del intelecto humano, como los razonamientos avanzados, la intuición y otras habilidades nacidas de la experiencia. Por ello, aunque muchos procesos fundamentales de la industria quedarán al cargo de máquinas robotizadas, los trabajadores humanos estarán al cargo de la toma de decisiones y de ciertos trabajos. Eso sí, en muchos casos asistidos por robots colaborativos, ya sean fijos o móviles, un campo en el que se están llevando a cabo grandes avances.

CIBERSEGURIDAD COMO PILAR DE LA TRANSFORMACIÓN DIGITAL

La seguridad informática siempre ha sido importante para las organizaciones, por lo que tradicionalmente han contratado aplicaciones y servicios de ciberseguridad para proteger sus sistemas. Pero con el progreso de la transformación digital las empresas han ido ampliando la superficie de ataque, añadiendo localizaciones remotas como la nube o el borde, lo que les ha obligado a incrementar el gasto en ciberseguridad. A esto se suma que los ciberdelincuentes se han vuelto mucho más creativos y han sofisticado aún más sus estrategias, sobre todo a raíz de la pandemia de 2020, lo que ha hecho que las organizaciones incrementen aún más el gasto en ciberseguridad.

La industria manufacturera está acelerando la transformación digital aprovechando nuevos avances en campos de la tecnología industrial como IIoT

Con el progreso de la digitalización, las organizaciones están capturando y acumulando más activos digitales de alto valor, que deben ser protegidos. Como explican los expertos en la materia, los riesgos de sufrir ciberataques aumentan constantemente, lo que está posicionando la ciberseguridad empresarial como uno de los pilares fundamentales de la transformación digital. Por ello, se espera que las empresas eleven este tipo de seguridad a un nivel superior, no solo incrementando el gasto, sino también creando un comité de ciberseguridad en su junta directiva.

Esto les permitirá garantizar que la organización es capaz de enfrentarse a los retos de seguridad que conlleva el progreso tecnológico, algo fundamental de cara al futuro. Porque en los próximos años comenzarán a expandirse nuevas tecnologías en los negocios y en la sociedad que requerirán nuevas estrategias se ciberseguridad. Entre ellas, los expertos destacan la bioseguridad, la cuántica y la seguridad integrada en dispositivos, aunque hay otras tendencias con un gran potencial

ATENCIÓN SANITARIA MÁS DIGITAL Y CONECTADA

Uno de los sectores que más ha sufrido el impacto de la pandemia es el de la salud, en el que los profesionales se han visto sobrepasados por la situación. Por ello, las organizaciones del sector están recurriendo a la tecnología para mejorar la atención sanitaria, ser más eficientes y proteger la salud de los profesionales y los propios pacientes. Los expertos pronostican que a partir de 2021 la industria va a invertir cada vez más en el desarrollo y la expansión de tecnologías como los dispositivos de monitorización remota de salud. Esto permitirá la evolución de conceptos como los wearables empleados en la monitorización de actividades deportivas, que incluirán capacidades y sensores cada vez más avanzados.

Estos dispositivos formarán parte de una nueva generación de plataformas de salud digital

que se alimentarán de grandes cantidades de datos provenientes de los pacientes. Estas plataformas sustituirán a los tradicionales archivos de salud, proporcionando a los médicos gran cantidad de información sobre el historial y el progreso de los pacientes en cada uno de los tratamientos a los que han sido sometidos. Y, para sacar el máximo partido a estas nuevas tecnologías de salud digital, la industria está creando nuevas soluciones de inteligencia artificial para la salud. Esta tecnología permitirá estudiar los datos de los pacientes, en particular y en conjunto, para acelerar la investigación de enfermedades y el desarrollo de tratamientos, algo que durante la pandemia está ayudando mucho a la industria médica y farmacéutica.

Una consecuencia lógica de la transformación digital que se está produciendo en el campo de la salud es un aumento de las ciberamenazas. Porque los datos de los pacientes y de las propias organizaciones de la salud se están volviendo más accesibles para los ciberdelincuentes, a través de los dispositivos remotos y las infraestructuras TI de los centros médicos. Por ello, las organizaciones dedicadas a la salud están cada vez más preocupadas por la ciberseguridad, y a partir de este año aumentarán el gasto en soluciones de seguridad informática.

Los ecosistemas de pago digital se expanden

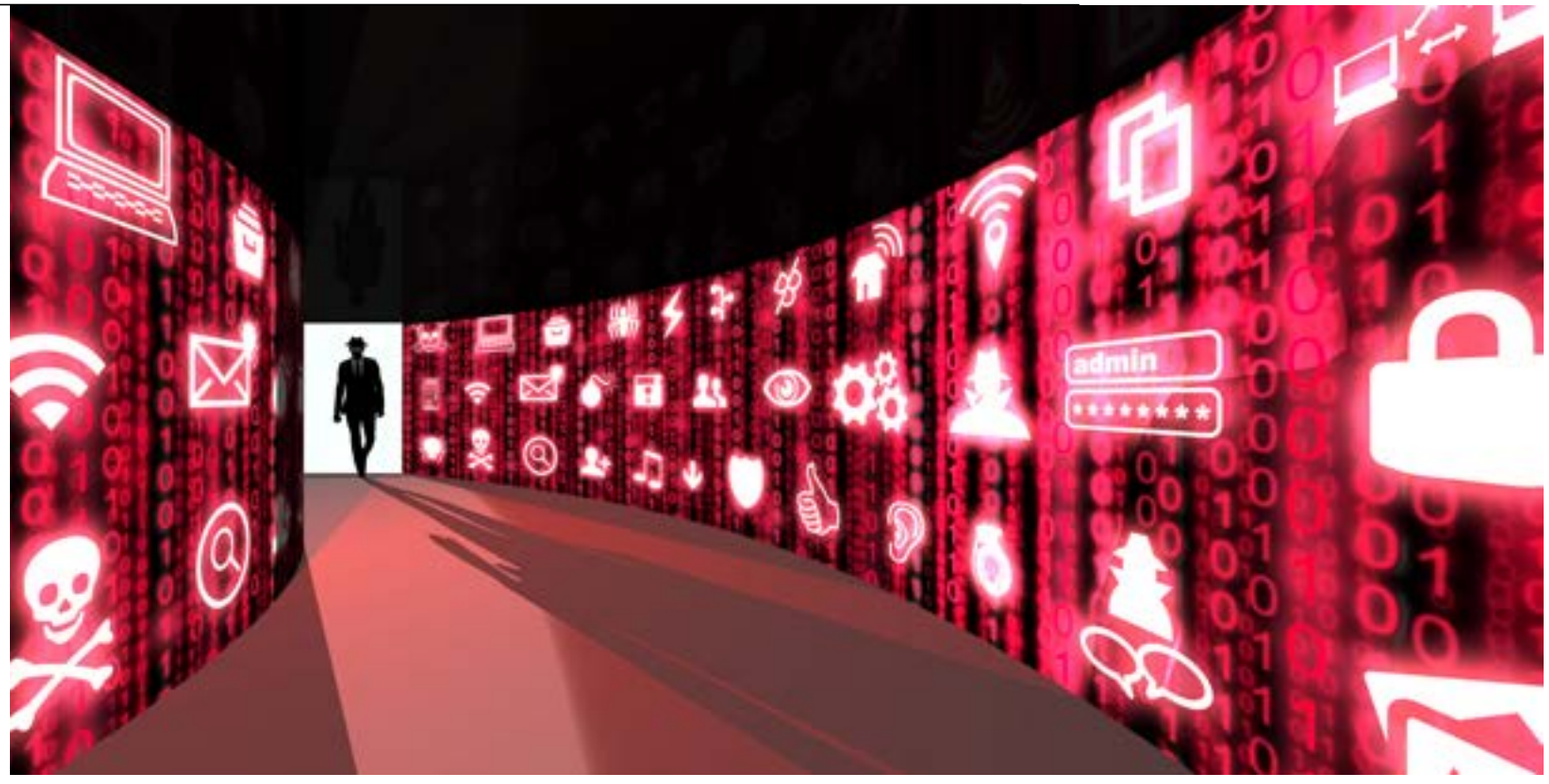
En los últimos años la economía digital ha evolucionado rápidamente, a medida que los consumidores han ido incrementando las compras a través de plataformas de comercio electrónico. En este tiempo han surgido nuevas formas de pago digital que ganan adeptos cada día, como los monederos digitales, que se están integrando progresivamente en la vida y la economía digital de las personas. Se encuentran cada vez más presentes en las plataformas de comercio electrónico y en las tiendas físicas, y los expertos han constatado un aumento considerable del gasto que realizan los consumidores a través de estas herramientas.

Al mismo tiempo, las plataformas de pago móvil se están expandiendo rápidamente, gracias a la necesidad de los consumidores de pagar sin contacto y a que los móviles pueden integrar diferentes medios de pago, desde tarjetas de crédito a monederos digitales y otras aplicaciones de economía digital. Como resultado de la pandemia, los pagos móviles están aumentando considerablemente, y los expertos esperan que sigan haciéndolo este año.

Otra tendencia interesante en el ámbito de los pagos digitales es uso cada vez mayor de la identificación biométrica para validar los pagos móviles. Esto se está logrando gracias a que los nuevos smartphones integran sistemas fiables de lectura de huellas digitales y de identificación de rostros y de voz. Según los expertos, estos sistemas seguirán evolucionando con las nuevas generaciones de dispositivos móviles, acompañando al desarrollo de otras tecnologías de pago móvil.

NUEVAS APLICACIONES PARA LA REALIDAD VIRTUAL Y AUMENTADA

Las tecnologías de realidad extendida (virtual y aumentada) están llegando a un nivel de madurez que permite ofrecer soluciones muy interesantes



Las plataformas de pago móvil se están expandiendo rápidamente gracias a la necesidad de los consumidores de pagar sin contacto

para las organizaciones. Esto generará un gran mercado en el futuro, más allá de las aplicaciones pensadas para el gran consumo. Todos los indicadores muestran que, tras un 2020 desafiante, a partir de 2021 se va a expandir rápidamente el mercado de realidad aumentada y virtual.

Esto se debe a que se están desarrollando nuevos casos de uso comerciales en diferentes industrias, que a partir de este año irán expandiéndose con fuerza, aprovechando que los fabricantes de dispositivos están lanzando nuevos dispositivos portátiles independientes con mejor calidad de imagen, rendimiento y autonomía. Al mismo tiempo, el desarrollo de plataformas y software de realidad aumentada y virtual está avanzando mucho, proporcionando soluciones interesantes en ámbitos como la salud, la ingeniería o la capacitación.

Este ecosistema de proveedores está diversificándose mucho, pero los expertos están convencidos de que en los próximos años va a dar comienzo la consolidación del sector, y anticipan un aumento de las fusiones y adquisiciones en la industria. Así, los grandes jugadores tratarán de absorbes las capacidades de los innovadores en AR/VR, ya que se anticipa una creciente competencia de cara a los próximos años.

INTELIGENCIA ARTIFICIAL MÁS ÉTICA Y EXPLICABLE

La inteligencia artificial se expande rápidamente con la llegada de nuevos casos de uso comerciales y también de ámbito personal. Esto está impulsando la IA a diferentes niveles, desde las aplicaciones más básicas, pensadas para el análisis de datos personales y los sistemas de recomendaciones, a las más sofisticadas, que utilizan las empresas y los gobiernos. Gracias a la IA las organizaciones pueden mejorar sus procesos y contar con mejor información para la toma de decisiones, lo que seguirá impulsando el mercado de inteligencia artificial en los próximos cuatro años.

En este tiempo, además, el concepto de inteligencia artificial irá diversificándose, ya que están surgiendo nuevas formas de entender la tecnología vinculada a la IA. Por ejemplo, las redes de IA distribuida, formadas por enjambres de dispositivos o nodos que cuentan con capacidades de IA propias. Estos son capaces de procesar los datos a cierto nivel, pero forma parte de una arquitectura de IA mayor, donde cada miembro contribuye para proporcionar un mayor nivel de inteligencia. Este enfoque de inteligencia distribuida se desarrollará más a partir de este año,

aprovechando el progreso de tecnologías como las redes 5G y los dispositivos IoT.

Aunque el progreso de la inteligencia artificial conlleva una serie de riesgos que preocupan cada vez más a las autoridades, ya que el tratamiento automatizado de los datos y la toma de decisiones si intervención humana pueden verse afectadas por un sesgo que genere discriminación. Por ello, los expertos en IA están desarrollando códigos éticos que puedan regir el diseño y el comportamiento de la inteligencia artificial, pero no parece que este año se vaya a lograr un avance significativo hacia una ética de IA. Esto se debe a que todavía hay que avanzar más para lograr que los algoritmos de inteligencia artificial sean más explicables, lo que permitiría democratizar el desarrollo de IA para que técnicos menos especializados puedan diseñar aplicaciones que sigan un determinado código ético.

LA BRECHA DE TALENTO DIGITAL SE ACENTÚA

El progreso de la digitalización en las empresas está acentuando un problema que lleva tiempo agrandándose, que es la gran brecha que existe entre la formación de nuevos talentos y las necesidades del mundo laboral. Así, en los últimos años la escasez de personal cualificado para ciertas áreas vinculadas a la tecnología se ha vuelto un problema más grave, y los expertos afirman que gran parte de los trabajadores necesita adquirir nuevas habilidades, muchas de ellas dentro del ámbito digital.

Durante las primeras oleadas de la pandemia muchas empresas han cambiado radicalmente su forma de trabajar, y en los próximos años el puesto de trabajo va a cambiar mucho, integrando nuevas tecnologías y deslocalizándose por la proliferación del teletrabajo. Mientras tanto, se espera que la crisis económica lleve al cierre de muchas empresas, inundando el mercado laboral de nuevos trabajadores, pero muchos de ellos no tendrán la cualificación necesaria para trabajar en los nuevos puestos de trabajo, cada vez más vinculados al uso de tecnologías digitales.

Las empresas y las instituciones públicas tratarán de ir cerrando la brecha de talento, peo esto también requerirá un cambio de mentalidad por parte de las personas. Porque, estudios recientes indican que muchos trabajadores no aplican los conocimientos adquiridos a través de la formación, y esto es un freno para su progreso profesional y para las empresas en las que trabajan. Esto implica que se debe impulsar un cambio cultural en las organizaciones, incentivando a los trabajadores a mejorar a través de un enfoque de aprendizaje constante. ■

CloudGuard

Check Point CloudGuard proporciona seguridad nativa en la nube unificada para todos sus activos y cargas de trabajo, lo que le brinda la confianza para automatizar la seguridad, prevenir amenazas y administrar la postura, en todas partes y en todo su entorno.

Más información:

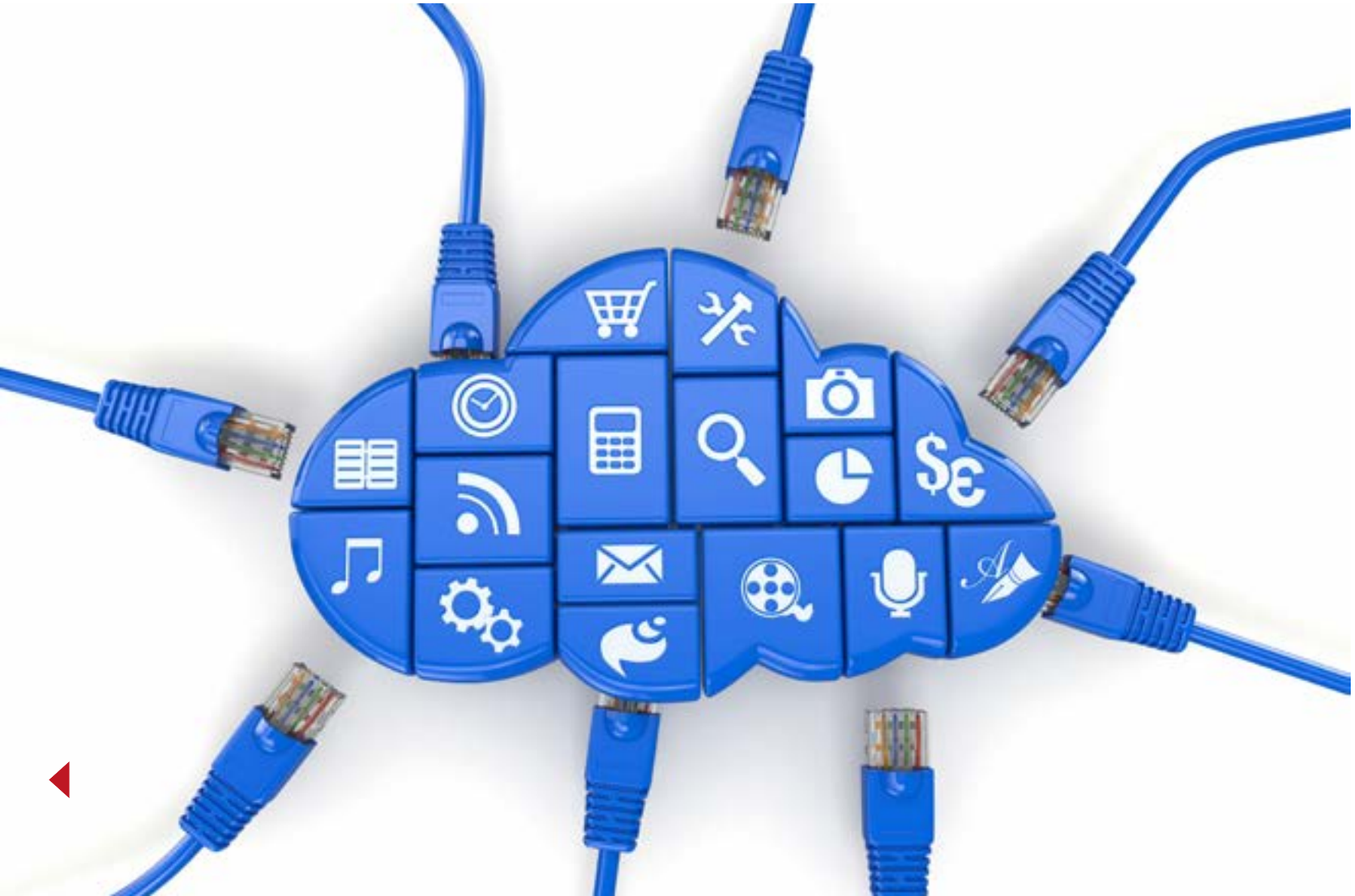
www.checkpoint.com/es

Check Point®
SOFTWARE TECHNOLOGIES LTD

it TRENDS

Tendencias en entornos cloud:

cambios en la arquitectura y perspectivas futuras



El uso de la nube ha crecido exponencialmente en los últimos años y continuará haciéndolo: según IDC, el mercado español de cloud experimentará un crecimiento cercano al 20% anual. La combinación de infraestructura y servicios compartidos para crear un entorno de TI flexible, escalable y bajo demanda ha convertido a la nube en el modelo dominante para entregar y mantener los recursos de TI empresariales, desde el hardware de computación, pasando por el almacenamiento, las redes, hasta el software empresarial.

El mantra de la resiliencia empresarial y digital seguirá pronunciándose este año a medida que las organizaciones se preparen para responder a la continua incertidumbre y disrupción. Para que las empresas puedan ser más competitivas en esta época es esencial que entiendan cómo se está transformando el panorama de TI, incluida la forma de administrar e implementar de manera efectiva los cambios necesarios para permitir la capacidad de respuesta rápida.

En un momento en el que las empresas necesitan agilidad y dinamismo para adaptarse a las circunstancias del mercado, la nube se ha

convertido en un dinamizador de la agilidad y transformación digital, especialmente en su versión híbrida, en el que se pueden unir las capacidades y ventajas de un entorno privado con todos los beneficios de una cloud pública gestionada por un tercero, con todas sus medidas de seguridad, elasticidad, innovación y conocimiento para la administración.

Este año las empresas se están preparando para que la nube llegue a todas las áreas e industrias. Por ello, los dirigentes empresariales deben observar las tendencias actuales para que sus servicios se ajusten a las necesidades de los clientes:

1 La eliminación de las cargas de trabajo innecesarias de la nube será la tendencia más destacada. Reconfigurar la estrategia para maximizar los beneficios, minimizar los costes y reducir la carga es crucial para el éxito de la nube a largo plazo. Contar solo con un proveedor de nube pública puede haber permitido la continuidad del negocio en 2019, pero tras la llegada de la pandemia, cada vez más proveedores están considerando otros modelos como un entorno multicloud como el sistema ideal para todas las operaciones.

2 Volver a activar la gobernanza de la nube para mantenerse seguro. Buscando fortalecer la estrategia de la nube, las empresas pueden reconsiderar los esfuerzos de gobernanza para priorizar la seguridad. Volver a los cimientos de las nubes y desarrollar un plan de gobierno sólido ayudará a las empresas a reforzar la infraestructura de seguridad para corregir la adopción apresurada que muchas realizaron en 2020.

3 Un crecimiento exponencial de la adopción de la nube. El año pasado el mercado global de infraestructura de nube pública creció un 35% a hasta los 100.000 millones de euros, según Forrester.

Además, en 2021 más de la mitad de las empresas aumentará la inversión en Amazon Web Services, Salesforce, Google u otros servicios en la nube este año con Microsoft Azure como la mejor opción.

4 Aumento de la innovación en la nube híbrida. A lo largo de 2021 comenzaremos a ver más estrategias multicloud com-

CINCO CONSIDERACIONES PARA PROTEGER LA INFRAESTRUCTURA EN LA NUBE

binadas con iniciativas de capacitación más amplias tanto de las empresas como de los propios proveedores.

En un futuro cercano, las innovaciones en la nube provocarán que el volumen de datos en la nube se centre cada vez más en los dispositivos que operan con IA para entregar a las empresas datos predictivos fiables para que la toma de decisiones sea fácil para los líderes empresariales. ■

MÁS INFORMACIÓN

- Forrester: Predicciones 2021: Cloud Computing potencia la recuperación de la pandemia
- Gartner predice el futuro de la infraestructura cloud y Edge
- Synergy Research: Los proveedores de cloud europeos luchan por revertir las pérdidas de cuota de mercado

FUERTE CRECIMIENTO DEL MERCADO CLOUD

El gasto total en servicios en la nube, en el hardware y el software que sostiene estos servicios y en los servicios profesionales y administrados vinculados a la cloud, crecerán aun ritmo anual del 15,7% hasta 2024, según IDC. Para entonces, pronostican que estas inversiones generarán oportunidades de negocio por un valor de más de 1 trillón (americano) de dólares en todo el mundo.

Como explica en este informe Richard L. Villars, vicepresidente de grupo de investigación mundial de IDC, "la nube en todas sus permutaciones (hardware/software/servicios/aaS, así como la nube pública/privada/híbrida/multi/edge) desempeñará roles cada vez mayores, e incluso dominantes, en la industria de TI en el futuro previsible".

Afirma que "para fines de 2021, sobre la base de las lecciones aprendidas en la pandemia, la mayoría de las empresas pondrán en marcha un mecanismo para acelerar su cambio a la infraestructura digital centrada en la nube y los servicios de aplicaciones, a un ritmo dos veces más rápido que antes de la pandemia".

Las principales fuentes de crecimiento del mercado asociado a la nube serán los servicios de nube pública (compartida) y los servicios de nube privada, una categoría que seguirá siendo la más grande del mercado, y que en este tiempo mostrará un crecimiento del 21% (CAGR). De cara a 2024, IDC anticipa que la categoría "como Servicio" logrará acaparar el 60% de todos los ingresos mundiales de la nube.

Mientras tanto, la categoría que abarca los servicios profesionales y los servicios de gestión relacionados con la nube crecerán al ritmo más lento (8,3%). Finalmente, el segmento de construcción de infraestructura, que abarca el hardware, el software y el soporte para nubes privadas empresariales y nubes de proveedores de servicios, seguirá siendo el más pequeño, pero crecerá a un saludable ritmo del 11,1% (CAGR).

La sencillez a veces esconde una gran complejidad

Cloud

Cloud

SaaS

Privada

Cloud Híbrida

Pública

Sin-Nube

Edge

Co-location

Sothis
Inteligent Services,
Inteligent Tecnology

www.sothis.tech

sothis

#ENCUENTROSITTRENDS

Ya vivo en la nube, ¿y ahora qué?

Mejores prácticas para desenvolverse en entornos híbridos

Los entornos de TI multicloud e híbridos se están convirtiendo en el modelo hacia el que se dirigen las arquitecturas de TI actuales. Gestionar estas infraestructuras cloud, controlar sus costes, desarrollar nuevos servicios nativos en cloud, asegurar la disponibilidad del negocio basado en la nube, garantizar el cumplimiento normativo y proteger los activos que residen en la cloud, son cuestiones que todo responsable de TI debe tener bajo control.

En IT Trends hemos reunido a diversos expertos para abordar las nuevas propuestas tecnológicas disponibles para una mejor resi-

dencia en una cloud que predominantemente es híbrida, así como para tener una mayor visibilidad entre las diferentes nubes y servicios. En este Encuentro IT Trends participaron Miguel López Calleja (Barracuda), Eusebio Nieva (Check Point Software), Elisa Martínez (Commvault), Jose Manuel Marina (Crayon), Nieves Gonzalez (Dell Technologies), José María Pérez (Entrust), Jorge Marín Sánchez (Ikusi), Miguel López Sánchez (Making Science), Antonio Picazo (Micro Focus), Agustín Sánchez Fonseca (NFON), Sergio Martinez Hernandez (SonicWall), Ceferino Raposo (Sothis), Alfonso Martinez (Thales Digital Identity & Security), Maica Aguilar Carneros (W4C Spain) y Víctor Escudero Rubio. ■

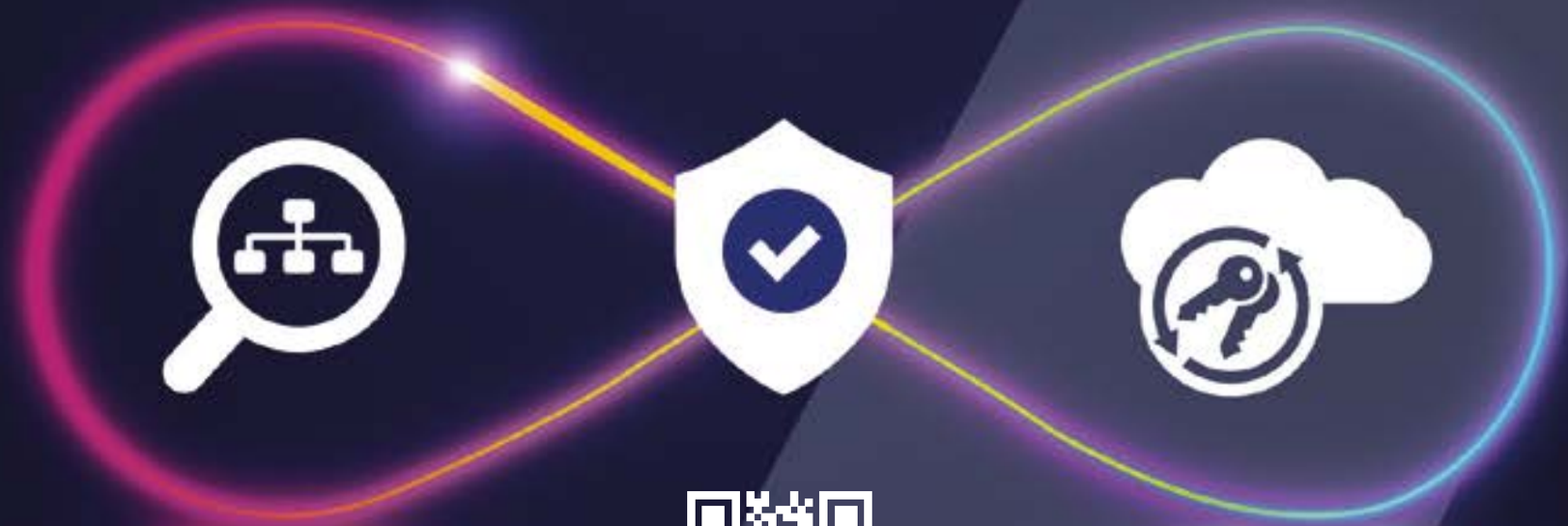
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar



Empiece a localizar, proteger y controlar sus datos hoy mismo

#ENCUENTROSITTRENDS

Conocimiento, adopción y adaptación para gestionar de manera eficiente la nube

Los entornos de Cloud continúan adoptándose en la empresa española de manera progresiva, tras demostrar en estos últimos meses ser un modelo que aporta flexibilidad a las estructuras tecnológicas de las empresas cuando éstas necesitan adaptarse a imprevistos.

Maica Aguilar (W4C Spain) y Víctor Escudero (experto en implantaciones Cloud), conversan sobre los retos que se les plantean a las empresas en su gestión de entornos multicloud. Clic para ver.

“Los estándares de auditoría, trazabilidad y herramientas permiten tener una visión amplia y transparencia en un mundo que ya no es nuestro, sino que se está gestionando por un tercero”

MAICA AGUILAR, WOMEN4CYBER SPAIN

Según la última encuesta realizada por IT Trends, la ciberseguridad será la principal área de inversión en 2021, pero le siguen los servicios y la infraestructura cloud. Además, el número de empresas cuya TI se limitaba a los entornos on premise ha disminuido porque se han unido tanto a la cloud privada como a la cloud pública, de acuerdo con el informe, que recoge que los niveles de infraestructura híbrida son los que más han crecido durante estos meses, y precisamente, son los que mayores inversiones van a recibir en este año. Respecto al número de clouds públicas contratadas, un 49% de los consultados asegura que su empresa cuenta con dos o más de estas nubes públicas. Asimismo, los encuestados consideran que para sus nubes será estratégico en este 2021 la seguridad, la integración de plataformas y la disponibilidad de las aplicaciones.

Ante estos datos, Maica Aguilar, experta en Ciberseguridad y Privacidad y miembro de la Junta Directiva de Women4Cyber Spain, explicó en la primera mesa de debate del Encuentro IT Trends titulado “Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos de Cloud híbrido”, que “el reto está en la adecuación, en tener capacidad dentro de las organizaciones para conocer el cloud y poder adaptarse al cambio de un modelo tradicional a estos ecosistemas”. Desde su punto de vista, hace años la ciberseguridad era uno de los principales frenos a la hora de migrar al cloud, pero hoy en día la perspectiva de muchas empresas ha cambiado. El cloud actualmente ofrece garantías tanto en la parte de compromiso como en la de ciberseguridad. “Sabemos cómo se están gestionando esas clouds porque tenemos estándares de auditoría, trazabilidad y herramientas que permiten una visión amplia y transparente en un mundo que ya no es nues-

“Los estándares de auditoría, trazabilidad y herramientas permiten tener una visión amplia y transparencia en un mundo que ya no es nuestro, sino que se está gestionando por un tercero”

VICTOR ESCUDERO, EXPERTO EN IMPLANTACIÓN DE CLOUD

tro, sino que se está gestionando por un tercero”, añadió Aguilar.

El coste de la cloud sigue siendo un punto clave en las organizaciones en la migración al cloud. El coste variable o pago por uso continúa siendo predominante en comparación a un pago por la contratación de una infraestructura o un pago por adelantado. “Pero lo más relevante ahora mismo tiene que ver con la escalabilidad y la flexibilidad; en época de pandemia, una empresa necesita saber qué puede crecer con un par de clics. Es decir, no haces una inversión a tres años vista de una infraestructura”, apuntó Victor Escudero, experto en implantación de proyectos Cloud, y compañero de debate. Ambos participantes estuvieron de acuerdo en que la economía de escala a nivel de seguridad no permite hacer inversiones como las grandes compañías, con Microsoft o Amazon como ejemplo. Pero, por otro lado, existen facilidades como el pago por uso para los usuarios residenciales y en consecuencia, muchos servicios de nube son más sencillos de operar y de utilizar. Las grandes compañías de cloud tienen grandes inversiones en ciberseguridad y las pequeñas empresas no pueden asumir esos gastos. Sin embargo, pueden acercarse al modelo cloud y entenderlo”, destacó Aguilar.

Los costes más directos son relativamente sencillos de ver. Sabemos cuánto pagamos por memoria o por consumo de CPU. Aunque es más difícil de ver lo que pagamos en tráfico saliente de datos hacia internet. “Hay que tener en cuenta muchos costes de licenciamiento o pago por uso. Cuando contratas una solución en modelo SaaS estás reduciendo la carga de administradores de bases de datos o de sistemas y estás difiriendo la carga operacional en un proveedor”, explicó Escudero.

Si se quiere parchear máquinas y para ello es necesario acceder a las soluciones de ciberseguridad, el proveedor de nube puede hacerse car-

go de gran parte de las actualizaciones, aunque sea un coste inmenso a nivel operativo. Además, esto provoca que no esté todo actualizado continuamente. “Cuando se calcula el TCO o coste total de oportunidad en tres años, rara vez sale más caro en nube que on-premise. Hay que computar los costes por todo lo que conlleva, no por lo que se ve de manera inmediata”, argumentó Escudero.

Por su parte, Maica Aguilar recordó que normalmente las nubes públicas hablan de seguridad compartida si tienen estándares aunque de base no está. Y “como no se puede vivir sin seguridad, no hay que olvidar esa capa tan necesaria en servicios y plataformas a la hora de hacer el análisis de costes”.

EL MEJOR MODELO DE CLOUD

Los expertos explicaron en la mesa que no existe un modelo de cloud concreto para un tipo de organización u otra, ya que es probable que en una gran empresa haya determinados procesos que encajen mejor en un modelo público y otros en un modelo privado. La clave está en lo que se quiere hacer y en ir con el partner adecuado. “Nosotros administramos nube pública, nube híbrida y mucho modelo de servicio dependiendo de cada empresa y sus necesidades”, subrayó Aguilar, que trabaja en Ferrovial.

Para Víctor Escudero, se pueden valorar las modalidades de consumo de la nube como IaaS, platform o modalidades de software, y señalar en la hoja de ruta los ritmos que ha de llevar la empresa en la transición hacia la nube. “Se puede mover infraestructura puntualmente o ir sacando partido de distintas funcionalidades según se necesiten”. Además, deshacer estos cambios suele ser simple.

Otro aspecto a considerar es ver qué capacidades nativas de nube se tienen, ya que algunas capacidades que se hacen de una forma tradicional no tienen una traducción exacta en la nube. “Los modelos de nube son mucho más naturales que los tradicionales. En esa línea, hay servicios legacy que no tiene sentido desglosar en la nube pero hay otros que te pueden interesar, como llevar los frontales y la parte de base de datos dejarla on premise de momento y seguir con ellos en la siguiente fase de la migración”, detalló Escudero.

Respecto al uso de entornos multicloud, en opinión de este experto, hay pocas diferencias entre Azure, Amazon Web Services o Google Cloud porque en todos ellos hay multi zona y multi región. Los cambios varían según se escala en cuanto a servicios, siendo los más avanzados en modalidad SaaS en los que hay grandes diferencias

A esto añade Maica Aguilar que “lo que hoy se vive de una forma, en el futuro puede ser de otra pero la clave es pasar por la estrategia multinube para que nuestro negocio evolucione de forma óptima”. ■

Run and Transform—Your Key to Success

Balance today's needs with tomorrow's opportunities.

When you can run and transform your business at the same time, you have the balance you need to optimize your enterprise and expose new opportunities as your markets evolve. No matter what's driving the change—technology innovation, the digital economy, and even pandemics and disasters—we can help you succeed with a customer-centric, measured, low-risk approach. That's High Tech, Low Drama.

#ENCUENTROSITTRENDS

Prácticas para desenvolverse en entornos híbridos y multicloud y ser competitivos

La combinación de entornos privados con las nubes públicas ha dado lugar a una nueva forma de TI híbrida de la que la empresa obtiene las ventajas de ambas modalidades, pero también sus desafíos: aprender a arbitrar las cargas de trabajo, segmentar las arquitecturas y a la vez integrarlas para poder mover aplicaciones y datos y, además, proporcionar herramientas que aporten agilidad a la administración de estos entornos.

(De izq. a dcha) Jorge Marín (Ikusi), Agustín Sánchez (NFON), Miguel López (Making Science), Nieves González (Dell Technologies), José Manuel Marina (Crayon Software), Antonio Picazo (Micro Focus) y Ceferino Raposo (Sothis). Clic para ver

“Como el entorno multicloud aumenta la complejidad, se necesita una estrategia global y la contratación y retención del personal adecuado”

JOSÉ MANUEL MARINA, CRAYON SOFTWARE

Además, es cada vez más común que las empresas distribuyan sus activos entre varias nubes, lo que puede añadir mayor complejidad a la estructura tecnológica de la empresa. Administrar estos entornos de nube híbrida y mutlicloud es posible con las recomendaciones que dejaron en el Encuentro IT Trends “Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos Cloud híbridos”, en el que participaron portavoces de Crayon Software, Dell Technologies, Ikusi, Making Science, Micro Focus, NFON, y Sothis.

Para conseguir ser competitivo, el negocio busca mucha innovación y reducir el tiempo de despliegue de nuevos servicios. “IT busca simplicidad, más eficiencia, escalabilidad y elasticidad. Es decir, que en determinados momentos, como en rebajas, un retail pueda coger cargas de nubes públicas y traerlas a las nubes privadas”, ejemplificó Nieves González, Manager Systems Engineer de Dell Technologies durante la mesa redonda sobre prácticas para desenvolverse en entornos híbridos y multicloud, y en cuya opinión, el reto de las empresas es controlar el coste consiguiendo innovación y adaptándose a los cambios.

Para José Manuel Marina, director general de Crayon, el mayor desafío de adaptación al

“No todo es consumible desde la nube pública o todo se tiene que transformar desde el data center”

NIEVES GONZÁLEZ, DELL TECHNOLOGIES

entorno multicloud es que el cliente puede no estar preparado realmente. Consumir servicios en la nube de varios proveedores es complejo y difícil de gestionar y hay que hacerlo con una estrategia determinada. “Como el entorno multicloud aumenta la complejidad, se necesita una estrategia global y la contratación y retención del personal adecuado con conocimientos on premise dispuestos a reciclarse de manera continua”, apuntó.

En este contexto, los CIO, además, han de decidir qué tipo de aplicaciones o servicios han de ubicarse en cada tipo de proveedor y dónde ubicar cada carga de trabajo. Cada servicio puede necesitar más registros de seguridad, más requisitos de cumplimiento normativo o más elasticidad. “Tener un servicio en cloud es lo mismo que tenerlo en el data center en el sentido de que es un servicio más que hay que gestionar. Para el cliente el proceso ha de ser totalmente transparente”, destacó Antonio Picazo, preventa de soluciones de Micro Focus.

Desde Making Science, Miguel López, CTO y Head of Infrastructure Operations, señaló que el Cloud, aunque presenta más beneficios que contras, conlleva unas elevadas necesidades de control. Además, “en los últimos años se han unido el multicloud con la contenerización. Pero no hay que olvidarse de la seguridad. Cuando se trabajaba con data centers había que usar máquinas físicas, pero ahora se piden máquinas virtuales dando a un botón

OPTIMIZANDO LA UBICACIÓN DE LAS CARGAS DE TRABAJO EN LA NUBE HÍBRIDA

A comienzos de 2020, IDC investigó acerca de cómo las organizaciones determinan la ubicación de las cargas de trabajo a medida que evolucionan en su transformación digital (DX). Entre sus hallazgos, señala que las principales consideraciones para determinar la ubicación de las cargas de trabajo entre la nube tradicional en las instalaciones y la nube pública y privada incluyen la seguridad, el rendimiento, la facilidad de administración, la disponibilidad, el coste, el cumplimiento, la agilidad, los patrones de uso y la importancia de los datos.

“Las redes tradicionales no están preparadas para abordar las cargas de trabajo tan grandes”

JORGE MARÍN, IKUSI

y esto ha llevado a un problema de gobierno que se está intentando paliar. Muchos proveedores intentan que la gestión de clusters y Kubernetes estén centralizados para tener políticas centralizadas, dando cierta libertad a los diferentes equipos. Pero muchas empresas han dado un salto a cloud sin saber cómo gestionar o controlar. Cada proyecto se ha hecho de manera diferente”.

En este sentido, Antonio Picazo, de Micro Focus, apuntó que ese control tiene que llevarse a cabo desde el primer momento sin perder agilidad. “No puede ocurrir que para que algo sea desplegado pasen días y días. Hay que tener una solución de gestión fácil; es decir, que se pueda acceder solo con un clic, pero centralizada para poder iniciar el control. Y es importante evitar el vendor lock-in de un proveedor de cloud. Las soluciones han de poder mover cargas de un sitio a otro, todavía la tecnología en caliente y tiempo real es complicada, pero hay que tener en cuenta que se puedan tener soluciones que nos ayuden en otro momento”.

Ceferino Raposo, Business Architect de Sothis, indicó que no solo hay que centrarse en la oferta tecnológica, sino que hay que cribarla según las necesidades de la organización. “Además, el número de recursos o soluciones queda limitado si se hace ese trabajo previo. El marco de referencia han de ser los objetivos estratégicos y las mejores herramientas, ya sean locales en el CPD o en la nube. A partir de ahí se pueden establecer los mejores mecanismos y técnicas de control”.

“Muchas empresas han dado un salto a cloud sin saber cómo gestionar y controlar el proyecto”

MIGUEL LÓPEZ, MAKING SCIENCE

Para este experto, es importante la comunicación entre equipos de desarrollo y equipos de sistemas porque no solo hay que ver si una máquina funciona bien o mal, sino si el proceso se está realizando de manera óptima. “Se está produciendo un cambio de cultura en el que los desarrolladores hablan más con los de sistemas. Y eso es un trabajo colaborativo entre todos para que no se disparen los costes. La gente pierde la perspectiva de que lo que va al cloud son las aplicaciones y por eso también se olvidan de que la aplicación se ha diseñado como un silo. Por eso lo mejor es saber de qué manera van a llegar los usuarios a mis aplicaciones. Hay que tener en cuenta lo que quiero hacer, cómo lo quiero hacer y cuáles son los mejores elementos para lograrlo”.

Respecto a la decisión de dónde ubicar las aplicaciones, Nieves González, de Dell Technologies, recuerda que “existen distintas aplicaciones: algunas se despliegan desde las nubes públicas, y otras se mantendrán en el data center. Existe un gran porcentaje de aplicaciones que se transformarán a una nube privada o a una nube pública en función del dato o los controles o tendrán que sufrir una rearquitectura para ser realmente movibles. No todo es consumible desde la nube pública o todo se tiene que transformar desde el data center. Lo que es necesario es que todas aplicaciones han de mantenerse de manera resistente”, puntualizó.

Junto a esta decisión, las empresas también necesitan decantarse por una plataforma de

“Hay que tener una solución de gestión fácil, que se pueda acceder solo con un clic, pero centralizada para poder iniciar el control”

ANTONIO PICAZO, MICRO FOCUS

red adecuada al entorno cloud. En opinión de Jorge Marín, Service delivery manager de Ikusi, la situación de incertidumbre total hace que las empresas necesiten una plataforma inteligente que responda a casi cualquier situación. “Las redes tradicionales no están preparadas para abordar las cargas de trabajo tan grandes, por eso existen armas que se deben facilitar a las empresas como la automatización de las operaciones de networking y el análisis de la IA para tener perspectivas más inteligentes del negocio”, indicó.

Asimismo, la recomendación de Jorge Marín es una estrategia de red proactiva y multicloud, que alinee las prioridades de la nube, la seguridad y las aplicaciones de los departamentos de IT. Para que esta estrategia tenga éxito tiene que apoyarse en la carga de trabajo, el acceso y la seguridad. “Se debe adoptar un modelo operativo para administrar las políticas de manera más ágil y en cuanto al acceso, hay que implementar soluciones del tipo SD-WAN para reducir los costes operativos. También ha de reducirse el riesgo asociado a los usuarios con distintas soluciones ya que las apps están en diferentes nubes”, explicó Marín.

FLEXIBILIDAD DEL CLOUD SÍ, PERO CONTROLANDO LA INTEGRACIÓN

Agustín Sánchez, responsable de Desarrollo de negocio de NFON, puso en su intervención el foco en el SaaS que presta servicios como las

SIMPLIFICANDO EL DESPLIEGUE DE SERVICIOS CLOUD PARA POTENCIAR LA TRANSFORMACIÓN DIGITAL

Muchas empresas buscan la nube para ofrecer agilidad, velocidad y escalabilidad para ejecutar con éxito sus transformaciones digitales, desde la creación de valor con la entrega acelerada de aplicaciones, servicios de plataforma e infraestructura, o la mejora de la experiencia del cliente, garantizando el cumplimiento y reduciendo costes mediante la automatización de procesos. Sin embargo, para ofrecer todas esas capacidades y reducir la complejidad asociada con la administración de entornos híbridos y de múltiples nubes, debe contar con las correctas herramientas de administración de la nube.

“El cloud te da proceso, capacidad de almacenaje, pero al otro lado también hay una aplicación de infraestructura que funciona bien, y está el receptor”

AGUSTÍN SÁNCHEZ, NFON

comunicaciones unificadas. Y ejemplificó bien esa complejidad y necesidad de integrar equipos y aplicaciones que se da en el entorno de la infraestructura, con el uso de aplicaciones de telefonía en la nube, para las cuales “hay que comprobar si se dispone del equipo adecuado, con suficiente RAM, y la compatibilidad de los sistemas para usar Teams y el teléfono a la vez”, apuntó.

En su opinión, “el cloud te da proceso, capacidad de almacenaje, pero al otro lado también hay una aplicación de infraestructura que funciona bien, y está el receptor. El mercado, especialmente la pyme, han aprendido que el cloud te permite tener también una buena comunicación sacando fuera el servicio, y ser flexible para poder mover tu centralita on premise a casa si surge un problema. El consumo flexible o quitarle carga de trabajo al responsable de redes han transformado la percepción de los servicios de comunicaciones en la nube”.

Otro efecto de la situación que estamos viviendo es la demanda de teletrabajo. En este sentido, José Manuel Marina, de Crayon, explicó que, en su caso, “hemos ayudado a los clientes a entender qué es lo que tienen que

SOLUCIONES CLOUD PARA LA CONTINUIDAD DEL NEGOCIO EN ENTORNOS VUCA

La nueva era digital que se dibuja en la actualidad está transformando no solo la forma en que las empresas están gestionando su relación con los clientes reales, sino también la forma en que las organizaciones ofrecen, acceden y consumen servicios y aplicaciones.

En este escenario de continuidad, IDC indica en este documento que las comunicaciones han sido la palanca que ha permitido a las organizaciones poder afrontar el proceso de recuperación y habilitar la transformación del puesto de trabajo, permitiendo la movilidad del empleado y la puesta en marcha de entornos colaborativos.

“El marco de referencia han de ser los objetivos estratégicos y las mejores herramientas, ya sean locales o en la nube. A partir de ahí se pueden establecer los mejores mecanismos y controles”

CEFERINO RAPOSO, SOTHIS

cargar y cómo hacerlo. Ofrecemos una plataforma multinube con nuestra propia IP con la que pueden aprovisionarse de soluciones y detectar posibles incidencias”.

Y sobre la calidad de servicio que apuntaba el portavoz de NFON, Miguel López, de Making Science, señaló que no puede olvidarse la gestión de las expectativas. “El cloud ha permitido tener muchos más KPIs, ya sea on premise o en cloud para sacar métricas de calidad de servicios. Muchos clientes están haciendo análisis con servicios cloud para que no se vaya información confidencial, pero también para transcribir las comunicaciones y analizar sentimiento para saber cual es la media en todos sus operadores”, concluyó.

Para ver la charla completa, accede aquí. ■

Si te ha gustado este artículo, compártelo

NUBE HÍBRIDA O TI HÍBRIDA: PERCEPCIONES PARA LA RESILIENCIA CORPORATIVA

Cuando se produjo la irrupción de la nube, la mayoría de los pronósticos apuntaban a que la migración de las TI corporativas a ese entorno sería la opción general a corto o medio plazo. Y con la aparición de la nube híbrida, parecía que las reticencias al traslado derivadas de las exigencias de seguridad y cumplimientos estaban salvadas y el camino hacia la migración despejado. Sin embargo, hoy se habla de TI Híbrida. ¿Cuál es la mejor estrategia, optar por la nube híbrida o por la TI híbrida? En este dossier, se analizan las diferentes opciones, para intentar allanar el camino de los CIOs hacia la respuesta que se adapte con mayor precisión a las necesidades específicas de su organización.

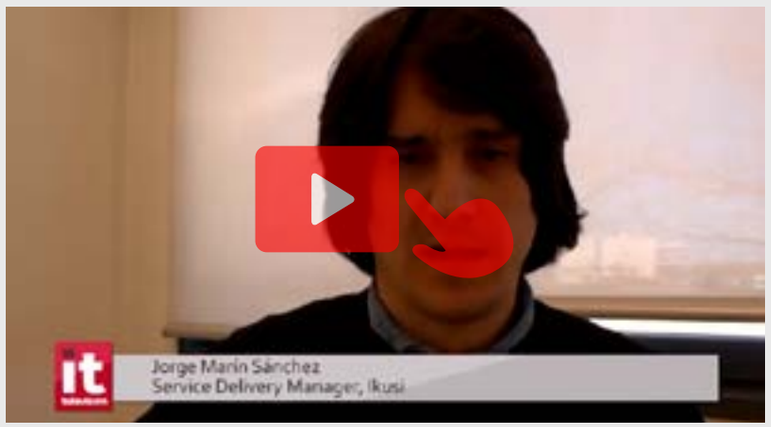
Gestión de entornos multicloud e híbridos, mejores prácticas

“Tratar los datos en los entornos híbridos requiere de una gran capacidad de análisis” (Sothis)

“Apoyamos las necesidades de comunicaciones unificadas basadas en cloud” (NFON)

“Apostamos por una solución que nos permita tener una ventanilla única” (Micro Focus)

“Ayudamos a los clientes a sacar el máximo partido a su transformación digital” (Making Science)



“Las redes inteligentes son uno de los pilares de una estrategia de entornos multicloud” (Ikusi)

“Ayudamos a evitar la repatriación de aplicaciones desde la nube” (Dell Technologies)

“Antes de migrar al cloud hay que prever qué va a ocurrir en el cloud” (Crayon)

making science

BRINGING TECHNOLOGY TO BRANDS

YOUR PARTNER FOR
DIGITAL BUSINESS

www.makingscience.com

#ENCUENTROSITTRENDS

¿Cómo protejo mis activos en un entorno de nube híbrido? Aspectos a tener en cuenta

Uno de los principales escollos del cloud es su seguridad. Así se constata en el informe IT Trends 2021, asimilando la aceleración digital. Un 17% de los consultados adjudica a la seguridad de la nube un papel estratégico para este 2021. Además, la ciberseguridad se considera una inversión prioritaria en estos doce meses. La protección de los datos, las aplicaciones y las infraestructuras que dan acceso y con las que se construyen las nubes híbridas, es una máxima siempre presente en la mente de los responsables tecnológicos de las empresas.

Sobre todo ello debatieron portavoces de Barracuda, Check Point, Commvault, Entrust, Sonicwall y Thales Data Protection, en el Encuentro IT Trends "Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos de cloud híbridos".

Uno de los primeros puntos que se abordaron en el debate fue la durabilidad de estos

(De izq. a dcha) Elisa Martínez (Commvault), Sergio Martínez (Sonicwall), José Pérez (Entrust), Alfonso Martínez (Thales), Eusebio Nieva (Check Point), Miguel López (Barracuda). Clic para ver

“Muchos clientes creen que el cloud no es tan seguro por la novedad, pero es importante planificar la migración y no dejar que únicamente sean las circunstancias las que nos lleven hacia allí”

MIGUEL LÓPEZ, BARRACUDA

entornos híbridos, un modelo que parece que permanecerá durante mucho tiempo a la luz de las experiencias de los clientes y de las normativas que rigen ciertos mercados. Y así lo deben garantizar las tecnologías que dan soporte a dicho modelo. “Es verdad que existen soluciones 100% cloud, como Office 365 o Salesforce que se despliegan totalmente en la nube, pero también hay situaciones en la que los clientes siguen manteniendo sus aplicativos on premise o legacy, y hay que seguir dándoles protección a estos entornos”, explicó Elisa Martínez, responsable de Metallic para España y Portugal de Commvault, quien se refirió a la normativa de la European Bank Agency, que establece como preceptivo para las entidades financieras que tengan una estrategia de salida del cloud para recalcar la necesidad de acompañar a las empresas allá donde tengan sus activos, “de una manera transparente. Hay que mantener garantizada la calidad de los datos, la integridad de la plataforma y la seguridad del ecosistema”.

Y es que tan seguro puede ser un entorno como el otro, En opinión de Miguel López, Country Manager de Barracuda para la región de Iberia, “todo depende de las medidas que se adopten en cada uno de ellos. El diferencial del entorno de seguridad on premise con el cloud es que este último

“Hemos de saber qué herramientas específicas de seguridad tiene que haber en un entorno on premise o en cloud, porque estas herramientas pueden ser específicas de un entorno o de ambos”

EUSEBIO NIEVA, CHECK POINT

ha conseguido democratizar el acceso a la seguridad. Los niveles de seguridad y resiliencia antes eran muy complejos para una empresa pequeña o mediana ya que, para ellas, la seguridad en cloud trae consigo nuevos interrogantes. Muchos clientes creen que el cloud no es tan seguro por la novedad, pero es muy importante planificar la migración y no dejar que únicamente sean las circunstancias las que nos lleven hacia allí”, aconsejó. Y una vez esté claro el plan, “se pueden desarrollar muchos pasos para tener un entorno mucho más seguro que on premise”.

Para tener todos estos entornos bajo control, “es importante contar con herramientas consistentes y homogéneas que permitan desplegar políticas de seguridad y visibilidad en cloud consecuentes con lo que ya tenía la empresa on premise”, sin pasarse por alto algunas administraciones que parecían tener poca importancia.

Aún con todo, “no hay que olvidar que el cloud incorpora nuevas amenazas para los entornos tecnológicos, como las autorizaciones de las administraciones, bajo qué condiciones se suben imágenes o se hace un despliegue de cargas en la nube o qué herramientas de terceros, incluso open source, se despliegan”, apuntó Eusebio Nieva, director técnico de Check Point.

Todo esto era más fácil de controlar on premise. Ahora la mayoría de los problemas surgen por ese tipo de desconfiguraciones. “Siempre

CLOUD SECURITY POSTURE MANAGEMENT

CloudGuard Posture Management permite a las empresas administrar fácilmente la seguridad y el cumplimiento de sus entornos de nube pública a cualquier escala en AWS, Microsoft Azure, Google Cloud Platform y Kubernetes. Además, visualiza y evalúa la actitud hacia la seguridad, detecta configuraciones incorrectas, modela y aplica activamente las políticas estándar y protege contra ataques y amenazas internas. Las organizaciones usan CloudGuard para operaciones de seguridad en la nube más rápidas y efectivas, cumplimiento y gobernanza sin problemas y prácticas de DevOps resistentes.

“De una manera transparente, hay que mantener garantizada la calidad de los datos, la integridad de la plataforma y la seguridad del ecosistema”

ELISA MARTÍNEZ, COMMVAULT

hay que tener en cuenta la parte del perímetro interno o el data center junto con la nube para saber coordinar ambos entornos a la vez y, además, saber qué herramientas específicas de seguridad tiene que haber en uno u otro entorno porque estas herramientas pueden ser específicas de un entorno o de ambos”, destacó. Si una empresa no tiene control, da igual que tenga visibilidad porque va a ser imposible evitar los incidentes.

Además, muchas organizaciones que están en el cloud no son conscientes de la problemática de la protección y la localización de los datos sensibles. En este sentido, Alfonso Martínez, country manager de Thales Data Protection, señaló que “el reto es securizar el entorno híbrido a la vez que el data center y tener visibilidad de los dos mundos. Muchas empresas han saltado a la nube de la noche al día por el miedo tras el año de pandemia y no han podido entrar en este entorno con toda la seguridad que les hubiera gustado”, subrayó. “A eso se le añade que el personal que está usando la nube está sobrecargado y a veces no han sido formados específicamente para manejar estos entornos de nube”. Y ante esto, “es imprescindible herramientas que permitan a las organizaciones descubrir y clasificar su información, independientemente de dónde esté, para luego implementar las medidas oportunas de cifrado, tokenización o enmascaramiento”.

Para José Pérez, Sales Engineer de Entrust, “el cifrado es una herramienta indispensable en el cloud hoy en día y es la última frontera antes de

“Hay que tener en cuenta qué infraestructuras, qué aplicaciones y qué datos se quieren subir a la nube prestando especial atención a los datos más críticos para añadirles medidas adicionales de seguridad como el cifrado”

JOSÉ PÉREZ, ENTRUST

acceder al dato. El hecho de que las empresas estén sacando datos que tenían dentro de casa hacia afuera, es algo que hace unos años hubiera sido impensable para un auditor. Y otros elementos que explica la importancia del cloud en el cifrados son las regulaciones, como las que tiene que cumplir el sector bancario con PCI-DSS”.

Respecto al acceso a la nube seguro, Sergio Martínez, Iberia Regional Manager de SonicWall, adviertió que “estamos en un momento de aceleración, donde las credenciales son la nueva frontera. Los ataques de ransomware han aumentado en un 60%. Acceder a los recursos de la compañía en remoto, se ha convertido en clave. Hay que desplegar el doble factor de autenticación, pero, ojo, porque los SMS están dejando de ser seguros. Hay que asegurar una defensa por capas para que los dispositivos remotos sean de confianza con un control del endpoint y hacer un enforcement para que los usuarios finales sean de confianza”.

Además, añadió que todo el tráfico ha de ser monitorizado para al menos que en las capas de defensa tradicional sean válidas. “Restituir los end point a las situaciones anteriores es clave. Si todo falla hay que desplegar también antivirus de nueva generación que permitan detectar todo aquello que pueda engañar al usuario”.

Aludiendo a esos volúmenes de ransomware citados por el portavoz de Sonicwall, Elisa Mar-

“Hay que asegurar una defensa por capas para que los dispositivos sean de confianza, con control en el endpoint y un enforcement para que los usuarios finales sean de confianza”

SERGIO MARTÍNEZ, SONICWALL

tínez, de Commvault, apuntó que “este año de tremenda aceleración para poder trabajar en casa, ha provocado que se adoptaran multitud de herramientas colaborativas donde la cloud ha sido crítica. Office 365 con Teams y su parte de Exchange han sido uno de los facilitadores y se han convertido en un gran valor para las compañías que las utilizan para gestionar proyectos, contratos u ofertas. Pero lo peor es que un año después de estos despliegues no se tienen en cuenta todas las vulnerabilidades en muchas empresas. Es ahora cuando se están implementando políticas de backup, ransomware y recuperación de la información en el caso de que ocurra, para volver al momento que se encontraba la empresa antes”.

Sobre estos ataques, Miguel López, de Barracuda, señaló que “estamos viendo que el malware funciona en un contexto de coste-beneficio y van a atacar a los eslabones más débiles de la cadena independientemente del tamaño de la compañía, aunque a veces en la prensa solo se vean reflejados los grandes ataques”.

Por esta razón, los CISO demandan ayuda a los proveedores desde el punto de vista de seguridad y, en muchas ocasiones para tener visibilidad, ya que los propios activos en la nube son desconocidos para estos profesionales. “Los departamentos de desarrollo a veces utilizan parte de la nube antes de ofrecer un producto a todos los clientes. Por eso, embeber los controles y los pasos de desarrollo es de lo más importante.

Esta es una carencia para la mayoría de las compañías", añadió Nieva durante el debate.

Otro punto clave al hablar de la seguridad de la nube es la responsabilidad: "los responsables de seguridad de las empresas tienen que saber securizar los datos después de haberlos subido a la nube. El último responsable de sus datos es la empresa no el proveedor de nube. Se puede proteger con muchos sistemas y controles, pero, si todo falla, hay que cifrar archivos, carpetas y aplicaciones. Es importante que los clientes tengan la posibilidad de compatibilizar nubes ya sea Amazon, IBM Cloud, Google Cloud o la que sea para configurar su propia estrategia", destacó durante la mesa redonda el country manager de Thales Data Protection.

Como remate al encuentro, José Perez, de Entrust, señaló que "l mejor consejo para una empresa es que se deje asesorar por expertos en cloud para poder hacer esa migración. Después hay que tener en cuenta qué infraestructuras, qué aplicaciones y qué datos se quieran subir prestando especial atención a los datos más críticos con medidas adicionales de seguridad, como el propio cifrado".

Para ver la charla completa, accede aquí.

"Son imprescindibles herramientas que permitan descubrir y clasificar información, independientemente de dónde esté, para luego implementar las medidas oportunas de cifrado, tokenización o enmascaramiento"

ALFONSO MARTÍNEZ, THALES DATA PROTECTION

LAS BASES PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CUALQUIER ORGANIZACIÓN

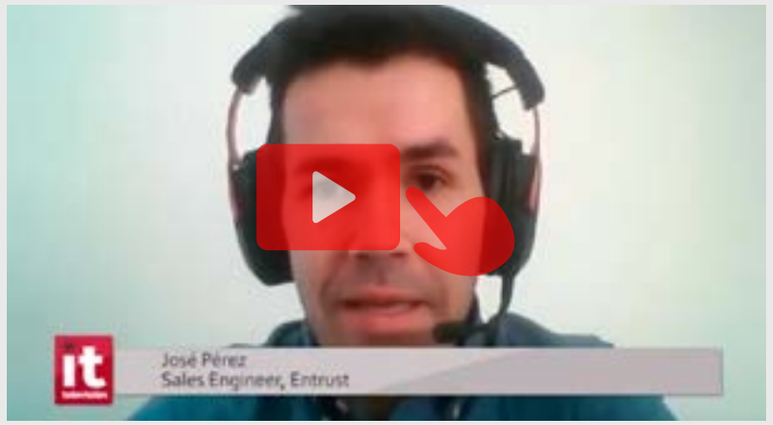
Con la proliferación de datos en la actualidad, el auge de los reglamentos de privacidad, el aumento en el uso de la nube y la persistencia de amenazas avanzadas, una seguridad centrada en los datos permite tener el control de los datos sin importar dónde estén y evitar así que los ladrones de datos los puedan leer. Pero, para ser efectiva, esta protección debe actuar automáticamente sin depender de la intervención del usuario. Este libro blanco se centra en los desafíos que supone la seguridad de los datos en esta era de proliferación de datos. También ofrece estrategias para localizar y clasificar sus datos críticos y aplicarles una seguridad centrada en los datos.

Si te ha gustado este artículo, compártelo

¿Cómo proteger mis activos en un entorno de cloud híbrida?

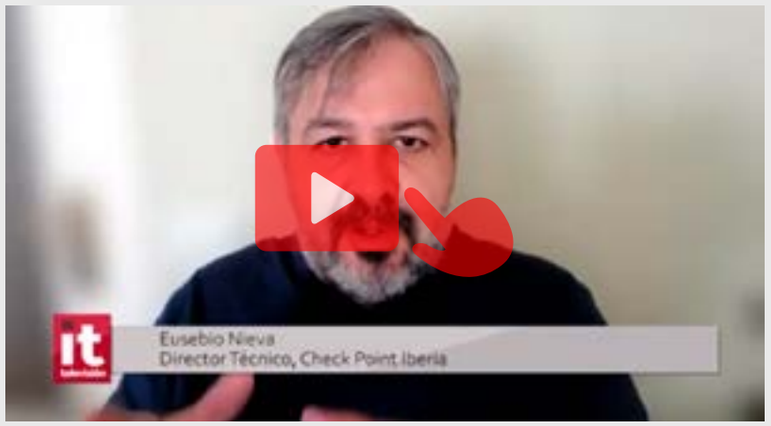
“La seguridad de los datos comienza con su localización” (Thales)

“La seguridad SASE Zero Trust es el nuevo paradigma” (SonicWall)



“No es buena idea migrar la nube sin cifrado” (Entrust)

“Las plataformas de backup y recuperación deben asegurar la integridad de la información” (Commvault)

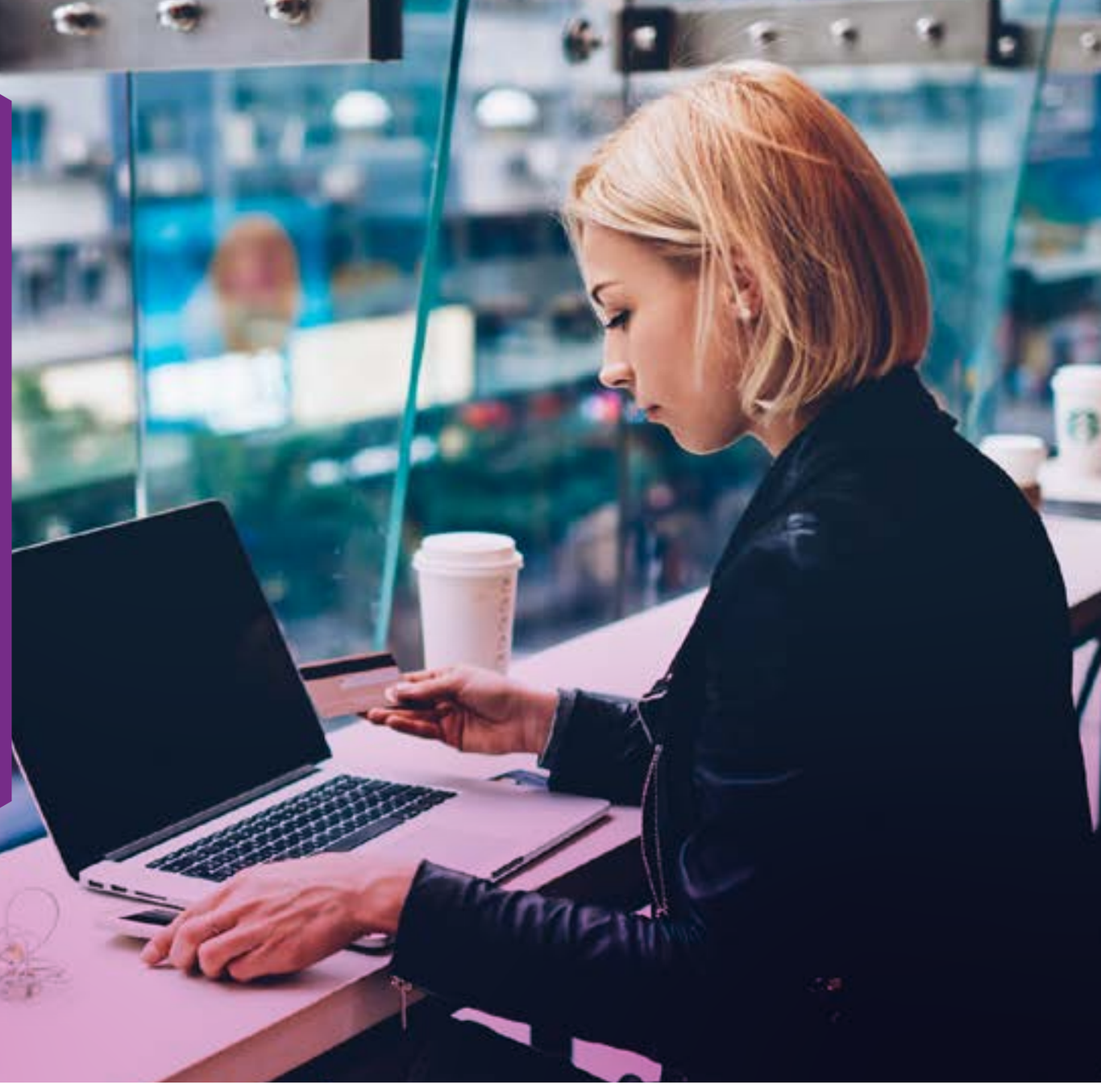


“Lo más importante es una protección unificada y nativa en la nube” (Check Point)

“Proponemos herramientas para tener seguridad, visibilidad y control también en la nube” (Barracuda)

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN



ENTRUST

ENTREVISTA

“Necesitamos modelos de infraestructura centralizada que permitan la transformación digital plena en la Universidad”

ANDRÉS PRADO, CRUE UNIVERSIDADES ESPAÑOLAS

La pandemia ha impulsado la transformación digital. También en el ámbito académico, uno de los más perjudicados por la Covid. Ahí es donde el Plan Director 2020, comenzado en 2018 por la conferencia de rectores Crue Universidades Españolas, ha resultado ser visionario. La importancia otorgada en el mismo a tendencias como blockchain y su aplicación en la Universidad, lucen hoy como un faro en la carrera acelerada hacia la adopción de una tecnología que nos ayude a navegar los convulsos tiempos que nos ha tocado vivir. Andrés Prado, Coordinador del grupo de trabajo “Dirección de TI” en Crue, repasa algunas de las claves de este fascinante proyecto.

Arancha Asenjo y Alberto Varet

Uno de los ambientes más trastocados por la pandemia es el de la educación. ¿Cómo conseguir formar a los estudiantes sin clases presenciales? ¿De qué manera pueden las innovaciones digitales solventar los problemas derivados de la Covid? Como si hubiera previsto tan penosa situación, Crue Universidades Españolas, una asociación sin ánimo de lucro formada por 76 instituciones nacionales (50 públicas y 26 privadas), puso en marcha, en 2018, el Plan Director 2020, una estrategia dirigida a estructurar acciones que aplicasen la tecnología a la vida universitaria. El tiempo y las circunstancias han acabado por darle la razón a sus responsables dos años después.

Uno de ellos es Andrés Prado, Coordinador del grupo de trabajo "Dirección de TI" en Crue Universidades Españolas, quien asegura que el valor de esta conferencia de rectores está en "su capacidad para ser la voz de referencia de las universidades con todos los agentes que tienen implicación en el sistema español de educación, investigación y transferencia". Una situación de privilegio que tiene, hoy más que nunca, un fuerte componente tecnológico que el entrevistado desgrana de esta manera: "Crue se estructura en torno a comisiones sectoriales compuestas por expertos dentro del ámbito universitario. Estos son responsables de las actividades que nuestra agrupación considera esenciales. Una de ellas es la

"Tratamos de diseñar un plan director o de actividad centrado no en la tecnología en sí misma, sino en los distintos ambientes de actuación con ellas"

tecnología, de la que surge la sectorial de TI, que tiene tres ejes fundamentales: el primero es el asesoramiento sobre su adopción en las misiones universitarias; el segundo, la evaluación de la capacidad tecnológica aplicable en docencia, investigación y gestión universitaria; y el tercero, el establecimiento de un elemento de colaboración entre esos proyectos con un marcado componente tecnológico".

La aguja que enhebra estos tres puntos es el citado Plan Director 2020, elaborado a iniciativa del rector de la Universidad de Jaén, quien pretendía impulsar una idea que fuera más allá de la asistencia de grupos de trabajo. El resultado acabó por dar visibilidad a la estrategia de Crue en el ámbito tecnológico desde una perspectiva claramente tangencial. "Tratamos de diseñar un plan director o de actividad centrado no en la tecnología en sí misma, sino en los distintos ambientes de actuación con ellas. Nuestra labor, pues, ha ido dirigida a estructurar todo ese tipo de acciones en torno a los susodichos ejes estratégicos, pero no tanto desde el punto de vista de las tendencias como de su aplicación en la universidad", argumenta el Director TIC.

Una esmerada tarea que consta de seis grandes bloques:

1. **Gestión de las TIC en el entorno universitario:** "Tratamos de identificar modelos de referencia en sociedad para luego adoptarlos en las diferentes instituciones".
2. **Tres grandes ejes relacionados con la actividad académica:** "La tecnología en la docencia, el ámbito de la investigación (donde se ha abrazado el prototipo europeo Open Science o ciencia abierta) y la aplicación de las innovaciones en la gestión universitaria".
3. **Administración digital:** "Buscamos un acercamiento a la comunicación en la Universidad marcada por conceptos como la movilidad o la conexión permanente".
4. **Gobierno del dato:** "Se ha trabajado en reconocer diferentes patrones para después decidir cuál era el más flexible a la hora de ser adaptado a las instituciones".
5. **Cultura digital:** "En el más amplio término. Aquí tuvimos en cuenta otro de los elementos más fundamentales en los últimos años: el de las competencias digitales. Es decir, esos temas más candentes que las universidades han tenido que ir adoptando".

6. Empoderamiento de los profesionales de la tecnología en nuestro medio: "Este último año, muchas de las instituciones han puesto en valor nuestras actividades. Nos estamos convirtiendo en una pieza fundamental dentro de esos espacios tan complejos que son las universidades".

Seis verticales muy estimulantes que, sin embargo, pueden ser un quebradero de cabeza a la hora de llevarlos a la práctica. ¿Cómo hicieron desde Crue para financiarlos y ejecutarlos? "Financiación hay poca. Es una labor puramente altruista de profesionales del sector que entienden que en el trabajo conjunto hay beneficio para todos. Es verdad que luego hay iniciativas que tienen un desarrollo más allá de la sectorial y que acaban por convertirse en un proyecto en sí mismas. Incluso en soluciones que sí terminan por llevar una línea de financiación. Pero nuestra labor es de asesoramiento, identificación de buenas prácticas y de tratar en muchos casos que esas buenas prácticas tengan una facilidad de adaptación y adopción por cada una de las universidades".

"Nuestra labor es de asesoramiento, identificación de buenas prácticas y de tratar en muchos casos que esas buenas prácticas tengan una facilidad de adaptación y adopción por cada una de las universidades"

La valía de semejante esfuerzo fue refrendada por el duro y atípico año 2020. Andrés Prado explica cómo llegaron a alcanzar unos números que incluso les sorprendieron a ellos mismos: "El 95% de los 73 proyectos propuestos fueron abordados a pesar de la pandemia, y 44 de estos se han culminado con éxito. Un resultado muy satisfactorio, sobre todo si tenemos en cuenta que algunas de estas líneas de acción tienen aún recorrido".

Una de esas líneas relaciona blockchain con la universidad. Se llama BLUE y ha surgido "de una dinámica de lanzar informes para poner en contexto la tecnología en la universidad". "Fue algo así como un pequeño análisis estratégico en el que incorporábamos diferentes puntos de vista para saber dónde y cómo adoptar blockchain en las instituciones educativas. El trabajo contó con la colaboración coordinada de RedIRIS (red española para Interconexión de los Recursos InformáticoS de las universidades y centros de investigación). Gracias a ellos, avanzamos en la mejora de procesos centrados en la actividad del estudiante. Y luego, tuvimos la suerte de coincidir en el tiempo con una iniciativa a nivel europeo llamada EBSI (The European Blockchain Services Infrastructure), que empezamos asimismo a coordinar, y que tiene un caso de uso dedicado a las certificaciones académicas", expone Andrés Prado.

Aparte de blockchain, la labor con RedIRIS se extiende a otros proyectos también de suma importancia para nuestro país que el entrevistado explica así: "Con ellos y el Ministerio de Universidades trabajamos igualmente para que las líneas de financiación puedan aportar novedosos mecanismos de transformación dentro del sistema universitario español. Es decir, que sean propuestas para mejorar como sistema, pues estamos viendo que hay una verdadera necesidad de adoptar modelos de infraestructura centralizada y consumo distribuido y personalizado que permitan acceder a una transformación digital plena en nuestro ámbito".

Sí, el famoso cambio de paradigma que tantas veces nos ha llevado a preguntarnos por el estado de las cosas en el mundo empresarial es igualmente palpable en el ambiente de la Universidad desde, al menos, 2018. "El informe TIC 360 de hace dos años trataba,

justamente, de la transformación digital de las universidades. Ahí estaban nuestras reflexiones sobre cómo enfocar las cosas en el presente para poder evolucionar en el futuro. 2020 ha puesto de manifiesto la pertinencia de nuestro estudio, así como el estado real de la digitalización de las universidades. El caso es que nunca tuvimos mayor visibilidad en la comunidad universitaria como hoy. Tampoco hubo nunca tanta aceptación de nuestros servicios y adopción de los mismos. Hemos tenido unos reconocimientos insólitos. En el fondo, este año sirvió para poner de manifiesto el valor de los proyectos en los que trabajamos durante mucho tiempo. Unos proyectos que han elevado la cultura digital universitaria", asegura el Director TIC.

Un triunfo meridiano de la propuesta de Crue que nos recuerda que la ruta hacia la digitalización es tan solo un camino que hemos empezado a andar, y que será demasiado arduo sin nuevas vías de financiación. En palabras de Andrés Prado: "Enriquecería mucho en el medio universitario la adopción digital en términos generales. Hablo de consumo de infraestructuras de software como servicio. Creo que ese ámbito personalizado es importante trabajarlo en la educación. Aparte, es necesario hacer una reflexión madura sobre las estructuras de las organizaciones y, dentro de las mismas, de las áreas de innovación. Capacitar a los profesionales en un entorno que se mueve imparable y en el que sus propios roles dentro de la universidad no dejan de evolucionar. La tecnología no se gestiona hoy como hace veinte años, y eso nos debe hacer reflexionar. Es un pilar fundamental para el desarrollo de la actividad universitaria".

La universidad, pues, no sólo como un foco de conocimiento, también como una palanca de la revolución digital en la que vivimos inmersos. ¿Pueden, entonces, ser las instituciones educativas generadoras de ese talento que tantas veces se demanda? Andrés Prado lo tiene claro: "Por supuesto. Las universidades han fortalecido los ambientes de emprendimiento. Esas misiones deben tener cabida igualmente en la universidad moderna. Que ésta no sólo sea transferencia, sino también capacidad para el emprendimiento".■

"Las universidades han fortalecido los ambientes de emprendimiento. Esas misiones deben tener cabida igualmente en la universidad moderna. Que ésta no sólo sea transferencia, sino también capacidad para el emprendimiento"

MÁS INFORMACIÓN

- CRUE Universidades Españolas
- El futuro de la educación pasa por un modelo de enseñanza híbrido
- La educación contribuye a frenar la caída del mercado de redes inalámbricas

Cisco Partner

IKUSI velatia

Aryse 360º

UNA SOLUCION INTEGRAL AVANZADA PARA TODAS TUS NECESIDADES

Te presentamos Aryse360º, la única solución integral de la industria que unifica Conectividad, Seguridad y Colaboración para que solo tengas que preocuparte por tu negocio.

www.aryse360.com

Cuota mensual
Todo Incluido, HW, SW,
Mantenimiento y
Servicios profesionales

it TRENDS

OPINIÓN

Diez empresas Big Tech con aplicaciones prácticas de computación cuántica

Jorge Díaz-Cardiel,
Socio director general de
Advice Strategic Consultants

Abu Dhabi comienza a construir la primera computadora cuántica de los Emiratos Árabes Unidos (UAE); el laboratorio que construye la computadora cuántica también tiene como objetivo producir microchips 'hechos en Abu Dhabi' para fines del verano de este año. Lo más significativo es que Abu Dhabi ha comenzado a fabricar su propia computadora cuántica con el objetivo de generar avances en el descubrimiento de fármacos y tecnología de baterías. Es decir, que hay una finalidad comercial, práctica. Y esto es un grandísimo avance: cuando aquí, en IT User publicamos sobre computación cuántica el 1 de octubre de 2019, aún no había aplicaciones prácticas, versus la computación "tradicional". Y, dejamos claro que la "Ley Moore" seguía siendo plenamente vigente.

El nuevo CEO de Intel Corporation, Pat Gelsinger, va a invertir 20.000 millones de dólares en recuperar el liderazgo que le disputan Nvidia, QUALCOMM, Samsung o Huawei. Para ello, Intel incrementará su dependencia del "outsourcing" en fabricación y renovará sus esfuerzos para proveer semiconductores a terceros. Pat Gelsinger es nuevo CEO, pero no es nuevo en Intel, donde trabajó 30 años con la "vieja guardia" de Andy Grove, "para quien, solo los paranoicos sobreviven". Y no le falta razón. En los últimos años, Intel abandonó sus valores y cayó en la autocomplacencia. Una parte de esa inversión de Intel será destinada a la computación cuántica.

"Y los de Abu Dhabi, con ciudades digitalizadas y rascacielos que tocan el cielo", se lanzan a la búsqueda de aplicaciones prácticas para la computación cuántica, que es el Santo Grial de las Tecnologías de la Información y Digitalización. En nuestro artículo de 2019, Google había hecho experimentos para la NASA (que publicamos en primicia en España en IT User) y decía que "lo llevado a cabo, hubiera costado 10.000 millones de años a la computación tradicional". Recientemente, "los chinos", sin especificar quienes porque son 1.500 millones..., afirman que han desarrollado una computadora cuántica "un billón de veces más rápida que aquella de Google". El que no corre... ¿vuela?

El Instituto de Innovación Tecnológica de Abu Dhabi, el brazo de investigación aplicada del Consejo de Investigación de Tecnología Avanzada de Abu Dhabi, está construyendo la computadora en sus laboratorios del Centro de Investigación Cuántica, en colaboración con Qilimanjaro Quantum Tech, con sede en Barcelona. Barcelona..., España. "Estamos en la cúspide de una nueva era con el advenimiento de la computación cuántica", dice Faisal Al Bannai, secretario general del Consejo de Investigación de Tecnología Avanzada.

En la misma línea, la computación cuántica representa "la capacidad de condensar décadas o incluso siglos de procesamiento numérico, en minutos", asevera un informe compilado por la Cumbre del Gobierno Mundial y PwC.

El laboratorio en Abu Dhabi había optado por usar qubits superconductores, que es la misma tecnología que Google e IBM están usando para construir sus computadoras cuánticas. Pero la computación cuántica es un campo más nuevo, popularizado por el físico teórico John Preskill, a quien se le ocurrió una formulación de supremacía cuántica, o la capacidad de las computadoras cuánticas para hacer cosas que no son posibles para las computadoras ordinarias. Desde entonces, las economías más grandes del mundo, de EE.UU., Rusia, China y Japón, así como los grandes de la tecnología IBM, Alibaba, Facebook y Google, han estado luchando por la supremacía en el campo de la computación cuántica.

Pero hasta ahora, solo se han solucionado problemas computacionales muy limitados con la finalidad de probar la velocidad. Las computadoras cuánticas aún no son capaces de resolver problemas prácticos-prácticos, muy prácticos: no saben poner la lavadora, por ejemplo.

Pero, cuando lo hacen, su potencial es enorme y puede acelerar rápidamente el descubrimiento humano. Por ejemplo, dado que las computadoras cuánticas pueden simular y diseñar estructuras moleculares a nivel atómico, uno podrá ver cómo funcionará un nuevo medicamento en un ser humano, eludiendo algún día las pruebas en humanos o animales.

Una computadora cuántica podría algún día responder preguntas sobre los orígenes del universo y preguntas persistentes sobre el espacio y el tiempo, que ahora solo "vemos" en películas como "Interstellar" o "Timeline".

Como dijimos más arriba, en 2019, Google afirmó que construyó la primera máquina en lograr la "supremacía cuántica"; es decir, una computadora que fue la primera en superar a las mejores supercomputadoras del mundo en el cálculo cuántico. Su prototipo de computadora cuántica completó en menos de cuatro minutos un cálculo que a una supercomputadora le habría llevado 10.000 años completar.

Otros, como IonQ Inc. se están preparando ya para convertirse en la primera empresa que cotiza en bolsa y se centra específicamente en la comercialización de la computación cuántica. Y su camino hacia la Bolsa de Valores de Nueva York es a través de un acuerdo de adquisición con fines especiales (SPAC) que valora la entidad combinada en aproximadamente 2 billones de dólares. IonQ Inc. es una startup de computación cuántica con sede en College Park, Maryland, y se convertirá en la primera empresa que cotiza en bolsa, enfocada totalmente en la comercialización de hardware y software de computación cuántica.

Aunque no es la única empresa. Microsoft Corp., IBM, D-Wave Systems Inc, Amazon, Alibaba, Facebook SpaceX y Google (Alphabet) están compitiendo para construir la primera computadora cuántica escalable de grado comercial. Facebook quiere una Inteligencia Artificial más rápida: al aprovechar el poder de la física cuántica, las computadoras cuánticas ofrecen la promesa de lanzar cálculos algorítmicos complejos para aplicaciones de inteligencia artificial al hiperespacio. Que son aplicaciones en las que Elon Musk (Testa SpaceX) y Jeff Bezos (Amazon) también están trabajando.

Cuando el río suena, agua lleva, dice el refrán. Una docena de grandes empresas tecnológicas norteamericanas desarrollando aplicaciones prácticas de computación cuántica es algo que tomarse muy en serio. Aunque la computación cuántica no sepa aún hacer la colada o llenar el lavavajillas. ■

MÁS INFORMACIÓN

- El gasto en computación cuántica se multiplicará por 35 en la próxima década
- DARPA lanza un programa para acelerar la tecnología de cifrado homomórfico
- Computación cuántica para ayudar a la cadena de suministro automotriz
- Taiwán quiere ser una potencia cuántica

8
ABRIL
11:00 CET

REGISTRO

Sophos ZTNA:

ON DEMAND

securizando el acceso a organizaciones en cualquier lugar

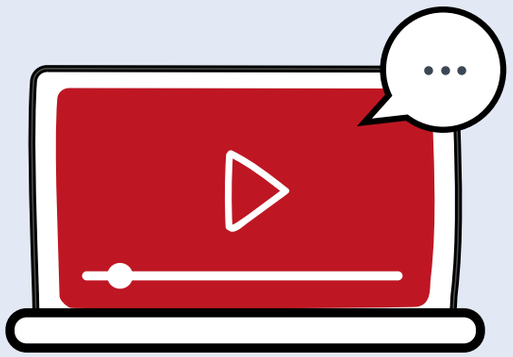
Sophos aborda la problemática actual de seguridad a la que se enfrentan las empresas, con un mayor volumen de ataques y la necesidad de extender las medidas de protección a una organización dispersa. Explica, además, qué es Sophos ZTNA (Zero Trust Network Access).

REGISTRO

Operaciones y Kubernetes

Infraestructura para cargas nativas en Cloud

La adopción de Kubernetes está permitiendo a las empresas implementar y administrar contenedores y, al mismo tiempo, administrar aplicaciones heredadas obteniendo ventaja competitiva, capacidad de innovación y productividad en sus entornos de desarrollo.



#ITWEBINARS

Aplicaciones,

¿cómo desarrollo y entrego mi mejor software?

6
MAYO
11:00 CET

Porque las aplicaciones son hoy -más que nunca- la cara del negocio... Únete a este Encuentro IT Trends con expertos y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlos en producción y administrarlos.

REGISTRO

22
ABRIL
11:00 CET

REGISTRO

Cómo hacer avanzar y proteger la empresa digital

El mercado de la ciberseguridad está adoptando nuevos o renovados planteamientos para obtener visibilidad de lo que ocurre en la red. En este webinar abordaremos los principios de las tecnologías de EDR, NDR, SIEM y SASE y sus capacidades para proporcionar la seguridad que toda empresa digital necesita.

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

TECNOLOGIA Y SANIDAD:

la mejora en la atención del usuario

Las TIC en Sanidad: el paciente como eje central de las nuevas tecnologías

En un mundo impulsado por la digitalización, la integración de la tecnología es prioritaria, más si cabe en un sector como el de la sanidad, sometido a significativos cambios durante el último año.

La pandemia generada por el Coronavirus SARS-CoV-2 ha puesto de manifiesto la importancia de contar con un sistema sanitario eficaz, accesible y resiliente, no solo a nivel de capacitación de los profesionales, sino también en lo referente a infraestructuras, servicios de alto valor, y, por supuesto, mejores tecnologías.

Y es que, como en todo, aunque en el sector sanitario con más razón, la adopción de nuevas tecnologías, sobre todo de las centradas en la Información y la Comunicación (TIC), puede aportar un valor diferencial. La Socie-

dad Española de Informática de la Salud (SEIS) considera las TIC, "imprescindibles para afrontar los retos actuales de los sistemas de salud en sus procesos de modernización y racionalización, y para lograr la transformación digital del sector. Además, su utilización intensiva favorece el tejido industrial, la innovación y la economía del país" .

Sin embargo, en este contexto de evolución digital, es importante tener en cuenta que la transformación tecnológica del sector sanitario debe ir más allá de la mera digitalización de los procesos; también implica ofertar nuevos productos y servicios digitales a los pacientes, además de acercar capacidades de diagnóstico, tratamiento y seguimiento a millones de personas, sin importar su ubicación.

Precisamente, y a lo largo del último año, con el sistema de salud colapsado a causa de la Covid-19, el redireccionamiento de la asistencia a los pacientes a través de la atención y el seguimiento a distancia ha sido más trascendental que nunca, convirtiéndose en muchos casos en la única alternativa, bien como primera capa informativa o canal de comunicación bidireccional entre el usuario y los diferentes profesionales de los distintos niveles asistenciales.

En este sentido, y junto a la telemedicina, Internet se ha alzado como medio idóneo para que los pacientes puedan acceder a asistencia médica sin tener que pasar por hospitales y centros de salud. Así, sistemas de videoconsulta, videollamadas, aplicaciones móviles o chatbots están siendo muy utilizados. También, otras tecnologías como Inteligencia Artificial, Machine Learning, Big Data o la analítica avanzada de datos están permitiendo progresar en cuanto a detección temprana y previsiones de evolución del coronavirus, entre otras. Y, por supuesto, IoMT, el Internet de las Cosas Médicas, un sistema de dispositivos médicos interconectados que utilizan sensores informáticos para así poder intercambiar datos a través de Internet. Con esta tecnología es posible conocer con mayor precisión la situación del paciente, aplicar tratamientos más efectivos y facilitar la prevención.

No obstante, y pese a estos avances, el sistema sanitario español, sobre todo la sanidad pública, sigue aquejado de una escasez de recursos de distinta índole. Años de falta de inversión, barreras administrativas, desajustes estructurales y una segmentación política incesante han lastrado su digitalización, actuando como verdaderos inhibidores. A este respecto, el Índice SEIS 2019 cifra la inversión sanitaria actual en TIC en España en 707.344 euros, un 3% menos que en 2018, mientras que el personal especializado en TIC y el gasto global en plataformas tecnológicas también se ha reducido un 1,86% y un 8,19% respectivamente.

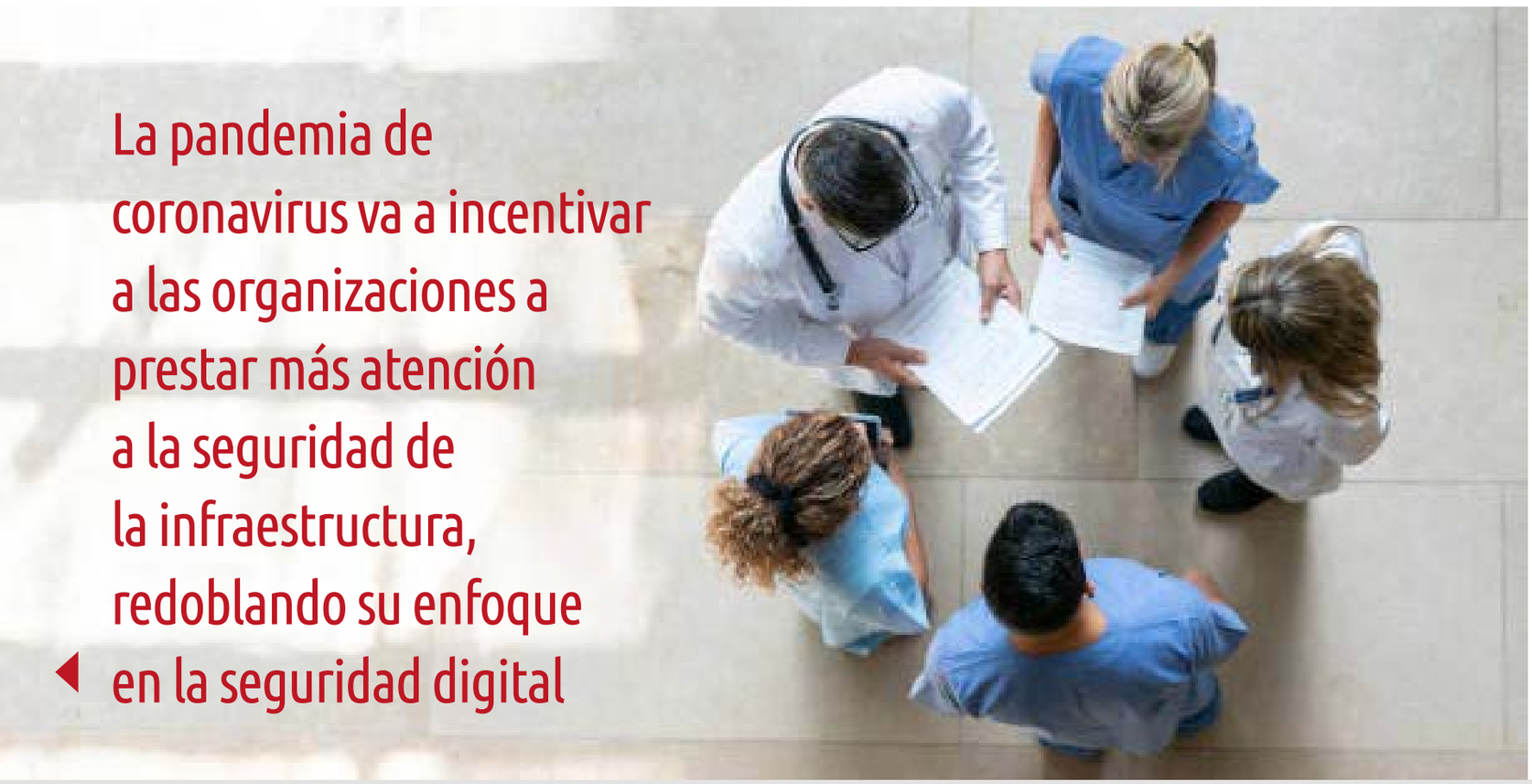
En la actualidad, y tras lo acontecido a lo largo del último año, es de esperar que la tendencia cambie: la Covid-19 ha acelerado la adopción digital en todos los ámbitos, incluido el sanitario, por lo que las TIC se hacen imprescindibles para afrontar los retos actuales.

IMPULSAR UNA ESTRATEGIA DE SALUD DIGITAL

Sobre este necesario avance, la ministra de Sanidad, Carolina Darias, adelantaba el pasado mes de febrero los principales puntos que constituyen la hoja de ruta de su Ministerio para los próximos años y entre los que se encuentran, la digitalización y la innovación de la sanidad. Adicionalmente, el Gobierno de España ha incluido en los Presupuestos Generales del Estado (PGE) para 2021 una dotación de 400 millones de euros para la Renovación de Tecnologías Sanitarias en el Sistema Nacional de Salud (SNS), además de 295,5 millones destinados a acelerar la estrategia digital del SNS.

A nivel privado, empresas como Accenture ya valoran que las empresas sanitarias preparadas para el futuro implementen estrategias digitales más innovadoras. Ya se trate de aplicaciones móviles, nube, EHR o wearables, las organizaciones líderes pueden cambiar fundamentalmente la forma en que se presta la atención médica.

Es de prever, por tanto, que estas iniciativas, y otras que estén por venir, potenciarán la innovación del sector sanitario, un nicho que hasta ahora se ha centrado mayoritariamente en integrar tecnologías dirigidas a modernizar el propio sistema en sí, como la Receta Electrónica o el acceso a la historia clínica electrónica por parte de los facultativos, más que en otras dirigidas a cubrir las necesidades reales de pacientes y profesionales.



La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando su enfoque en la seguridad digital

Preciso es también procesar adecuadamente los volúmenes masivos de información que caracterizan la actividad propia de los servicios de salud y que bien aprovechados pueden generar enormes beneficios.

EL DATO, EL ACTIVO MÁS SENSIBLE

La digitalización de los dispositivos utilizados en el entorno de la sanidad genera una ingente cantidad de información sensible sobre el ser humano. Se estima que en 2020 se alcanzaron los 25.000 petabytes de datos en el entorno sanitario, una cifra que sigue incrementándose de forma exponencial, influida también por el desarrollo de dispositivos IoT, que están contribuyendo a que los datos crezcan a una escala nunca vista.

Tal acumulación masiva de datos hace imposible su gestión a través de sistemas tradicionales, por lo que tecnologías como Big Data, Business Intelligence o la analítica de datos ofrecen nuevas posibilidades para la elaboración de modelos predictivos, patrones de comportamiento o para la provisión de servicios más personalizados en tiempo real. Igualmente sientan la base para la interoperabilidad electrónica de la información sanitaria y allana el acceso a la tan ansiada Medicina 5P (Personalizada, Predictiva, Preventiva, Participativa y Poblacional); el cruce entre la sanidad y Big Data.

El análisis de grandes conjuntos de datos también ha servido como base para la aplicación de la Inteligencia Artificial, Machine Learning o Deep

Learning en el campo de la salud, como una herramienta fundamental de la medicina personalizada. Estas tecnologías pueden ampliar la analítica con el aprendizaje continuo y los análisis, derivando en una ventaja para el ser humano gracias a mejoras en el diagnóstico precoz de enfermedades, los tratamientos a medida, y una mejor administración eficaz de recursos sanitarios.

Por tanto, no hay duda de que el tratamiento global y sistemático de los datos ha abierto un nuevo mundo en distintas áreas. Sin embargo, el acceso a datos personales por parte de facultativos, máquinas y demás responsables no gusta a todos por igual.

En este contexto, satisfacer las expectativas sobre la privacidad y seguridad de los datos se hace clave para impulsar la sanidad digital. Sin duda, el conocimiento por parte del paciente de la finalidad del uso de sus datos y de los mecanismos de protección empleados incrementará la confianza en la sanidad digital.

PROTEGER Y CUIDAR LOS DATOS

La información confidencial que maneja el sector sanitario es de gran interés para la ciberdelincuencia por lo que se ve continuamente sometida a ataques, además de ser víctima de brechas o fugas de información que generan un gran coste económico (5,8 millones de euros, en 2020, según Data Breach Report publicado por IBM). Y es que, por su importante información, los registros médicos de pacientes tienen un valor en el mercado negro hasta 50 veces superior al de la información financiera personal, lo que explica que los ataques contra el sector sanitario se incrementen sin medida. No hay más que ver que el número de intentos de ataque contra empresas de la salud aumentó a nivel mundial un 45% durante los dos últimos meses de 2020, según indica Check Point, más del doble de lo que creció en todos los sectores a nivel mundial. En el caso de España, el número de ataques contra infraestructuras sanitarias también se duplicó en ese periodo, tal y como revela dicha fuente.

Las amenazas más comunes que afectan al sector salud tienen su origen en el correo electrónico: suplantación de identidad, campañas de phishing, adjuntos maliciosos, aunque es el ransomware el que muestra el mayor aumento, sobre todo la variante Ryuk. Los cibercriminales saben que una interrupción del servicio en un hospital puede ser crítico, por lo que apuntan sus objetivos a estos blancos, más propensos a satisfacer sus demandas de rescate.

SIN VACUNA PARA LOS ATAQUES

En cuanto a las tendencias, es de esperar que la pandemia de Covid-19 siga actuando sobre la mayoría de las amenazas y riesgos, muchos de estos directamente relacionados con el aumento del teletrabajo. En este sentido, el mayor uso de soluciones en la nube, conexiones VPN, servicios de escritorios VDI, redes de confianza cero y ges-

La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital

tión de identidades, servicios y tecnologías para el acceso remoto, uso de herramientas colaborativas o aplicaciones de videoconferencia generará que los ataques a estos entornos, en especial a los sistemas públicamente expuestos, sigan creciendo . También los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales y los dirigidos contra farmacéuticas, laboratorios de investigación dedicados a la Covid-19. Asimismo, y en relación a los ataques de ransomware, es necesario señalar una tendencia, ya consolidada, como es la sofisticación de dichos ataques.

Sin duda, la medicina se usará como señuelo al menos hasta el final de la pandemia. El factor humano es uno de los componentes más importantes de muchos ataques, y la información sobre nuevas restricciones regulatorias, tratamientos potenciales y la salud del paciente seguirá atrayendo la atención de los usuarios. Los expedientes médicos filtrados también se convertirán en parte del gancho de los ataques dirigidos, ya que la información precisa del paciente hará que los mensajes falsos sean mucho más creíbles.

No obstante, también hay buenas noticias. La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital. Es más, según se desprende del Informe de Ciberpreparación de Hiscox 2020, la industria española de Pharma y Salud ha mejorado con respecto a 2019 tanto su ciberpreparación, incrementándose desde el 4% al 12% el número de empresas calificadas como expertas, como la inversión en TI. Las compañías participantes han pasado de invertir el 4,6% del presupuesto de TI en ciberseguridad al 13,73% en 2020. Además, más de la mitad (56%) dicen integrar aspectos de ciberseguridad en todos los procesos y proyectos desarrollados en su plan de negocio, convirtiendo esta área en una variable transversal a toda la organización.

A raíz de esta situación, no hay duda de que las TIC juegan y jugarán un papel determinante en las organizaciones sanitarias, para facilitar la gestión eficiente de los servicios ofrecidos a la ciudadanía y la capacidad asistencial. La necesidad de comunicarse de manera efectiva con los pacientes es una prioridad, como ha quedado demostrado. Por tanto, hay que seguir trabajando para aumentar las conexiones digitales con los pacientes (más datos y análisis en tiempo real) para mejorar la calidad asistencial mediante una medicina basada en la evidencia y en al análisis del dato para la toma de decisiones adecuadas. Es hora de desarrollar una medicina personalizada con la ayuda de las TIC. ■

MÁS INFORMACIÓN

- Índice SEIS 2019
- Hoja de ruta del Ministerio para digitalizar e innovar en Sanidad
- Renovación de Tecnologías Sanitarias en los Presupuestos Generales del Estado
- IBM Data Breach Report
- Incremento de ataques a organizaciones sanitarias por la Covid19

Una infraestructura de red inteligente mejora los resultados, las operaciones y la seguridad a todos los niveles.

Los centros de atención médica super conectados del mañana ofrecen oportunidades casi ilimitadas para potenciar la conectividad universal (cableada, Wi-Fi y celular en interiores) para construir una red estable de servicios, aplicaciones y herramientas que sirven como base de la evolución de su red a largo plazo. Desde la oficina más pequeña hasta el laboratorio de investigación más avanzado y el campus hospitalario más grande, existen nuevas y emocionantes formas de mejorar la atención sanitaria y la eficiencia operativa.

Conozca las soluciones de CommSCope para el Sector Sanitario: **Click aquí**

Transformación tecnológica como paso previo hacia un nuevo modelo de sanidad

El de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. Por ello, este sector debe poner todo de su parte para ofrecer un servicio continuado, pero sin descuidar aspectos como la seguridad de la información o la protección de los dispositivos de salud. Los retos, por tanto, no dejan de crecer. ¿Está la Sanidad española preparada para superarlos?

Para hablar de estos temas y analizar otras cuestiones como el estado actual de la inversión en la Sanidad, nuevas formas de financiación y servicio o conocer qué se está haciendo, tanto desde la sanidad pública como privada para proteger los datos y luchar contra el incremento de ciberataques, hemos contado con la participación en esta #MesaRedondaIT de Bernardo Gómez, territory account manager Iberia de CommScope; Marco Frühauf, vicepresidente de Grenke; e Iván Mateos, Ingeniero preventa de Sophos. Asimismo, incluimos las opiniones y valoraciones de Jairo Alonso, ICS security consultant de S21Sec, quien por problemas de última hora no pudo conectarse al debate.

ESTADO DE SALUD TECNOLÓGICO

Sin duda, y en lo que respecta a la adopción de Tecnologías de la Información y la Comunica-

TECNOLOGÍA Y SANIDAD: mejora en la atención al paciente

“La situación actual puede repetirse, y hay que estar preparados. No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. En un año hemos avanzado lo que en condiciones normales hubiese llevado entre tres y cinco”

BERNARDO GÓMEZ, TERRITORY ACCOUNT MANAGER IBERIA DE COMMSCOPE

ción, el sector sanitario ha dado un gran paso de gigante a lo largo del último año. En este contexto, Bernardo Gómez considera que la situación provocada por la pandemia ha servido como “catalizador para impulsar la adopción de este tipo de tecnologías y si bien aún queda mucho camino por recorrer, el sanitario se encuentra en un punto significativamente desarrollado”.

Algo distinto ocurre en lo concerniente a los flujos de caja, donde Marco Frühauf, evidencia algunos desafíos: “durante el último año, algunos subsectores, como el de las farmacias, han tenido que hacer frente a una falta de tesorería, al no recibir, o fluir más lenta, la financiación proveniente de las Administraciones Públicas”. Por tanto, y aunque por su trascendencia este sector demanda estar perfectamente equipado, “también requiere estar bien financiado, y aquí todavía hay aún muchos retos”.

“La rápida digitalización de principios de 2020 abrió la puerta a nuevos riesgos en ciberseguridad, que han tenido que ir mitigándose”, reconoce Iván Mateos. Sin embargo, y aunque la situación actual es más positiva de lo que se preveía, el sector sanitario sigue en el punto de mira de muchos atacantes. No obstante, “las empresas están actuando, tomando decisiones a corto y medio plazo y en ese sentido no vamos por mal camino, aunque hay que seguir avanzando”.

“La sanidad española dispone de prácticamente los últimos dispositivos del mercado”, destaca Jairo Alonso, por lo que, a nivel de equipamiento tecnológico está bastante actualizada para hacer frente a los problemas de ciberseguridad. Sin embargo, “esto no significa que no existan otros equipos y dispositivos tradicionales que sigan funcionando perfectamente”, reconoce este responsable.

INVERSIÓN SIN PLANIFICACIÓN

A raíz de lo comentado, no hay duda de que la inversión en tecnologías a lo largo del último año ha sido muy importante en Sanidad. Sin embargo, ¿se han hecho estas adquisiciones en base a una planificación o las empresas se han dejado llevar por la alarma del momento?

Aunque, en los primeros meses, la aceleración en los procesos de digitalización llevó a muchas empresas a realizar una inversión tecnológica no planificada, Marco Frühauf considera que según se fue avanzando, y teniendo acceso a más información, la situación varió. “Las grandes inversiones se han hecho bien, han sido planificadas. Sin embargo, sobre todo al principio, se tomaron decisiones precipita-

das; se adquirió equipamiento que no era necesario o que no era la solución adecuada, debido a una gran desinformación".

En la misma línea, Iván Mateos coincide en destacar cierta improvisación a la hora de adquirir equipamiento, porque al principio lo que primaba era la productividad. "Hoy con el conocimiento de que esta situación aún se va a extender en el tiempo se impone la planificación, ajustar los presupuestos a las necesidades, ya sin prisa. En su momento se cometieron muchos fallos, se abrieron más puertas de las necesarias y esto trajo distintas consecuencias. "Lo peor ya pasó y ahora estamos intentando hacerlo todo mejor".

Sobre las infraestructuras de comunicaciones, Bernardo Gómez destaca que se han acelerado los tiempos de despliegue de las agendas de digitalización ya preestablecidas, variando las prioridades. "Si antes de la pandemia, hospitales y residencias apostaban por el desarrollo de las redes de uso interno, con la integración de tecnologías como IoT, la nueva situación ha llevado a priorizar las redes de accesos para los pacientes. "Hemos pasado de la incertidumbre a la racionalización de la tecnología, una vez entendido a qué nos enfrentamos".

La adquisición de tecnología debe responder a un plan ya previsto. Así, Jairo Alonso se muestra convencido de que la aceleración en los procesos de digitalización provocada por la Covid-19, ha comprometido la planificación necesaria en cualquier proyecto de digitalización. Es más, según este responsable, "en el mundo de la seguridad la falta de planificación acaba pasando factura a largo plazo, bien sea en forma de ataque, que no sería lo deseado, o bien obligando a las empresas a incrementar sus presupuestos para optimizar su seguridad".

> "La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad"
>
> MARCO FRÜHAUF, VICEPRESIDENTE DE GRENKE

CIBERSEGURIDAD

Con una amalgama de empresas públicas y privadas, el de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. ¿Son los retos en ciberseguridad los mismos para la sanidad pública y privada?

Independientemente de que sea público o privado, el sector sanitario tiene que ofrecer un servicio continuado. Por ello, Iván Mateos explica que "enseguida entiendes su forma de trabajar". Para el personal de IT, la ciberseguridad es importante, pero lo es más que un dispositivo no funcione o que falle una conexión entre máquinas. "Así, es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos. Los fabricantes debemos poner ciberseguridad sin implicar dificultad, una vez que lo comprendes, el planteamiento coge buen rumbo".

Sobre esta necesidad de elevar la seguridad, Bernardo Gómez destaca que esta exigencia

es igual tanto en la sanidad pública como en la privada. La diferencia fundamental estriba en la velocidad con la que se adopta y adapta la tecnología, que sin duda es mucho más rápida en el sector privado. No obstante, no hay que olvidar que "la información es crítica, y cada vez hay más dispositivos conectados en el entorno sanitario, por lo que hay muchos riesgos a los que hacer frente".

Para Marco Frühauf la sanidad pública y la privada abordan sus retos de forma totalmente distinta. Así, "hay enormes diferencias en cuanto a la rapidez en la adopción de medidas o en la toma de decisiones, aunque las necesidades sean las mismas". Respecto a la financiación de la tecnología, el sector privado está mucho más abierto a nuevos métodos más alejados de las tradicionales. "Los retos y las posibilidades se entienden mejor y se pueden dar soluciones de un modo mucho más eficiente".

Por su parte, Jairo Alonso reconoce que además de ser un segmento esencial, gran parte de la sanidad, tanto pública como privada, se considera infraestructura crítica. "Esa significación conlleva que deben aplicarse medidas de seguridad más concretas y que apoyen y favorezcan en todo momento la prestación del servicio".

Ahora bien, ¿por qué hay tanta diferencia a la hora de afrontar un escenario de ciberseguridad?

Según Marco Frühauf este contraste se debe principalmente a que el sector público es mucho más complejo. "Hay que lidiar con distintas administraciones y organismos por lo que el proceso de toma de decisiones es mucho más largo y difícil, además de existir cierta opacidad a la hora de interpretar por dónde va la cosa".

En cuanto al ritmo de digitalización, ¿es de esperar que continúe en la misma línea tras la pandemia?

Sobre esta cuestión, Bernardo Gómez observa que esta nueva aproximación a la digitalización se mantendrá. "La situación actual puede repetirse, y hay que estar preparados". No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. "En un año hemos avanzado lo que en condiciones normales nos hubiese llevado entre tres y cinco".

Pese a estos avances, toca saber si el dato, está adecuadamente protegido.

El sector sanitario debe gestionar información muy sensible, que no es fácil de manejar, y que si se filtra o se pierde puede traer graves consecuencias. Por ello, Iván Mateos apunta a que es necesario buscar soluciones concretas: "El primer paso es identificar el riesgo, y luego querer abordarlo. Buscar una solución de seguridad concreta para ese problema es más sencillo".

Muy importante es también cumplir con las distintas normativas para la seguridad de la información. En este punto, Jairo Alonso afirma que a nivel TI, normas de seguridad como la ISO 27001 son seguidas ampliamente en el sector, "el problema viene cuando el sector se olvida de su parte industrial, de cumplir con normas como IEC 62443 que afectan a los dispositivos médicos y a sus redes.

"La seguridad como servicio puede suplir muchas carencias, pero la falta de conocimientos y experiencia de los usuarios no es uno de ellos. El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad"

JAIRO ALONSO, ICS SECURITY CONSULTANT DE S21SEC

PRINCIPALES RETOS EN SANIDAD

La telemedicina ha llegado para quedarse, tanto en el sector público como privado, por lo que hay que adaptar las infraestructuras para ofrecer un servicio de calidad al usuario.

Así, según Bernardo Gómez es necesario poner los recursos para el personal sanitario en

“Para el personal de IT, la ciberseguridad es importante, pero lo es más aún que un dispositivo no funcione o que falle una conexión entre máquinas. Es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos”

IVÁN MATEOS, INGENIERO PREVENTA DE SOPHOS

su dispositivo, dotar de conectividad a todo el equipamiento con el que cuentan los centros sanitarios, para que la información fluya libremente, además de garantizar su seguridad: “No solo preocupa que alguien pueda acceder a la información, sino también que pueda modificarla. Estos son los grandes retos”.

Por su parte, Marco Frühauf considera que “la inversión tiene que continuar”, pero es necesario que quienes controlan el dinero, los financieros, cambien su enfoque hacia uno centrado en el pago por uso. “La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad, que en España está costando bastante”.

Según Iván Mateos, el principal desafío es que el sector sanitario pueda seguir avanzando tecnológicamente, sin incurrir en un riesgo para la seguridad. Una vez llevado este riesgo al mínimo exponente, se podrán ofrecer soluciones en todos los ámbitos: software, hardware y servicios. El reto por tanto pasa porque “tecnológicamente el servicio pueda crecer, que se pueda dar sin interrupción y que la ciberseguridad no sea un problema, para que los trabajadores puedan dedicarse a su trabajo”.

Asegurar una compartición segura de los datos para que los pacientes puedan ser atendidos en cualquier lugar o incluso en remoto y el médico pueda disponer de todo el historial clínico es el principal reto, según considera Jairo Alonso. “Tampoco debe ignorarse la seguridad de los dispositivos que monitorizan y controlan la salud de los pacientes, tanto los que pueden llevar en su propio cuerpo como los utilizados en quirófanos y UCI”.

TECNOLOGÍA Y SEGURIDAD COMO SERVICIO

¿Es el sector sanitario un buen escenario para el despliegue de tecnología como servicio?

Sobre este aspecto Bernardo Gómez reconoce que el sector privado está empezando a desplegar este modelo por su bajo impacto presupuestario y por la rápida evolución de las tecnologías, lo que permiten estar siempre actualizados. A la contra el sector público sigue anclado en el modelo presupuestario tradicional y se muestra más reticente a este tipo de inversiones. “Es una tendencia que acabará cambiando, pero queda tiempo para este cambio de mentalidad”.

En la misma línea, Marco Frühauf también reconoce el avance de la sanidad privada en este punto, sin embargo, valora que el cambio en el sector público tardará bastante tiempo

en producirse. “Con intereses y procesos que cambian, y atrapadas en concursos públicos y partidas presupuestarias ya fijadas, las administraciones públicas son presas de sus propios métodos y o te adaptas a ellos o no juegas. Al contrario que en la privada, es complicado cambiarles el paso”.

Para Iván Mateos ofrecer la tecnología como servicio es la respuesta, también en ciberseguridad. Ante la falta de capacidades tecnológicas y de expertise, la opción más adecuada es contratar un servicio que se dedique a vigilar la infraestructura, implementar soluciones de pago por uso, sencillas de utilizar y que no afecten a la operativa diaria. “Como fabricantes tenemos que facilitarles el trabajo, ofrecerles una tecnología sencilla, que le permita centrarse en su trabajo. Cuanta más tecnología se tiene, más eficiente se vuelve el sector sanitario”.

Por su parte, Jairo Alonso también señala que el sector sanitario es un buen escenario para el despliegue de seguridad como servicio, no obstante, considera que la falta de conocimientos y experiencia de los usuarios no es uno de ellos. “El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad”. ■

MÁS INFORMACIÓN

Tecnología y Sanidad: mejora en la atención al paciente

Un mensaje para los responsables tecnológicos

Tras el empujón en inversión tecnológica vivido a lo largo del último año, es de esperar que todo esto siga mejorando de cara a maximizar los resultados. ¿Cómo puede lograrse? Sobre este hecho, “es importante aprovechar la inercia”, reflexiona Bernardo Gómez, “continuar invirtiendo en dos líneas críticas a nivel de infraestructura: la digitalización de los procesos de los centros hospitalarios, pero sin olvidar al paciente, a fin de darle capacidad de comunicación en los centros hospitalarios y en las residencias de mayores cuando se encuentre en ellos”.

Asimismo, Marco Frühauf también aboga por sacar partido de la experiencia, aprovechar todas las herramientas existentes para flexibilizar el modelo de gestión de las tecnologías para una mejor toma de decisiones. “Aprovechar la experiencia y el conocimiento para poder tomar las decisiones adecuadas y ser flexibles, manteniendo una inversión permanente”.

Dialogar, escuchar las necesidades de los responsables de tecnología y ciberseguridad es imprescindible para mantener esta tónica de implementación tecnológica, reconoce Iván Mateos. “A lo largo del último año se han visto los beneficios de implementar tecnología; ante un problema, se puede seguir trabajando e incluso la productividad se incrementa. Tanto técnicos como personal sanitario son igual de importantes para que el servicio no se detenga”.

Por último, Jairo Alonso concluye este bloque con un mensaje similar dirigido a las organizaciones de salud, “que no tengan miedo en contactar con empresas de seguridad. Estamos para ayudarles y podemos identificar sus necesidades principales a nivel de seguridad”.

GRENKE

FAST // FORWARD // FINANCE

¿TUS CLIENTES QUIEREN TU TECNOLOGÍA PERO NO TIENEN LA LIQUIDEZ PARA PAGARLA?

CONTACTA CON NOSOTROS

916305672

O CONTIGO@GRENKE.ES

Estar a la vanguardia tecnológica para ser más competitivo es una necesidad, pero en ocasiones resulta complicado sin que esto afecte a la liquidez de tu negocio.

Gracias al renting tecnológico y de equipamiento de GRENKE podrás ayudar a tus clientes a conseguirlo. Ellos pagan cómodas cuotas mensuales, en lugar de desembolsar el total, mientras tu cobras el 100 % de tu factura en 24 horas. ¡Así de fácil!

WWW.GRENKE.ES

JUAN DIZ, ASESOR SÉNIOR TIC SANIDAD

“Hemos visto que la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales”

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan una excelente usabilidad y movilidad de los sistemas de información

En su opinión, ¿qué carencias desde el punto de vista tecnológico ha destapado la situación de pandemia que estamos viviendo en las Infraestructuras sanitarias?

La obsolescencia de los actuales sistemas de información y la baja calidad del dato han quedado al descubierto con esta pandemia. Asimismo, hemos visto como la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales, lo que en casos como esta pandemia ha colapsado y retrasado toda la actividad no “covid” existente, impidiendo la accesibilidad y equidad del sistema.

Teniendo en cuenta la criticidad de la Infraestructura sanitaria, ¿qué ventajas aporta la tecnología a los profesionales del sector, tanto desde el punto de vista sanitario como de gestión?

Las tecnologías que subyacen en la Transformación Digital son claves para apuntalar la transformación de la sanidad a la medicina 5P. Los sistemas de “Big Data” son vitales para una medicina poblacional y predictiva, las aplicaciones móviles y portales web son esenciales para una sanidad participativa y preventiva y el “Deep learning” y la Inteligencia Artificial dan soporte a la medicina de precisión o personalizada.

¿Cuáles son las principales demandas tecnológicas de los profesionales del sector sanitario?

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan

“La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y por último sistemas”

una excelente usabilidad y movilidad de los sistemas de información que realmente le descargue de tareas burocráticas y de sus procesos, así como que le asista en su actividad profesional de una manera “responsive” no intrusiva y que aprenda y se adapte a cada profesional y su contexto de manera dinámica e incremental

Poniendo en el centro la atención al paciente/usuario, ¿cuáles son las tecnologías más relevantes que impactan en esta atención?

Aquellas que le apoyen en su rol de medicina participativa mediante aplicaciones móviles, asistentes virtuales, portales de paciente y “wearables” sanitarios, los cuales deben aportar datos objetivos de los pacientes. Muchas veces los pacientes y los profesionales establecen una relación de manera verbal con indicación de percepciones que no ayudan a acotar los problemas de salud con eficiencia. Los datos recogidos y cuantificables (hábitos de sueño, actividad, pulsaciones durante las 24h, así como saturación de oxígeno pueden dar una dimensión objetiva de los problemas de salud y son además susceptibles de ser gestionados por sistemas de “machine learning” que descarguen al profesional de tareas de poco valor. La calidad y cantidad de los datos aportan mejor información y como ultimo mejoran el conocimiento de los ciudadanos y sus dolencias.

¿Hasta qué punto la Transformación Digital es una realidad en el entorno Sanitario? ¿Podemos diferenciar entre Sanidad Pública y Privada?

La Transformación Digital en este sector tiene que ser precedida de una Transformación de la Sanidad. La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y, por último, sistemas.

La Sanidad en general va atrasada en esta transformación, si bien es cierto que hay tanto en el sector Público como Privado excepciones, pero en todo caso es un proceso muy complejo y lento.

¿Hacia dónde debe evolucionar la Sanidad y cuáles son los aspectos más críticos de mejora?

La sanidad debe y está evolucionando hacia las líneas estratégicas que indica la Sanidad 5P antes mencionada (Poblacional, Preventiva, Participativa, Preventiva y de Precisión/personalización) con el último objetivo de ser medida en base e a resultados de salud, a su valor aportado a la sociedad.

Sin embargo, en tecnología en sistemas de información en Sanidad existen elementos tan básicos por mejorar como la simple identidad única del paciente o la obsolescencia del puesto de trabajo, así como la capacitación digital de profesionales y pacientes, además de escasez de profesionales TIC con experiencia en Sanidad. No tenemos que olvidarnos que venimos de una escasez de financiación TIC en Sanidad que de manera crónica ha retrasado su evolución. Esperamos que los anunciados Fondos Europeos en sanidad transformen para bien un sector tan crítico y esencial como es la sanidad y que la pandemia ha subrayado. ■

Juan Diz, asesor sénior TIC Sanidad

Master en Dirección de Sistemas y Tecnologías de la Información y Comunicaciones de la Salud por la ENS Escuela Nacional de Sanidad del Instituto Carlos III, e ingeniero de Telecomunicaciones Universidad Politécnica de Madrid. Más de 32 años de experiencia en empresas de equipamiento médico de alta tecnología médica, empresas de soluciones digitales de Imagen Medica, así como consultoras TIC de Sanidad.

Las redes de atención sanitaria obtienen más beneficios de una solución de infraestructura llave en mano

COMMSCOPE®
RUCKUS®

Internet de las cosas (IoT) está revolucionando innumerables sectores de la industria, permitiendo una automatización más avanzada y un mayor control de todo tipo de aplicaciones IT y OT. Estas incluyen iluminación, sistemas de seguridad y climatización (HVAC). Si bien casi todas las industrias pueden beneficiarse del IoT, la atención sanitaria ofrece un conjunto particularmente diverso de casos de uso.

Aunque esto supone un futuro apasionante para la evolución de las redes de atención sanitaria, también introduce un considerable nivel de complejidad que puede impedir que una organización médica aproveche plenamente la eficiencia operativa, la mejora de la seguridad y la ampliación de las capacidades que posibilita el IoT, o como se suele denominar en el contexto de las redes sanitarias, el Internet de las cosas médicas (IoMT).

IOMT APORTA UNA ENORME DIVERSIDAD DE APLICACIONES

Pocos espacios comerciales pueden siquiera acercarse al tipo de necesidades de procesamiento de datos de una moderna institución sanitaria u hospital. El movimiento fiable y rápido de información es de misión crítica, la seguridad física y de los datos debe cumplir con estrictos estándares regulatorios, el personal y los pacientes ampliamente distribuidos requieren una conectividad de gran alcance, y tanto el inventario como los equipos deben ser minuciosamente gestionados de forma cercana.

Algunos ejemplos específicos de los dispositivos que responden a estas necesidades son:

- Cámaras y sensores de seguridad conectados por IP en todas las instalaciones
- Señalización digital para dirigir a pacientes y visitantes a sus destinos
- Sistemas de gestión de alerta de cama y desplazamientos que mantienen a los pacientes seguros

“Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red, una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto”

❖ Acceso a la información y entretenimiento en la habitación a través de la red

❖ Botones de llamada del paciente y alarmas de pánico para garantizar que la ayuda llegue rápidamente

❖ Gestión de inventario mediante RFID o Tags activos WiFi para asegurar que las existencias sean adecuadas y que las auditorías sean sencillas

❖ Automatización de edificios con la integración de las cerraduras de las puertas de acceso con tarjetas, via WiFi, Zigbee y BLE

❖ Software de gestión automatizada de infraestructuras (AIM) que supervisa y protege todas las conexiones de red en tiempo real, automatiza las alarmas y administra toda la documentación de la red en tiempo real para asegurar los datos y garantizar la privacidad de los pacientes

Mirando todas estas funciones, aplicaciones y servicios, parece una tarea casi imposible integrar tantos tipos diferentes de conectividad en una sola infraestructura de red. Sin embargo, eso es exactamente lo que CommScope ofrece a las redes de salud de todo el mundo.

Una infraestructura de red llave en mano que es simple, fiable y adaptable

Con tantas piezas móviles, una red que permita el IoMT no puede permitirse ser una solución fragmentada. Unir un mosaico de tecnologías de infraestructura no solo degrada el rendimiento general, sino que también aumenta el tiempo y los problemas de instalación. Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red (abrir techos y paredes a menudo requiere cerrar partes necesarias y rentables de las instalaciones), una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto. ■

La comunicación como puntal para la telemedicina

El sector sanitario, sobre todo en lo que tiene que ver con tecnología, ha vivido una catarsis a lo largo del último año. A este respecto, Bernardo Gómez, territory account manager Iberia de CommScope, considera que las agendas tecnológicas sobre digitalización que tanto la sanidad pública como privada tenían concretadas se han acelerado, permitiendo que en poco tiempo se haya avanzado lo que en circunstancias normales habría llevado cuatro o cinco años. Sin duda la tecnología aplicada al sector sanitario ha acelerado este proceso de adopción.

Ahora bien, pese a este paso de gigante en cuanto a adopción de tecnologías, lo cierto es que el sector sanitario tiene por delante aún muchos retos, desafíos que bien encarados, gracias al apoyo de empresas especializadas, pueden suponer no desandar lo ya andado.

Sobre estos retos, Bernardo Gómez reconoce que el principal es que ha cambiado el modelo de negocio de la sanidad. Cada vez surgen nuevas aplicaciones en el entorno sanitario, como la telemedicina, que está muy ligada a la infraestructura de comunicaciones y es precisamente ahí donde CommScope puede aportar valor al sector sanitario, tanto en la parte de infraestructura con redes de cableado y fibra, para toda la parte de comunicaciones de los centros sanitarios; como en lo que concierne a la infraestructura activa con la conectividad inalámbrica y las redes LAN, requisitos indispensables para poder ofrecer un servicio de telemedicina de forma adecuada.

Asimismo, Gómez razona que para desarrollar este modelo de telemedicina es ineludible interconectar todos los centros de toma de decisiones con los puntos donde se genera la información. Esto en el entorno sanitario es crítico porque hay que conectar un ecógrafo o un equipo de radio diagnóstico con un médico que trabaja desde su casa dando tele asistencia a sus pacientes. Es decir, la información generada en diferentes sistemas tiene que fluir de una manera eficiente y de manera segura. Por tanto, es crítico dotar de infraestructuras de comunicaciones robustas y seguras a los centros sanitarios para poder trabajar en este nuevo modelo de servicio.

VALOR DIFERENCIAL

Cuando se plantea una estrategia de comunicación, un director de IT de un centro sanitario tiene que pensar tanto en la conectividad de las personas como en la conectividad de las cosas. Son las dos líneas de actuación críticas, y que permitirán que un médico pueda acceder a toda la información relevante de un paciente.

Para ayudar a las organizaciones del sector sanitario a dar este paso, desde CommScope consideran que estas entidades deben realizar una actualización de sus redes de comunicación empresariales, evolucionando desde una arquitectura tradicional de un punto de acceso inalámbrico, o punto de acceso WiFi, hacia un modelo de nodos de comunicaciones convergentes. En estos nodos de comunicaciones no solo se va a poder dar conectividad WiFi al usuario, a un dispositivo concreto, sino que también va a ser posible adoptar nuevas tecnologías sobre todo del espectro de IoT dentro de esta propia infraestructura.

Gracias a esta correlación, las organizaciones podrán reforzar sus redes LAN para convertirlas en redes multiservicio, dada la convergencia hacia el mundo IT, principalmente hacia el mundo IoT.

Tecnología para una sanidad más eficiente

JUAN CARLOS FARIÑAS, Área Manager de GRENKE España

La pandemia de Covid-19 ha dejado lecciones muy valiosas para el futuro de la sociedad. Una de ellas es la importancia de la tecnología como una herramienta necesaria para la gestión del sistema sanitario. En España, la Sanidad ha visto cómo los avances en materia tecnológica se han convertido en sus mejores aliados durante los meses más virulentos del coronavirus.

Desde las video llamadas, que consiguieron conectar a familiares con enfermos aislados, hasta la telemedicina, una forma de recibir prescripción médica que algunas comunidades autónomas ya han implantado en sus sistemas sanitarios.

La pandemia ha acelerado la puesta al día de la Sanidad con una revolución tecnológica de la que se había quedado descolgada, si la comparamos con otros sectores donde las soluciones y herramientas IT están a la orden del día.

De esta manera, empresas e instituciones sanitarias han visto la necesidad de utilizar esta vanguardia tecnológica para ofrecer una mejor atención al paciente y mejorar el trabajo del profesional.

Conseguir la implementación de los avances tecnológicos en la sanidad es la función de empresas como GRENKE, donde lo que aportamos se traduce en agilizar el trabajo de los sanitarios al favorecer y mejorar el seguimiento de los pacientes con herramientas que pueden evitar que tengan que acudir en repetidas ocasiones a los centros de salud.

Así, ciencia y tecnología se conjugan al cuidado de la salud para el diagnóstico, vigilancia y tratamiento de diversas enfermedades.

“La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias”

Gracias a ella, se obtienen diagnósticos precoces y más certeros, tratamientos menos invasivos y se reduce el tiempo de hospitalización y de rehabilitación, mejorando así la calidad de la atención sanitaria y aumentando la esperanza de vida de los pacientes.

La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias.

Beneficia a miles de millones de personas en todo el mundo, no solo en los hospitales, sino también en residencias y en el propio hogar. Forman parte de ella desde material desechable, como agujas o test de embarazo, hasta sofisticados equipos de diagnóstico, glucómetros, desfibriladores, robots quirúrgicos menos invasivos, máscaras de oxígeno, marcapasos, y un largo etcétera.

El futuro ya está aquí con los avances en tecnología sanitaria centrados en la robótica aplicada a la atención médica, la biotecnología, la telemedicina, los chatbots entre médico y paciente o las aplicaciones móviles orientadas a la salud, entre otros.

TECNOLOGÍA MÉDICA ACCESIBLE

Así y todo, el talón de Aquiles de toda esta revolución tecnológica viene siendo su financiación. No obstante, y al mismo tiempo, la inversión en nuevas tecnologías es fundamental para mantener el ritmo del progreso de las ciencias médicas modernas y para afrontar los retos que se ciernen sobre el sector. Los hospitales, centros clínicos y farmacias experimentan la presión de mejorar la experiencia de los pacientes en lo que se refiere al tratamiento, el diagnóstico, la atención y la comunicación.

Desde GRENKE aportamos soluciones que permiten un acceso a la tecnología de forma asequible y sin castigar su cuenta de resultados; y a sus pacientes disfrutar de lo último en tecnología sanitaria.

La apuesta es sencilla: un amplio portfolio de alternativas a la financiación tradicional de equipos médicos. Hay distintas soluciones de arrendamiento disponibles, y cada una de ellas se puede estructurar de forma diferente para ajustarse a necesidades concretas, ya sea en términos de presupuesto o de uso previsto. El arrendamiento ayuda a garantizar un acceso a las mejores y más recientes tecnologías sanitarias sin necesidad de una inversión sustancial por adelantado.

Y ya hay soluciones reales que van más allá del simple arrendamiento y que cubren toda la gestión del ciclo de vida de los equipos. Algunas de ellas pueden ser el pago por escaneo, los servicios de equipos gestionados y el mantenimiento inclusivo. Un aspecto crucial es que estas soluciones se ocupan del activo al final de su vida útil, de modo que los métodos de reciclaje y eliminación segura no son responsabilidad del cliente.

Al final de lo que se trata es de brindar el acceso a la tecnología repartiendo los costes y el presupuesto con más eficacia. ■

Financiación flexible al servicio de la sanidad

Tecnología y sanidad van de la mano. Sin embargo, en ocasiones el acceso a la tecnología puede ser un proceso complicado bien por la inversión que conlleva o porque el proceso de gestión se torne farragoso. Para ayudar a las empresas sanitarias en su digitalización, existen soluciones financieras flexibles capaces de adaptarse a las distintas necesidades que presentan estas organizaciones. Marco Frühauf, vicepresidente de Grenke, aborda estas alternativas y explica cómo han ido ganando en importancia a lo largo de estos últimos meses.

Desde el inicio de la pandemia, el modo de adquirir tecnología ha ido cambiando. Durante una primera fase el sector sanitario, como tantos otros, se lanzó a adquirir equipamiento tecnológico para dar respuesta a las nuevas necesidades que iban surgiendo a causa del confinamiento, para después, tras unos meses de grandes inversiones, volver a un periodo de mayor moderación. Se ha pasado por tanto de un escenario de prisas y desorganización, de compra y financiación sin análisis previo de las necesidades reales, a otro de mayor mesura y examen, avanzando ya lo que podría ocurrir después del confinamiento.

A este respecto, Marco Frühauf reconoce que ha sido una época de grandes cambios para las empresas del sector sanitario, pero también para compañías como la suya, dedicadas al renting tecnológico, y que han tenido que adaptar sus sistemas y modelo de negocio a cada nueva situación surgida.

En este punto, y teniendo en cuenta, además, que la solvencia de las empresas se ha ido debilitando a causa de las grandes inversiones iniciales, desde Grenke se aboga por que las organizaciones del sector sanitario avancen hacia nuevas fórmulas de financiación que les permitan superar estos y otros escollos que les afectan de cara a adquirir tecnología. En este contexto, los principales desafíos a los que tienen que hacer frente estos actores tienen que ver con su necesidad de hacer inversiones y su incapacidad para realizarlas con las herramientas que normalmente utilizan; una financiación tradicional.

Por eso, Marco Frühauf expone la importancia de que estos agentes, no solo grandes hospitales, comunidades autónomas, sanidad pública, sino también sanidad privada, doctores o farmacéuticos conozcan nuevos métodos de financiación con los que invertir en tecnología y adaptar sus negocios a la situación actual, como puede ser el pago por uso, que permite disponer del uso de tecnología y bienes de equipo sin aumentar el endeudamiento de la empresa.

PAGO POR USO COMO SOLUCIÓN

Ahora bien, ¿es esta situación de pago por uso igual cuando se habla de grandes clientes, pequeños clientes, sector público, privado…?

Por su dimensión, se trata de realidades muy distintas, ya que, por ejemplo, mientras una pequeña farmacia tiene que subsistir con la tesorería que genera, un gran hospital, ya sea público o privado, cuenta con un importante respaldo económico.

No hay que olvidar que el sector sanitario es muy tradicional en cuanto a la gestión y manejo de los fondos y los recursos económicos. Esto le da una gran dependencia de la financiación tradicional, que está en manos de bancos, ya sean comerciales o especializados.

No obstante, toda la banca tradicional está ahora exigiendo un nivel de solvencia o unos requerimientos para ofrecer financiación muy altos, también sobre la documentación a aportar. Por ello, y cuando se trata de operaciones más sencillas, con una menor cuantía para hacer la inversión, el cierre de la operación puede depender más de cómo se gestione la documentación de la financiación que de la propia decisión del dueño del pequeño negocio y del fabricante de hacer la instalación. De este modo, y en un sector en el que se exige que todo sea rápido y sencillo, Gerke apuesta por simplificar este proceso. Realizar una gestión en minutos, sin un solo papel y de forma digital.

Ciberseguridad y funcionalidad, el futuro de los entornos OT

JAIRO ALONSO, ICS Security Consultant, S21sec

Desde la pandemia, el sector sanitario ha cobrado más relevancia que nunca y ha experimentado un rápido proceso de transformación digital. Sin embargo, esto ha provocado que el sector se exponga a importantes riesgos de ciberseguridad, cuya solución requiere de una mayor colaboración entre las empresas de ciberseguridad y el sector sanitario, en especial, los fabricantes de dispositivos médicos. La evolución tecnológica ha ayudado a los hospitales y al personal sanitario a proporcionar una mejor atención a los pacientes, pero la situación de emergencia ha provocado también que se pasen por alto ciertos protocolos de ciberseguridad necesarios en el sector sanitario. Esto no solo supone un riesgo para los trabajadores de los hospitales, sino que también puede repercutir en la salud de los pacientes.

Es comprensible que los fabricantes quieran presentar sus productos al mercado lo antes posible para llevar ventaja con respecto a la competencia, pero, en ocasiones, esa urgencia hace que se salten el primer paso de trabajar conjuntamente con las empresas de seguridad ya que, en un inicio, ahorran tiempo y costes. Aun así, sus productos quedan expuestos innecesariamente a riesgos de ciberseguridad. Además, tampoco suele tenerse en cuenta que al aplicar la seguridad más adelante, dichos dispositivos requerirán de recertificaciones, cuyos procesos suelen ser todavía más lentos y costosos. Es cierto que existen limitaciones a la hora de aplicar ciertas medidas de seguridad en este

“Una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector”

tipo de dispositivos, dado que podrían afectar a su funcionalidad. No obstante, este riesgo se puede solventar integrando la ciberseguridad desde la etapa más temprana: su diseño.

La seguridad de los dispositivos médicos es de vital importancia, y la única forma de garantizarla es haciendo que los fabricantes y las empresas de ciberseguridad trabajen de manera conjunta desde un primer momento, para así evitar costes adicionales y otros problemas más graves, como pueden ser los ciberataques. De hecho, desde S21sec hemos tenido constancia de varios ataques de ransomware dirigidos al sector sanitario que implicaban el secuestro de equipos o cifrado de datos, y ha sido una de las razones por las que la ciberseguridad se ha convertido ahora en una preocupación global para los profesionales del sector.

El aumento de la conectividad entre dispositivos, el uso de tecnologías estándar y la acelerada digitalización de los sistemas de automatización, ha provocado que muchos sectores queden expuestos a riesgos de ciberseguridad. En este caso, los ciberataques son una amenaza todavía mayor para el sector de la atención sanitaria, ya que un ataque que interrumpa cualquier actividad puede suponer una cuestión de vida o muerte. Por ello, desde S21sec consideramos que el sector sanitario debe implantar determinadas estrategias con el objetivo de protegerse.

Para empezar, una de las estrategias más eficaces a adoptar es el modelo de ciberseguridad de confianza cero o Zero Trust. En los entornos OT, es básico separar las comunicaciones propias de Internet de la red IP corporativa y de los dispositivos médicos. El enfoque de confianza cero también recomienda y se basa en implementar controles en el tráfico de la red con el fin de evitar y contener ataques de usuarios que aprovechan estas vulnerabilidades para, en el mejor de los casos, hacerse con información personal y confidencial de salud.

Es crucial que el sector sepa cómo protegerse de los ataques de ransomware ya que, como he mencionado anteriormente, desde S21sec hemos detectado varios ataques a centros hospitalarios, infectando sus equipos informáticos y extrayendo información confidencial para posteriormente reclamar un rescate económico. En este sentido, los empleados deben saber qué acciones suyas pueden poner en riesgo la ciberseguridad de la infraestructura y, en última instancia, facilitar una brecha que los atacantes aprovechen para desplegar un ramsomware.

Es por ello, que una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector, como estafas en materia de ciberseguridad o tácticas de phishing. Es alarmante que exista tal desinformación en este aspecto, pues la realidad es que hay vidas que dependen de un dispositivo médico, ya sea en su hogar, o en el propio hospital. Ya que es complicado superar la escasez de perfiles cualificados en seguridad, es importante formar al personal y además, confiar en empresas de ciberseguridad que puedan proporcionar respuestas de incidentes desde un SOC-OT.

En definitiva, además de apostar por la formación en ciberseguridad en entornos sanitarios, los fabricantes de los dispositivos médicos y las empresas de seguridad deberían trabajar conjuntamente para diseñar dispositivos óptimos, velando por la seguridad de los pacientes y empleados de los centros sanitarios. En S21sec contemplamos un futuro cercano donde será posible lograr este objetivo que podrá reducir tiempo y costes y, lo más importante, priorizar la seguridad, ante todo. ■

Seguridad y concienciación para evitar ataques

Tres son los retos que tiene el sector sanitario en estos momentos: asegurar la confidencialidad de los datos, proteger la red de comunicaciones y salvaguardar los dispositivos de salud. Para afrontarlos, se debe establecer una estrategia basada en la seguridad de esos activos, pero sin descuidar la formación de las personas.

El sector sanitario se ha alzado como uno de los principales objetivos de los ataques cibernéticos, incrementándose el número de ofensivas alarmantemente. Por este motivo, Jairo Alonso, consultor de sistemas de control industrial de S21sec, explica qué acciones son necesarias para proteger datos y recursos adecuadamente, además de ofrecer otra serie de recomendaciones de seguridad a llevar a cabo.

Efectivamente, por las actuales circunstancias, el sector sanitario se enfrenta a tres retos principales: asegurar la confidencialidad de las historias médicas, proteger su propia red corporativa de comunicaciones, y salvaguardar los dispositivos de salud destinados a monitorizar las constantes vitales de los pacientes cuando están ingresados en un centro médico.

La historia médica no deja de ser información que debe resguardarse ya que se trata de datos críticos que pueden determinar en muchos casos acciones respecto a una persona.

En base a ello, se hace imperativo que esa información no quede alojada en cualquier servidor, sino en servidores internos corporativos. Los datos tampoco deben estar publicados en Internet, ni ser accesibles desde el exterior, y cuando sea necesario realizar un intercambio de información, por un tema de pacientes o similar, utilizar siempre canales seguros. Asimismo, y siempre que sea posible, es recomendable utilizar redes propias, y no recurrir a servicios de terceros que puedan poner en riesgo la información de los pacientes.

No obstante, y pese a seguir estas recomendaciones los datos pueden enfrentarse a amenazas que, como el ransomware, están golpeando con fuerza desde hace meses al sector sanitario.

Como medidas de seguridad y de protección ante este tipo de amenaza, Jairo Alonso recomienda, como primer punto, la formación, a fin de que las personas sean capaces de identificar por dónde puede entrar un ataque de ransomware y

notificar cada vez que detectan una brecha. También es muy importante disponer de herramientas de monitorización de la red del sistema sanitario en general, para que al menor indicio de una posible brecha de seguridad o de un ataque, se tenga constancia, y pueda contenerse. El objetivo es evitar por todos los medios que el ransomware se expanda a otros servicios y que los ciberatacantes consigan cifrar historias clínicas de pacientes, lo que impediría tratar adecuadamente a estos usuarios. Además de acciones para luchar contra el ransomware, Jairo Alonso ofrece tres recomendaciones de seguridad a llevar a cabo.

La primera de tiene que ver con la separación o aislamiento de diferentes componentes que integran la infraestructura tecnológica, como son la red que da servicio a los dispositivos de monitorización de salud, la red en la que se incluyen las herramientas de trabajo habituales del sector (correo electrónico, páginas web, etc.), y las historias clínicas y su acceso. Adicionalmente, es muy importante crear políticas y procedimientos que permitan asegurar y elevar el nivel de seguridad sanitario, imponiendo medidas que impliquen mejoras de dispositivos o adquisición de nuevos elementos de seguridad, entre otros.

El último es la concienciación. Es fundamental que todo el personal, esté muy concienciado y comprenda de dónde puede venir un ataque, y qué medidas se pueden tomar para prevenirlo y que no se produzca.

Ciberseguridad en el sector sanitario en pandemia

IVAN MATEOS, Ingeniero Preventa, Sophos

El sector de la salud es hoy muy vulnerable. En medio de una de las peores crisis sanitarias que ha golpeado a la sociedad moderna, los ciberatacantes están explotando hechos como el aumento del teletrabajo, que en muchos casos se ha iniciado con poca o ninguna experiencia y planificación previa, miedo y ansiedad, y una fuerza laboral médica con exceso de trabajo.

El fallo de los sistemas de atención médica puede tener consecuencias nefastas: problemas en ordenar medicamentos, perder el historial médico de un paciente, programar operaciones o hacer que las ambulancias no estén disponibles a tiempo durante las emergencias. Por otro lado, los ciberdelincuentes aprovechan cada vez más la mayor dependencia de la atención médica de herramientas y dispositivos digitales. Se han aprovechado de esta crisis global lanzando ciberataques a través de correos electrónicos de phishing con temas relacionados con la pandemia, ataques de ransomware spear-phishing, que paralizan la atención médica y comprometiendo emails empresariales.

Además, para adaptarse al número de infecciones en rápido aumento y para respaldar la infraestructura de atención médica existente, muchos países han tenido que crear instalaciones médicas temporales para albergar a los pacientes infectados por COVID-19 o para atender los turnos de vacunación. Dado que estas instalaciones se crean rápidamente y la prioridad es brindar atención al paciente, la seguridad se convierte en una prioridad menor, y se pasan por alto muchos pasos cruciales para proteger las redes y los dispositivos y la información que estos manejan

Un resultado de la pandemia también ha sido el aumento significativo en la cantidad de datos de salud de los pacientes almacenados por el gobierno y las organizaciones de salud. Los datos personales como los parámetros de salud diarios, el estado de salud comórbido, los proveedores de seguros, así como el seguimiento de todos aquellos que entran en contacto con una persona infectada, pueden explotarse para el robo de identidad y venderse por un alto valor en la dark web.

Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques. A continuación, damos cinco consejos de seguridad para intentar conseguirlo:

1. ADOPTAR EL MODELO DE SEGURIDAD DE CONFIANZA CERO O ZERO TRUST

Un informe reciente muestra que en el sector sanitario hay más infracciones causadas por amenazas internas que externas. Esto puede atribuirse a un error humano, a la falta de supervisión en ciberseguridad o al abuso intencionado del privilegio de acceso a datos y sistemas confidenciales.

Al implementar un enfoque de confianza cero, las organizaciones de salud pueden introducir controles granulares en el tráfico de la red. Esto limita la oportunidad de que los atacantes y los usuarios deshonestos obtengan acceso a información personal confidencial de salud (PHI) mientras permanecen bajo el radar.

2. MEJORAR LA CIBERSEGURIDAD CONTRA LOS ATAQUES DE RANSOMWARE

El ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario, y es responsable de más del 70% de los brotes de malware en el sector.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros sanitarios para que los sanitarios no puedan acceder a ellos.

Sophos no sólo ofrece una seguridad líder en ransomware, sino que también realiza un seguimiento del desarrollo de ransomware mediante una rigurosa investigación de SophosLabs. Sophos Intercept X con EDR y Sophos XG Firewall trabajan conjuntamente para interrumpir y rechazar los ataques avanzados de ransomware.

3. SUPERAR LA ESCASEZ DE PERSONAL CUALIFICADO

La falta de personal contratado con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud. Esto es especialmente un dolor de cabeza para aquellos que no tienen un experto en seguridad a tiempo completo.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio ofrece una supervisión eficaz y una evaluación continua de los riesgos, así como un equipo de expertos dedicado las 24 horas del día, los 7 días de la semana a mitigar y resolver cualquier ataque.

> "Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques"

Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta a incidentes reales contra las amenazas, asegurando que el riesgo se identifica, se contiene y que se toman medidas correctivas de inmediato.

4. CUBRIR LOS PUNTOS CIEGOS EN SUS ESFUERZOS DE TRANSFORMACIÓN DIGITAL

Las transacciones de información entre los pacientes, los cuidadores, aseguradoras y otras partes interesadas deben ser fluidas pero tambien seguras.

Es crucial proporcionar un acceso fiable y seguro a los datos clasificados de la asistencia sanitaria en un momento en que muchos hospitales están adoptando nuevas tecnologías como los dispositivos médicos conectados a la red, la telesalud y aplicaciones médicas como los sistemas de comunicación y archivo de imágenes (PACS).

Sophos, con sus últimos dispositivos XG Firewall y SD-RED, hace posible conseguir una conectividad en línea con sus objetivos de seguridad y continuidad. Se permite no solamente enrutar tráfico a nivel de aplicación o usuario sino también aprovechar todas las ventajas de la seguridad sincronizada de Sophos en entornos SD-WAN

5. PROMOVER LA CONCIENCIACIÓN EN CIBERSEGURIDAD

Otra preocupación importante para el sector sanitario es la falta de formación sobre ciberseguridad y la escasa conciencia sobre la privacidad de los datos entre los empleados.

Las organizaciones de atención sanitaria deberían realizar campañas periódicas de sensibilización para que sus empleados, socios y proveedores sean más conscientes de las últimas estafas y de las tácticas de phishing, y así estar mejor preparados para tomar las medidas adecuadas cuando se encuentren con malware o phishing.

Con Sophos Phish Threat, los equipos de seguridad informática pueden simular ataques de phishing con sólo unos pocos clics, y proporcionar formación rapida,automatizada e in situ a los empleados de atención sanitaria según sea necesario. ■

Mantener el servicio activo protegiendo la información

Los ciberataques contra el sector sanitario se han multiplicado en el último año, y este sector se enfrenta al reto de proteger sus activos. Abordando esta realidad, Iván Mateos, Sales Engineer de Sophos, explica por qué el sector socio sanitario está recibiendo más ataques que ninguna otra industria, y ofrece las claves para mantener la actividad diaria sin alteraciones mientras se aseguran todos los activos.

Efectivamente, por las actuales circunstancias, el sector sanitario, no solo hospitales sino también los laboratorios o las farmacéuticas, se ha convertido en una realidad muy visible, hecho que no pasa desapercibido para los ciberatacantes.

En este sentido, Iván Mateos considera que además de lanzar su artillería en modo de ciberataques contra organizaciones, también lo han hecho contra los usuarios, que a diario reciben emails de phishing, con la excusa de una vacuna o de cualquier otro tema sanitario.

Por tanto, y para frenar esta incertidumbre, el sector sanitario tiene que poner remedio, y afrontar algunos retos, siendo el principal el de mantener el servicio lo más activo y productivo posible, pero sin olvidar que lo que manejan y gestionan es información muy sensible: los datos de los usuarios o de los pacientes. De este modo, esta digitalización que está acometiendo el sector sanitario para mejorar la infraestructura debe ir acompañada innegablemente de ciberseguridad, que debe ser tomada como un valor elemental.

DISPOSITIVOS IOT

Importante es también custodiar los dispositivos que manejan datos sensibles, como los dispositivos IoT, que pueden recolectar cantidades significativas de información sobre sus usuarios y su entorno. Por ello, es imperativo minimizar los riesgos de sufrir un incidente de seguridad, protegiendo tanto el dispositivo como la información que gestiona. A este respecto, es necesario salvaguardar la conexión a la red de estos dispositivos, limitar su acceso, (el qué y quién puede acceder a qué).

Hoy en día, en el mercado, ya existen soluciones de segmentación de red, firewalls, y dispositivos de protección que ya tienen en cuenta los equipos de IoT, por lo que es perfectamente compatible la integración de este tipo de dispositivos con la parte de ciberseguridad.

Por último, Iván Mateos lanza también unas cuantas recomendaciones para que los responsables de IT mantengan la seguridad a raya. Entre ellas destaca la importancia de no alargar la vida de equipos que están fuera de soporte, aplicaciones antiguas, sistemas operativos obsoletos. En este sentido reconoce que, aunque es difícil el cambio, hay que entender que estos son problemas de seguridad. Por tanto, hay que intentar mantener aplicativos y sistemas lo más actualizados posibles, optar por soluciones de ciberseguridad que permitan un manejo sencillo, como es el caso de Sophos, que cuenta con una consola para todos los productos, lo que simplifica la ecuación.

Adicionalmente, y para mejorar esta seguridad, Mateos sugiere aplicar el concepto de las tres Cs: cifrado de los dispositivos, con el objetivo de que si se pierde un dispositivo que no se pierda la información; cambio de contraseñas; y, por supuesto, concienciación, con recursos didácticos y de entrenamiento. Si se consigue eso, si se acompañan las herramientas de nueva generación con concienciación, todo puede ser mucho más efectivo.

S21SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

Los cuidados sanitarios deben dejar atrás las redes heredadas

Nadie duda de que en plena pandemia es más complicado planificar una actualización tecnológica de amplio espectro en la red de su organización de cuidados sanitarios. Sin embargo, de algún modo, el estrés experimentado por los proveedores de cuidados sanitarios hace que ahora sea el momento perfecto para observar cómo funciona la red desde un nuevo ángulo y determinar qué nuevas e inteligentes posibilidades surgen a raíz de la pandemia

Si hay algo que hemos aprendido todos desde comienzos de 2020 es que la adaptabilidad y la flexibilidad de las redes es incluso más importante de lo que se creía antes. Las redes de atención sanitaria a menudo se ven limitadas por sistemas antiguos ineficaces y aislados que resultan difíciles de mejorar y, algunas veces, imposibles de integrar. Ahora que las normas de atención sanitaria han cambiado radicalmente, estos límites resultan más costosos e insostenibles. Si la eficacia operativa se ve mermada, también se resiente el estado operativo de su organización.

LOS RETOS DEL FUTURO Y LOS QUE YA ESTÁN AQUÍ

El rápido cambio realizado para adoptar interacciones de telemedicina, los servicios digitales de hospitalización y la conexión al Internet de las Cosas Médicas (IoMT) crean nuevos requisitos para la red y su infraestructura.

Para seguir el ritmo y abordar la necesidad de disponer de redes fiables, adaptables y seguras, la actualización de la red es la única opción que permite la forma de suministrar atención médica al paciente. Al mismo tiempo, los elevados costes asociados a la actualización pueden resultar abrumadores y los proveedores de servicios sanitarios deben sopesar las opciones de soluciones con sus necesidades. La inversión debe estar justificada por la duración de la solución, y dicha duración puede determinarse en función de lo sólida y adaptableque sea.

OPORTUNIDADES DISPONIBLES CON LA INFRAESTRUCTURA DE RED ACTUALIZADA

Una red preparada para el futuro es algo más que una infraestructura física más rá-

pida. Supone analizar las estrategias y las soluciones para mejorar el modo en el que se ofrecen los servicios sanitarios y se utilizan las instalaciones. Las soluciones adecuadas pueden hacer posibles nuevos enfoques, arquitecturas y capacidades, como los que se describen a continuación:

- **Capacidades de edificio inteligente** que conectan los sistemas de calefacción, refrigeración, iluminación y otros servicios ambientales y de seguridad a un gestor de redes automatizado que maximiza el bienestar y reduce los costes
- **Robótica y realidad aumentada** impulsadas por redes con ultra alta velocidad que realizan procedimientos complejos para ofrecer decisiones mejor informadas y resultados óptimos para los pacientes
- **Sistemas blockchain seguros** que permiten realizar un registro preciso del inventario y la cadena de suministro, las transacciones financieras, los tratamientos de los pacientes, el procesamiento de reclamaciones de seguros sanitarios y mucho más
- **Plataformas de aprendizaje mejoradas** necesarias para que los médicos y el personal puedan adoptar estas múltiples y beneficiosas prácticas de manera rápida y eficaz y disfrutar así de un uso compartido de datos más eficaz tanto en el ámbito de la práctica médica como en el de la investigación
- **Informática en la nube** que proporciona una plataforma más sólida que la que se obtendría in situ y que aumenta las oportunidades de procesamiento analítico, automatización operativa y comunicación del personal
- **Redes 5G** que ofrecen lo más novedoso en alta velocidad, rendimiento de baja latencia en interiores y exteriores para conectar a médicos, personal, pacientes, visitas y dispositivos IoMT conectados como dispositivos “wearable” para los pacientes
- **Plataformas interoperables** que conectan disciplinas y departamentos con el objetivo de simplificar el uso compartido de información crítica y la toma de decisiones
- **Sistemas basados en IA** que ayudan a obtener diagnósticos precisos y tratamientos eficaces
- **Soluciones de procesamiento del lenguaje natural (PLN**) que pueden generar notas médicas precisas a partir detexto hablado
- **Análisis médicos** que pueden procesar de manera eficaz enormes cantidadesde datos no estructurados para revelar patrones ocultos en tratamientos y resultados de pruebas
- **Análisis operativos** que pueden informar a los responsables de la toma de decisiones del flujo de trabajo, la seguridad, la sostenibilidad y los procesos logísticos para aumentar la eficacia operativa de todos los aspectos del centro

Estas son solo algunas de las nuevas herramientas disponibles para los proveedores de servicios sanitarios que, en una realidad post pandémica, serán cada vez más importantes para el funcionamiento eficaz de una organización de servicios médicos, tanto en el caso de prácticas médicas individuales como hospitales y centros de investigación.

No obstante, el único prerrequisito que comparten todas ellas es una infraestructura de red unificada, sólida y preparada para el futuro, y aquí es donde más destaca el exclusivo valor de CommScope como Partner de soluciones. ■

MÁS INFORMACIÓN

- Soluciones CommScope para el sector sanitario
- Infografia de la Solución de Healthcare
- Infografía de la Solución de Redes

GRENKE. Una amplia experiencia en renting

GRENKE es una compañía especializada en ofrecer a las pequeñas y medianas empresas, y a toda empresa en expansión, el renting como alternativa a la financiación tradicional para la adquisición de tecnología y equipamiento.

Los esfuerzos de GRENKE, van enfocados a combinar el negocio innovador del renting con la rapidez, la confianza y la cercanía, manteniendo siempre vivo nuestro espíritu emprendedor.

La adquisición de equipamiento tecnológico a través del renting es un modelo en alza por sus claras ventajas financieras, fiscales y operativas: Se paga a medida que se usa el bien, no en el momento de la adquisición; las cuotas mensuales son deducibles al considerarse gasto; y al finalizar el contrato se pueden renovar los equipos para así estar siempre a la vanguardia y ofrecer una inmejorable imagen al cliente.

Sabemos que hoy por hoy la tecnología es clave y gracias a nuestras soluciones de renting queremos hacer llegar a todas las empresas, pertenezcan al sector o industria que pertenezcan, la posibilidad de crecer, adaptarse o innovar.

GRENKE permite que el cliente, ya sea un autónomo, una empresa, un organismo público o una startup, pueda arrendar prácticamente todo el equipamiento necesario para el desarrollo de la actividad de su negocio incluyendo software, iluminación, TPV, robots o cualquier otro equipamiento. También permite al cliente obtener una planificación realista gracias a las cuotas fijas y una optimización de su tesorería, mejor pagar por uso que hacer un gran desembolso inicial.

GRENKE ofrece a clientes dos grandes líneas de soluciones:

Contrato Classic: Con esta solución cualquier empresa o negocio podrá adquirir el equipamiento que necesite en un momento dado. Desde una máquina de café hasta un equipo de resonancia.

Póliza Máster: Si la empresa requiere el renting de equipos con regularidad, enton-ces la opción perfecta es nuestra línea de renting,

permitiéndole ahorrar dinero y ofreciéndole ventajosas condiciones.

De esta forma cuidamos y ayudamos a nuestros clientes o partners. Ya que consi-de-ramos cada relación única, debido a que cada negocio tiene necesidades particulares que suponen para nosotros retos distintos cada vez. Por ello trabajamos día a día en soluciones de renting tecnológico y de equipamiento que se adapten 100 % a cada necesidad: contratos desde 500 euros, respuesta a las operaciones en 20 minutos con la mínima documentación y, por supuesto, firma electrónica de los contratos.

En este sentido primero ofrecimos la firma digital eSignature, con la que se pueden firmar los documentos contractuales directamente en pantalla y devolverlos firmados vía digital en un abrir y cerrar de ojos, de forma segura y jurídicamente vinculante. Desde casa, desde la oficina o en movimiento. Todo lo que se necesita es un ordenador, un portátil o un Smartphone, y acceso a internet.

Y ahora, adicionalmente a la firma digital eSignature, nuestros clientes y partners pueden optar por la firma del contrato a través nuestra Signing App. Una carpeta virtual que permite firmar los contratos de manera electrónica sin perder el contacto cercano entre ambas partes.

De esta forma podemos alcanzar nuestro objetivo que no es más que facilitar a los empresarios la puesta en marcha de sus ideas y proyectos. Después de todo, GRENKE también comenzó siendo solo una idea. Cuando empresarios y emprendedores necesitan adaptar la tecnología de su negocio y no disponen de solvencia para hacerlo, el renting de GRENKE es la solución perfecta.

Algo que ya muestra nuestro propio eslogan de marca «Fast. Forward. Finance». Ofrecemos un valor añadido a nuestros clientes porque son nuestra prioridad. ■

MÁS INFORMACIÓN

- Información para partners
- Información renting tecnológico
- Información Productos
- Información Contrato Classic
- Información Póliza Máster
- Información Rent Back
- Información GRENKE para la sanidad

La detección y prevención, claves en la protección

S21sec es la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones.

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

Una plantilla de más de 410 expertos reflejan las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec es líder sectorial en España y Portugal por historia, formación, infraestructura y equipo. Está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC global distribuido en cuatro localizaciones, que garantiza la integridad de más de 500 organizaciones en España, Portugal y México.

Su porfolio, que aúna soluciones diferentes de manera transversal, está diseñado en torno a cinco necesidades:

1. Identificar: análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.

2. Proteger: diseño y despliegue de arquitecturas y tecnologías, servicios de forma-

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones

ción y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

3. Detectar: SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.

4. Responder: CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.

5. Recuperar: Continuidad de negocio y planes de respuesta ante ciber-desastres.

Por último, S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

* **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
* **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
* **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
* **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
* **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
* **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse. ■

MÁS INFORMACIÓN

- Rediseños de arquitectura de red en SCI
- Detección de anomalías
- Evaluación y gestión de vulnerabilidades
- Inventario de activos

Proteger las TI a partir del conocimiento de las amenazas

La ciberdelincuencia está cambiando y los ciberdelincuentes cada vez están más preparados y coordinados entre sí, utilizando herramientas muy sofisticadas y difíciles de detectar y de parar, por lo que hay que estar constantemente monitorizando y conocer cuál es la situación de la empresa ante cualquier potencial amenaza.

Las soluciones de Sophos destacadas este año y las que mayor crecimiento están demostrando son:

SOPHOS EDR/XDR

Un completo sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti Exploit, Comportamiento, anti ransomware y anti hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con nuestros firewalls y sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

SOPHOS MTR, MTR-E Y RAPID RESPONSE

Sophos Managed Threat Response (MTR) es un servicio gestionado de Respuesta frente a Amenazas, que ofrece a las empresas funciones de búsqueda, detección y respuesta ante

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos así como los accesos a servicios en nube

posibles amenazas 24/7. Está formado por un equipo de detección de amenazas y expertos en dar respuesta, capaz de tomar medidas para neutralizar incluso las amenazas más sofisticadas. El factor diferencial de esa solución es que, cuando otros sólo notifican, Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y mitigación de la amenaza.

Si aún no es cliente de Sophos, cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response. Un conjuntode productos y un equipo de expertos que son capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible.

SOPHOS ZTNA

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos, así como los accesos a servicios en nube. Todo ello gestionado desde Sophos Central, integrándose con el cliente de Seguridad Endpoint para facilitar los despliegues y adopción de las nuevas metodologías de conexión, evitando los problemas “habituales” de los sistemas VPN y SD-WAN tradicionales. El modelo Zero-Trust Network Access permite a los usuarios conectarse de forma sencilla a los recursos corporativos desde cualquier ubicación y al mismo tiempo mejora su seguridad al verificar de manera constante al usuario y validar el estado y el cumplimiento del dispositivo, así como la red desde donde se conecta.

SEGURIDAD SINCRONIZADA

Sophos lleva ya más de 5 años conectando a través de su Seguridad Sincronizada los distintos sistemas de protección, compartiendo información.

SOPHOS CLOUD OPTIX

Conscientes de que la TI está migrando a la nube, Sophos propone CSWP y CSPM gracias tanto al agente para servidores como a Cloud Optix, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud o Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake.

SOPHOS FIREWALL

La seguridad de red no queda desatendida en Sophos. Desde la compra de Astaro en 2008, la han seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de nuestra estrategia XDR. ■

MÁS INFORMACIÓN

- Informe de Amenazas 2021
- La evolución de la ciberseguridad: el impacto empresarial de Sophos
- Guía de respuesta a incidentes

El sector sanitario está en el punto de mira de los ciberdelincuentes

Sophos Endpoint

Intercept X with EDR

Impida que su organización se vea afectada por el ransomware.

Sophos Endpoint incluye tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

SOPHOS

Cybersecurity evolved.

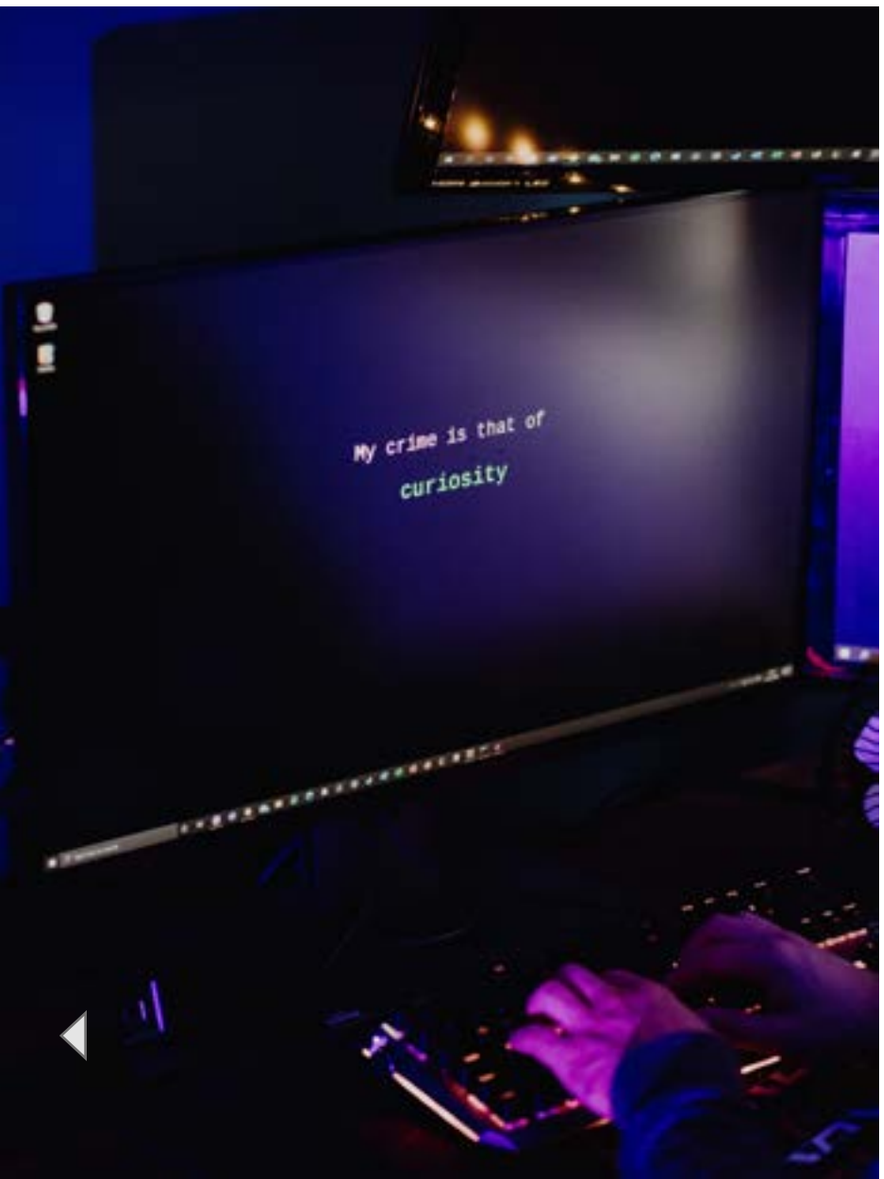
BAS, la simulación de ataque al rescate

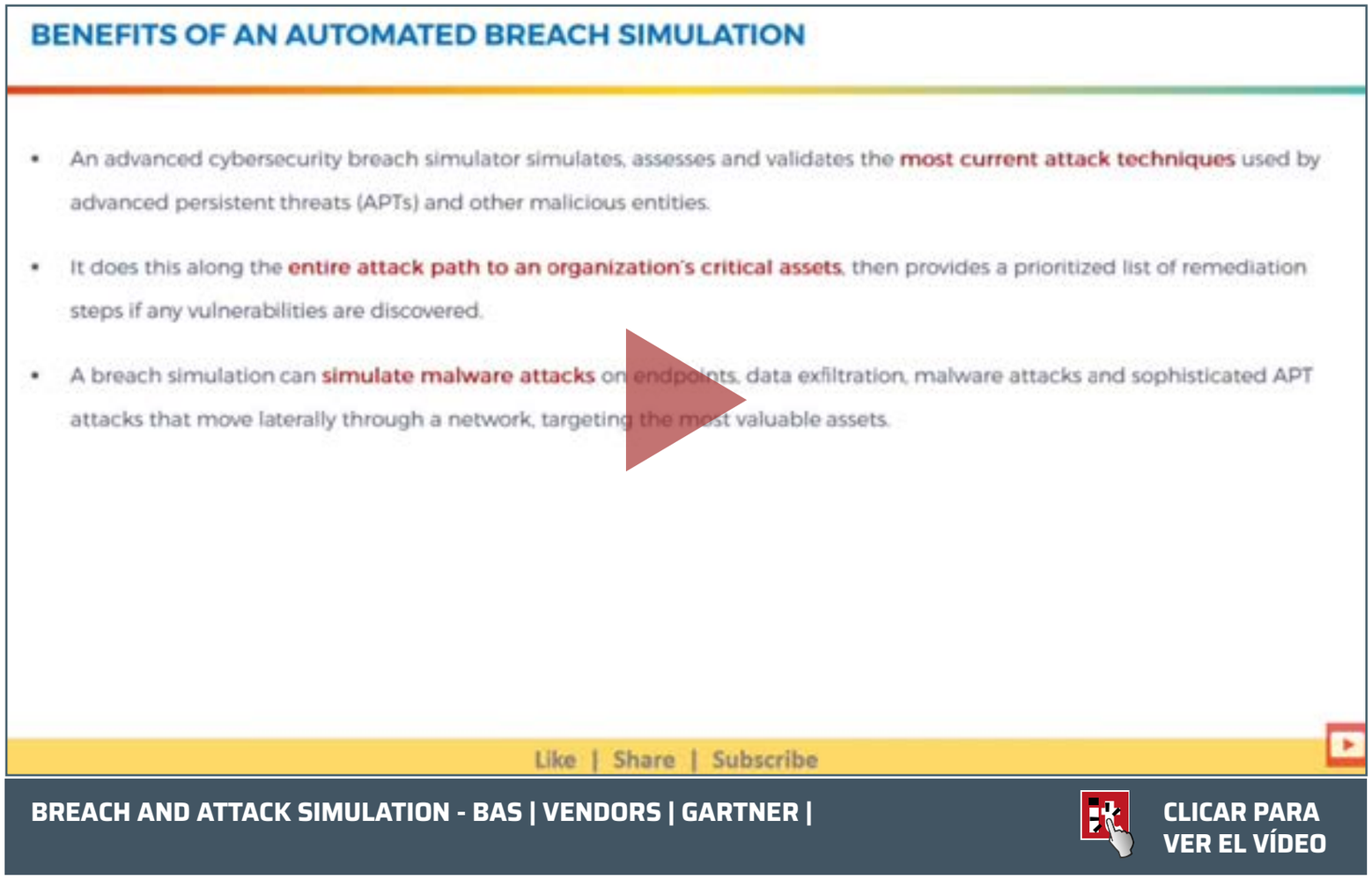
Con el crecimiento de la complejidad de los entornos empresariales y la naturaleza dinámica del panorama de amenazas, los equipos de seguridad no pueden confiarse. Tener la mejor solución en un entorno cambiante, híbrido, multicloud y deslocalizado no es garantía, ni siquiera tener, como así es, decenas de soluciones que tienen que interactuar y ser flexibles. Cuando un error de configuración puede habilitar el ataque, la necesidad de comprobar de manera constante y automatiza cuál es la postura de seguridad de las empresas se vuelve vital. Las soluciones BAS, o de simulación de brechas y ataques, vienen al rescate haciendo que las pruebas de seguridad sean mucho más simples.

Los ciberataques han evolucionado drásticamente en las últimas dos décadas en cuanto a sus capacidades, alcance, repercusiones, número de objetivos, etc. Lo que la ciberdelincuencia genera a nivel mundial está alcanzando máximos históricos y parece que esto solo empeorará. El riesgo de ser atacado es tan alto que las empresas, en general, buscan mejorar su postura de seguridad pasando de una actitud reactiva a una proactiva, apostando por soluciones, modelos y arquitecturas que sean capaces de hacer frente a los ciberdelincuentes.

Las empresas tienen cada vez más soluciones que cuesta integrar y gestionar. Además, se puede observar un crecimiento continuo y rápido en la adopción de negocios digitales en todo el mundo, lo que aumenta la cantidad de soluciones que dependen de las aplicaciones y a menudo se pasa por alto la necesidad de probar si las soluciones implementadas realmente funcionan o si los perímetros defensivos tienen alguna brecha que los atacantes puedan aprovechar. La cruda realidad es que solo se necesita una vulnerabilidad para que los ciberdelincuentes se cuelen en los sistemas.

Las simulaciones de brechas y ataques de seguridad pueden desempeñar un papel fundamental en la protección de los activos





Ahora es posible verificar las defensas a través de una variedad de métodos de prueba. Se pueden realizar escaneos de vulnerabilidades, pruebas de penetración, implementar los red y blue teams, y realizar simulaciones de brechas y ataques (BAS), que son los que están emergiendo como uno de los enfoques más avanzados, fiables y sencillos.

En 2017, Gartner acuñó el término Breach and Attack Simulation (BAS) para describir una nueva ola de tecnologías de prueba de controles de seguridad capaces de automatiza las capacidades de testing. Las soluciones BAS ejecutan ataques simulados para determinar si los controles de seguridad detectan y responden a las amenazas como deberían, y luego informan sobre los resultados, ayudando a encontrar brechas de seguridad en una variedad de fuentes.

La misma consultora identificaba, en marzo de 2021, a las soluciones BAS como una de las ocho

Las pruebas de penetración automatizadas requieres de expertos, mientras que las soluciones de simulación de brechas y ataques de seguridad hacen que las pruebas de seguridad sean accesibles para los analistas de seguridad de una gama más amplia de niveles de habilidad

tendencias que desafían las prácticas tradicionales de ciberseguridad. “Están surgiendo herramientas de simulación de ataques y violaciones (BAS) para proporcionar evaluaciones continuas de la postura defensiva, desafiando la visibilidad limitada proporcionada por evaluaciones puntuales anuales como las pruebas de penetración. Cuando los CISO incluyen BAS como parte de sus evaluaciones de seguridad regulares, pueden ayudar a sus equipos a identificar las brechas en su postura de seguridad de manera más efectiva y priorizar las iniciativas de seguridad de manera más eficiente”.

Las plataformas basadas en tecnología BAS permiten a las organizaciones ejecutar simulaciones de ciberseguridad continuas y bajo demanda en cualquier momento sin afectar sus sistemas. Bajo un modelo de Software-as-a-Service (SaaS), simula ataques multivectoriales, internos o externos al enfocarse en las vulnerabilidades más recientes. Estos ataques simulados exponen brechas de vulnerabilidad que le permiten a la organización

determinar si su arquitectura de seguridad brinda la protección adecuada y si sus configuraciones se implementan correctamente.

Find The Gap

No existe la tecnología perfecta. El software, incluidos los sistemas operativos, las aplicaciones e incluso las soluciones de seguridad, a menudo

"El Pentesting comenzó aplicándose en las organizaciones inicialmente verificando la solidez y seguridad del perímetro de las redes de las organizaciones"

Roberto Lopez, Head of Offensive Security Services, Cipher

contienen errores que los atacantes pueden aprovechar. Dado que las aplicaciones de software reciben cambios y actualizaciones continuamente, siempre existe la posibilidad de que se introduzcan fallos en los sistemas.

Además, la mala implementación es otro riesgo. Es común, sobre todo cuando el año pasado la pandemia sanitaria obligó a todos a correr, que algunas organizaciones y equipos de TI apresuren la adopción de herramientas de seguridad. Al hacerlo, es posible que se pasen por alto ciertos pasos al configurar soluciones de seguridad, y la realidad es que incluso las mejores soluciones pueden volverse inútiles si se implementan mal.

Por ejemplo, se pueden tener implementadas las políticas de firewall más estrictas para accesos desde el exterior de la red, pero si falta la protección de su endpoint, es posible que el malware aún encuentre la manera de acceder. Lo mismo ocurre si un empleado inserta una memoria USB infectada en un ordenador, haciendo que el malware pueda propagarse fácilmente desde allí.

Para encontrar la vulnerabilidad o el fallo que permita a los ciberdelincuentes adentrarse en los sistemas hay una serie de tecnologías que pueden utilizarse. Las más habituales son el escaneo de vulnerabilidades, que permite identificarlas buscando software desactualizado, puertos abiertos y certificados caducados que se encuentran en su red.

También son habituales los Penetration Testing, o pruebas de penetración, también conocidos como 'pentesting', en los que se los evaluadores prueban hasta dónde pueden llegar para violar la red empleando tácticas similares a las utilizadas

CYMULATE: BREACH AND ATTACK SIMULATION

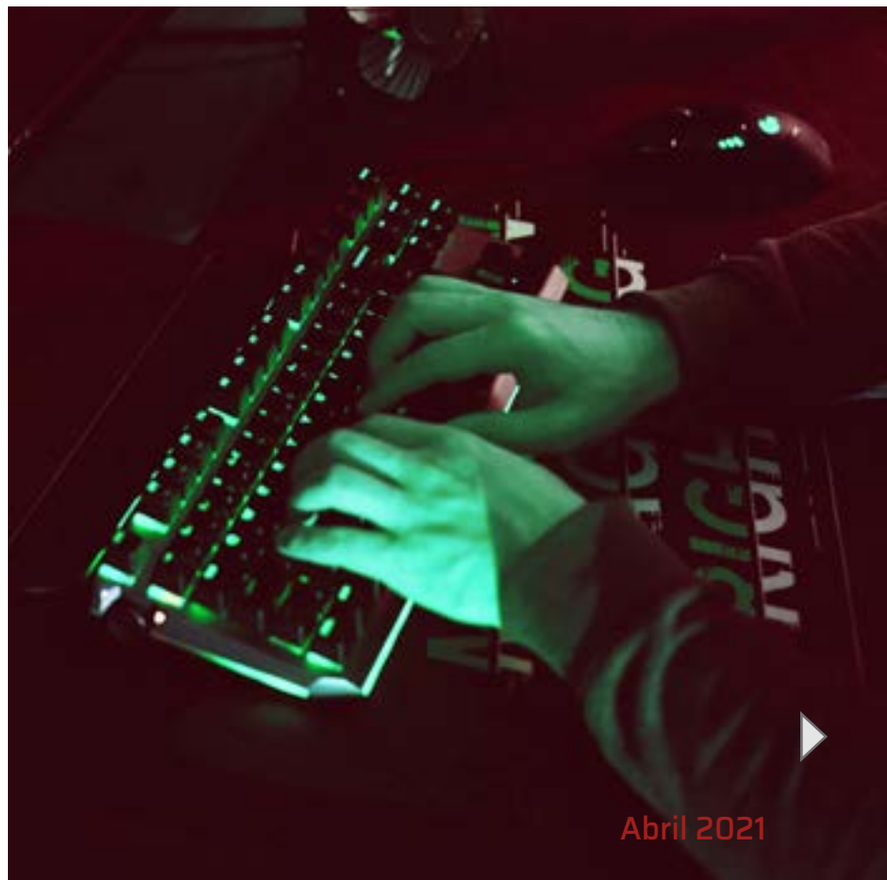
CLICAR PARA VER EL VÍDEO

por los piratas informáticos del mundo real. Y por último están los Red and Blue Team, que son como juegos de guerra en los que el equipo rojo juega el papel de ciberdelincuentes intentando violar el sistema y el equipo azul actúa defendiéndolo.

Penetration Testing

En un mundo en el que la complejidad de los sistemas crece de una manera ilimitada, en el que los entornos y arquitecturas IT de las organizaciones no paran de evolucionar apoyándose en tecnologías que tienen vulnerabilidades, en el que la seguridad no fue implementada nativamente y en el que las aplicaciones están evolucionando de entornos controlados dentro de perímetros a otros basados en la nube, Webs y API´s, el mercado del Pentesting ha tenido que evolucionar adaptándose a los requerimientos de la industria. Quien lo dice es Roberto Lopez, Head of Offensive Security Services de Cipher, el negocio de ciberseguridad de Prosegur.

Explica Roberto López que el pentesting comenzó aplicándose en las organizaciones inicialmente verificando la solidez y seguridad del perímetro de las redes de las organizaciones, pero conforme el perímetro se desplazó al endpoint, y la realidad de las redes en las organizaciones evolucionó a un modelo híbrido, en el que la superficie de exposición se amplió, los requerimientos de auditoría de seguridad crecieron. A los requerimientos iniciales de chequeo de perímetro, se añadieron requisitos para chequear y analizar la seguridad del código de aplicaciones y API´s en el momento



BAS vs Pentesting

Hay una similitud en el mercado del pentesting/BAS y el de antivirus/EDR. Los primeros han evolucionado, los segundos han irrumpido en el mercado. No significa que los primeros no sigan avanzando, pero no por eso los segundos van a desaparecer, y cada uno quiere su parte del mercado.

Dice Roberto Lopez, Head of Offensive Security Services de Cipher, que la principal diferencia entre el pentesting y el BAS radica en la manera de la ejecución de los análisis de seguridad; "mientras una solución BAS permite automatizar la ejecución de pruebas y chequeos de seguridad ahorrando tiempo e inversión en conocimiento, la inteligencia ofensiva está implementada en el propio software, una solución de Pentesting , realizada de manera manual y con un perfil altamente cualificado, va a permitir identificar fallos de seguridad que no pueden ser detectados de una manera automatizada". De forma que, como decíamos unas líneas más arriba, "en muchos casos podrían actuar incluso de una manera complementaria".

Haciendo referencia a las soluciones de pentesting automatizados, dicen desde Cymulate que si bien los los equipos de seguridad están recurriendo a las pruebas de seguridad automatizadas para que sus pruebas sean más frecuentes, exhaustivas y más sencillas de realizar, "la automatización no es sinónimo de simplicidad". Las pruebas de penetración automatizadas requieres de expertos, mientras que las soluciones de simulación de brechas y ataques de seguridad hacen que las pruebas de seguridad sean accesibles para los analistas de seguridad de una gama más amplia de niveles de habilidad. "BAS simplifica las pruebas de seguridad", asegura la compañía.

de desarrollo. Igualmente empezó a ser necesario realizar comprobaciones no solo de integridad de dentro a fuera de la organización, si no que adicionalmente también fue necesario empezar a chequear la seguridad de los sistemas en relación al riesgo interno, seguridad en comunicaciones, etc….evolucionando las pruebas a nuevos modelos definidos como ejercicios de seguridad de Caja Roja, gris, blanca….todo esto contando adicionalmente con el valor de que sea un tercero ajeno a la organización el que realice estas comprobaciones de una manera trasparente y libre de posibles injerencias internas.

"Cualquier empresa necesitaría comprobar la seguridad de sus sistemas, y únicamente sería necesario definir el alcance y la manera de hacerlo teniendo siempre en consideración la naturaleza y particularidades normativas y específicas del negocio, ya que en caso de no hacerlo, el impacto

Las herramientas BAS son una excelente manera para que las empresas y otras grandes organizaciones emulen y comprendan mejor los ciberataques del mundo real

puede hacer que la empresa/el negocio sea inviable", responde este ejecutivo cuando le preguntamos qué perfil de empresas necesitan un pentesting.

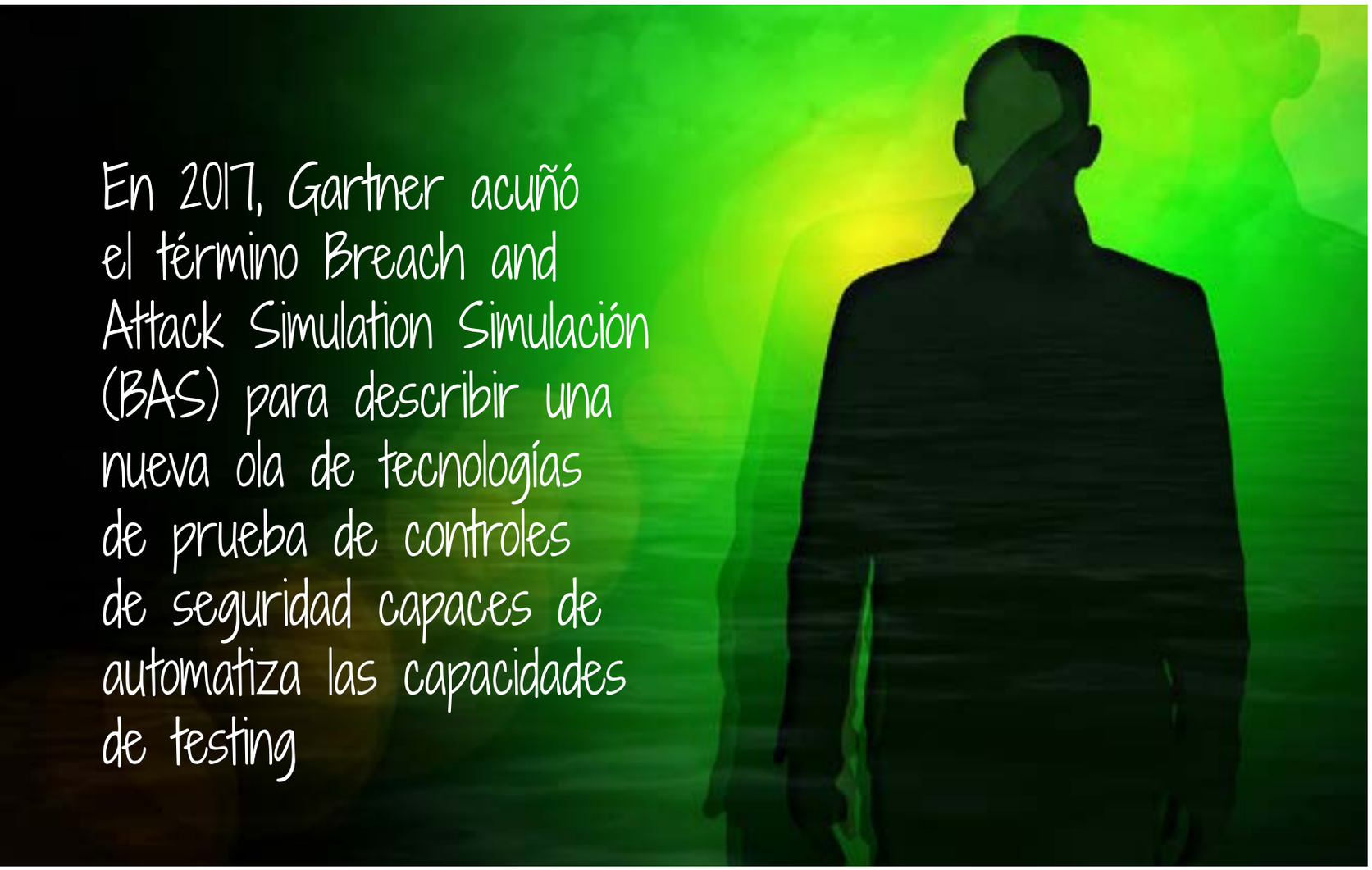
BAS, Breach and Attack Simulation

Generalmente de naturaleza reactiva, los controles de ciberseguridad suelen depender demasiado de la detección y respuesta a incidentes inmediatos. Este enfoque puede ser adecuado para algunos ataques, pero no funciona bien ataques avanzados. Para una mejor defensa, las empresas están comenzando a recurrir a las soluciones de simulación de ataques y brechas (BAS), que prueban la seguridad de forma automatizada y continua. Además son una excelente manera para que las empresas y otras grandes organizaciones emulen y comprendan mejor los ciberataques del mundo real.

La inevitable rotación de personas y los cambios de ciclo dejan brechas en la seguridad, como servidores sin parchear, firewalls mal configurados o el temido shadow IT. Las pruebas periódicas pueden no ser suficientes para detectar esos fallos porque pueden quedar obsoletos rápidamente, por eso una de las grandes ventajas de las soluciones BAS es que permiten realizar pruebas continuas y automatizadas.

El escaneo de vulnerabilidades a menudo simplemente enumera las vulnerabilidades encontradas, lo que requiere que se revise y comprenda la información antes de poder hacer algo. BAS proporciona información procesable en los informes para que pueda realizar ajustes más específicos a las medidas de seguridad de manera inmediata.

También permiten simular diferentes tipos de ataques en cortos periodos de tiempo, por lo que pueden medir más rápido la seguridad de una empresa frente a un ataque. Otra de las ventajas de las soluciones de simulación de brechas y ataques de seguridad imitan diferentes tipologías de ataques, adecuándose a la industria y ubicación del cliente. También pueden centrarse en la seguridad de activos específicos, como pueden ser las bases de datos, las aplicaciones o los dispositivos de red, que tienen vulnerabilidades y controles únicos que deben probarse continuamente para garantizar el nivel más alto de protección.



Enlaces de interés...

- Cómo BAS acabó con el pentest
- BAS, o cómo la simulación de ataques puede aumentar tu seguridad
- Breach Attack Simulation (BAS) – Advanced Penetration Testing

Además, las soluciones BAS son muy útiles para probar la eficacia de los nuevos controles de seguridad, que necesitan una simulación de ataques automatizada y exhaustiva antes de poder confiar en ellos en la producción.

También hay que destacar que muchas plataformas BAS son intuitivas y ofrecen interfaces y paneles de control fáciles de usar. Esto significa que no es necesario ser un experto para ver si las defensas de una empresa son vulnerables. Por otra parte, algunos servicios están disponibles como plataformas basadas en la nube, lo que le permite ejecutar pruebas desde prácticamente cualquier lugar.

Lo que está claro es que la falsa sensación de seguridad es peligrosa. Contar con soluciones de seguridad del más alto nivel no significa que las defensas sean impenetrables. Esto hace que las simulaciones de brechas y ataques de seguridad pueden desempeñar un papel fundamental en la protección de los activos.

Al hacer esto de manera automatizada y continua, las simulaciones de infracciones brindan protección ininterrumpida y permiten a los defensores adoptar una postura más agresiva para mantener la seguridad en todos los aspectos de un entorno de seguridad.

Compartir en RRSS

it Reseller
TECH&CONSULTING

Cada mes en la revista,
cada día en la web.

EDU ORTIZ

PRESIDENTA DE WOMEN4CYBER SPAIN

Ingeniera industrial por la PUCMM y Master of Science en Ingeniería por la Arizona State University con una beca Fulbright, Edu Ortiz lidera las Alianzas Estratégicas en SAS y es la fundadora y presidenta de la asociación Women4Cyber Spain. Con más de 30 años de experiencia, principalmente en el área de consultoría de negocios y sistemas de información, las prioridades de Edu Ortiz en los últimos años han sido desarrollar soluciones utilizando Ciberseguridad integrada con analítica de datos, inteligencia artificial y transformación digital. Edu tiene una amplia experiencia en transformación y desarrollo de negocios y gestión de alianzas en entornos internacionales y multiculturales, y además es líder del MeetUp de Madrid de Women in Machine Learning & Data Science (WiMLDS) y mentora de varios programas de apoyo al talento femenino.

Ciberseguridad y alfabetización digital:
El desafío de la diversidad y la inclusión

Desde Women4Cyber Spain agradecemos a IT Digital Security por ofrecernos este espacio como altavoz para dar visibilidad a las referentes femeninas que tenemos en el sector, a dar relevancia a los temas que nos parecen clave para enfrentar mejor los retos a los que nos enfrentamos como sociedad para promover, impulsar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad y la tecnología en general.

Compartir en RRSS

La pandemia que estamos viviendo ha acelerado aún más la adopción de la vida digital en todos los aspectos profesionales y personales. Se ha consolidado la necesidad de contar con una sólida estrategia digital centrada en los datos y en la ciberseguridad para las empresas de todos los sectores y tamaños.

Las consecuencias económicas y de reputación asociadas al riesgo cibernético se multiplican y la Transformación Digital en la vida y el negocio apuran esta necesidad. No está tan extendido aún el concepto de Ciberseguridad por diseño en las organizaciones, ni está claro que apostar por la innovación y la calidad signifique apostar por ello.

Sin embargo, numerosos estudios indican que las empresas aumentan anualmente su gasto en Ciberseguridad, aunque no a la par de que crecen las vulnerabilidades. La inversión se destina más a remediar que a prevenir. Lo que promovemos es apostar por la Ciberseguridad desde el diseño y concepción de los servicios, aplicaciones y desarrollo de software, y no como un agregado posterior.

Cada día es más relevante para las organizaciones implementar políticas y herramientas para desarrollo seguro y modelado de amenazas, antes de comenzar a desarrollar cualquier aplicación

Cada día es más relevante para las organizaciones implementar políticas y herramientas para desarrollo seguro y modelado de amenazas, antes de comenzar a desarrollar cualquier aplicación o servicio

WOMEN4CYBER SPAIN ES EL CAPÍTULO ESPAÑOL de la Fundación Europea sin ánimo de lucro W4C, cuyo objetivo es promover, impulsar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad y la tecnología en general. Está dirigida a todos los públicos, masculino y femenino, porque juntos es que logramos hacer el cambio social necesario para aprovechar todo el talento disponible. Nuestra misión es fomentar e impulsar las sinergias público-privadas, privadas-privadas y con la sociedad civil de manera de crear entre todos un mundo digital más seguro, colaborativo e inclusivo.

o servicio. Poner el acento en la seguridad en la nube, para proteger y controlar el acceso a los servicios, aplicaciones y datos, y no delegar, si no compartir con los proveedores de servicio en la Nube la responsabilidad en ciberseguridad.

También son y seguirán siendo relevantes los servicios de analítica de ciberseguridad, donde las organizaciones orquestarán los elementos de Ciberseguridad y de Internet de todas las cosas (IoT) usando todas las tecnologías disponibles (Machine Learning, IA, Threat Intelligence) para tener una visión global, predecir amenazas y enfrentar mejor los riesgos. Todo esto, sin perder de vista lo importante que es concienciar a los empleados para que no sigan siendo el eslabón más débil.

En W4C Spain tenemos un compromiso para enfrentar estos retos que nos plantea el día a día digital en la línea de:

El 90 % de los puestos de trabajo requieren capacidades digitales básicas. Las mujeres solo representan el 17 % de las personas que estudian o trabajan en TI en la Unión Europea

▪ 1.-Contribuir con acciones de formación y concienciación a crear una cultura digital y de ciberseguridad en la sociedad y en las empresas:

Favoreciendo la alfabetización digital promoviendo talleres, cursos, ponencias y todo tipo de actividades que ayuden a las personas no sólo a tener competencias digitales básicas para encontrar y consumir contenidos, también a cultivar lo más importante que es tener criterio para evaluar y analizar esta información. Donde adquirir competencias digitales también signifique crear conciencia de los riesgos a los que nos exponemos y lo alerta que

Enlaces de interés...

- Women4Cyber Spain
- 'Hay una voluntad real de que haya más diversidad' (Eduvigis Ortiz)
- Women4Cyber Spain en el Día Internacional de la mujer

La pandemia que estamos viviendo ha acelerado aún más la adopción de la vida digital en todos los aspectos profesionales y personales.

debemos estar en la vida digital. De esta forma promover el uso responsable de la tecnología siendo conscientes del alcance que tienen nuestras acciones al almacenar e intercambiar todo tipo de datos en nuestras vidas digitales a nivel profesional y personal.

▪ 2.- Visibilizar el talento femenino que existe actualmente en el sector y que sean referentes para las nuevas generaciones y las personas que quieren reciclar su vida profesional.

Dada la rápida transformación y digitalización de la economía y el mercado laboral, actualmente el 90 % de los puestos de trabajo requieren capacidades digitales básicas. Las mujeres solo representan el 17 % de las personas que estudian o trabajan en el campo de las tecnologías de la información en la Unión Europea y solo el 36 % de los graduados en carreras relacionadas con la tecnología, a pesar de que las jóvenes obtienen mejores resultados que los chicos en las competencias digitales. (1)

Otros estudios indican que la tendencia no va a mejor en los últimos años y que una de las causas principales es que las jóvenes no se ven reflejadas y no ven mujeres siendo exitosas en estos sectores. W4C trabaja cada día para cambiar esta tendencia y mostrar todo el talento femenino que existe y la transversalidad de la ciberseguridad en particular y la tecnología en general. Trabajar con los medios de comunicación para que apoyen en cambiar esta percepción es básico para lograr que la tecnología y la ciberseguridad se vean como opciones interesantes y llenas de oportunidades para cualquier persona que sea curiosa y tenga ganas de tener una carrera en el sector.

Cuando la tecnología es creada y usada por equipos que reflejan el mundo en el que vivimos, nos acercamos más al mundo que aspiramos tener: más diverso, más inclusivo y más justo.

(1) Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025 COMISIÓN EUROPEA Bruselas, 5.3.2020 COM (2020) 152 final

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos it User

Almacenamiento it

Con la colaboración de: FUJIFILM Value from Innovation Western Digital.

TRIBUNA TECNOLOGÍA Y NEGOCIO

SOCIO DIRECTOR GENERAL DE ADVICE STRATEGIC CONSULTANTS

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.

La realidad del mito del monopolio de las Big Tech

¿Las compañías Big Tech compiten o dominan el mercado repartiéndoselo? Tanto en EEUU como en China se da una conjunción de factores que permitiría cualquier opinión. Otra cosa son los datos y su interpretación.

Por ejemplo, Scott Galloway en “The Four” y Tepper Hearn en “The Myth of Capitalism” defienden que Apple, Alphabet (Google, YouTube), Facebook, Amazon y Microsoft dominan el mercado norteamericano de Tecnologías de la Información y Digitalización. En China, de manera parecida, Kai-Fu Lee en “AI Superpowers” y Edward Tse en “China’s disruptors”, sostienen que Alibaba Group (Ant es el holding) y Tencent (WeChat, WeChat Pay…) dominan el mercado y se lo reparten.

Las autoridades, el legislador, el regulador, tanto en EEUU como en China, parecen estar de acuerdo con estos autores. China acaba de abrir expedientes “para el análisis de la competencia” a Tencent y a Ant (Alibaba), por entender que son un duopolio que, por un lado, compiten y, por otro, colaboran con la única finalidad de impedir la entrada de nuevos jugadores en el mercado y, por tanto, “fijar los precios”, habitualmente más elevados cuando hay poca competencia real.

Apple, Google, Facebook y Amazon tienen un problema similar a la de sus homólogos/competidores chinos. No se sabe si peor o mejor. En China no hay democracia y, lo que decida el partido será lo que digan tribunales y otras autoridades. Hemos visto cómo el Estado/Partido/Gobierno/

Competencia chinos han parado en seco la OPV o salida a bolsa de Ant (que hubiera sido la más grande en volumen en un lustro, con una valoración de mercado de 32.000 millones de dólares). ¿Por qué se paró esa salida a bolsa de una empresa que, al final y al cabo, depende del estado chino? Hoy ya lo sabemos, y por fuentes oficiales chinas: el nuevo culto a la personalidad (concepto acuñado primero por el comunismo soviético entre 1924 y 1953 en torno a la figura de Stalin y seguido por Mao Zedong en China entre 1949 y 1978) del actual premier chino, Xi Jinping, hacía incompatible el protagonismo de un empresario chino de éxito con estudios en Estados Unidos (Jack Ma) y la figura del presidente, secretario general y jefe de las fuerzas armadas chinas, que quiere el protagonismo para él. Durante un mes, Jack Ma estuvo desaparecido y, cuando se le ha vuelto a ver, su aspecto físico es el mismo de siempre, pero su carácter es más tímido y retraído; prudente.

Estados Unidos es una democracia desde 1783. El poder ejecutivo y el legislativo están en manos del partido demócrata, que se encuentra en un dilema difícil de resolver: “Big Tech” es el sector que más ha contribuido económicamente a la victoria electoral de los demócratas. Y no solo las empresas, sino sus empleados, que, en 2020, crearon un PAC (Political Action Comittee) con 3,5 millones de miembros, que recaudaron (mucho) dinero para financiar la campaña demócrata, en las elecciones del pasado 3 de noviembre. Y no olvidemos que, en 2016, cuando se enfrentaron Donald Trump y Hillary Clinton por la presidencia, 150 líderes empresariales de las compañías tecnológicas más importantes, apoyaron públicamente por carta a Hillary Clinton. Allí estaban demócratas como Tim Cook (Apple) y Jeff Bezos (Amazon), pero también, dos mujeres muy destacadas del sector TIC norteamericano que tienen mucho en común: Carly Fiorina y Meg Whitman: ambas, republicanas; ambas presidentas y CEO de la antigua Hewlett-Packard (hoy HP y HPE); las dos, candidatas conservadoras al poder legislativo de California (ambas perdieron); las dos, con larga trayectoria en el sector TIC: Fiorina en Lucent-Technologies y HP; y Whitman en Ebay y, tras su paso por HP, en Quibi.

Tres directivos TIC de máximo nivel se mantuvieron al margen del debate político en 2016 y 2020: Larry Ellison (Oracle), Peter Thiel (Paypal, Palantir) y Elon Musk (Tesla, SpaceX). En 2020, Tim Cook y Jeff Bezos no apoyaron a nadie, porque ambos, tras borrascosas relaciones con Donald Trump, acabaron haciéndose amigos y consejeros del expresidente.

Hace 4 décadas, Washington estaba lleno de lobistas de los sectores farmacéutico, tabaquero, aerolíneas, automóvil…; "estos" son hoy nada y menos que nada, comparados con lo que se gastan en lobby las empresas tecnológicas en Washington. 3.500 abogados-lobistas trabajan para estas empresas. Es un factor que tener en cuenta a efectos de lo sucedido en octubre de 2020, cuando los líderes de las empresas TIC comparecieron ante Cámara de Representantes, Senado, FTC (Federal Trade Commission) y demás autoridades que velan por la libre competencia.

Mark Zuckerberg (Facebook), Sundar Pichai (Alphabet-Google), Satya Nadela (Microsoft), Tim Cook (Apple), Jeff Bezos (Amazon) y Jack Dorsey (Twitter) comparecieron durante días ante los organismos oficiales para defenderse de acusaciones tales como: abuso de posición dominante; impedir la libre competencia, vetando la entrada al mercado de pequeños y nuevos jugadores; violación de la privacidad de sus clientes, utilizando sus datos para hacer campañas de marketing y ofertas personalizadas; participación ilegal en las elecciones presidenciales de 2016 (Facebook, el escándalo de Cambridge Analytica) y competencia desleal con los medios de comunicación, entre otras muchas acusaciones. La última, la de la competencia desleal hacia los medios está de moda en todo el mundo: Francia le ha impuesto a Google ya varias sanciones billonarias, porque no paga a los editores franceses sus derechos de autor; Facebook, en Australia ha tenido el mismo problema, al que respondió con la suspensión de su servicio de noticias, movimiento que imitó Google. En cambio, Microsoft se posicionó de parte de los medios de comunicación -dijo Google- para promocionar su buscador, Bing.

Son solo algunos ejemplos. Que Amazon es líder en comercio electrónico, en e-commerce retail…, de todos es sabido. De hecho, tras liderar el comercio digital, ha saltado al retail físico, abriendo tiendas de casi todo lo que se puede vender: muebles, libros o alimentación fresca. Pero hay ámbitos

donde los liderazgos dominantes dan miedo a la competencia y a los reguladores. Por ejemplo, en cloud computing y en Inteligencia Artificial, hay pocos jugadores dominantes: en cloud, Amazon, con Amazon Web Services (AWS), Google Cloud y Microsoft Azure. Competir con ellos es muy duro y difícil. Que se lo digan a IBM, a pesar de haber comprado Red Hat para precisamente esto: competir en cloud con los tres grandes. El resultado, aún, deja mucho que desear para IBM.

Otro campo es la publicidad online, para Facebook 95% de sus ingresos y para Google 85% de su facturación. Teniendo en cuenta el volumen de negocio de estas empresas, es fácilmente deducible que al resto de jugadores les quedan las migajas de la publicidad, incluidos los medios de comunicación. La inteligencia artificial la dominan Apple (Siri), Amazon (Alexa), Microsoft (Cortana), Salesforce (Einstein) e IBM (Watson). El resto de jugadores, como diría un es director de la CIA “son meros turistas”.

Hay ámbitos donde los liderazgos dominantes dan miedo a la competencia y a los reguladores, como, por ejemplo, en cloud computing y en Inteligencia Artificial, donde hay pocos jugadores dominantes

¿Y qué decir de la televisión en streaming? Jugadores hay muchos, pero solo tres se llevan la parte del león en número de suscriptores: por este orden, Netflix, Amazon Prime Video y Disney+. Detrás, están AppleTV+, HBO, Peacock y muchos más, casi irrelevantes. En algunos países hay empresas que actúan como agregadores de contenidos: es el caso de Movistar+ en España, que además de contenidos de otras plataformas digitales y los suyos propios, “aloja” a otras plataformas, como Netflix y Disney+.

A todas estas empresas les interesa, además, colaborar de manera que no parece intencionada, pero que es causal o correlativa: la demanda de iPhones de Apple, también está motivada por el deseo de los consumidores de utilizar el “search engine” de Google y su correo electrónico, Gmail, por no hablar de las redes sociales (Facebook, Twitter, Twitch, Tik Tok, Instagram…), por no hablar de los servicios de mensajería instantánea. Cuando Amazon provee de servicios baratos de cloud computing, esto se traduce en una mayor venta de aplicaciones de Apple’s App Store. Amazon es el principal

anunciante de Google. Y Microsoft vende licencias de Android para su teléfono inteligente Surface Duo.

La realidad es que no hay una respuesta nítidamente clara a si las empresas tecnológicas compiten sólo, colaboran sólo o hacen ambas cosas, sólo. Si continuásemos con más ejemplos, como los de más arriba, llegaríamos a la conclusión de que hacen las tres cosas en abundancia. Y, ni legislador, ni regulador, ni autoridad de la competencia van a poder solucionar el problema, porque es extremadamente complejo. Si no lo hizo en épocas más fáciles, menos aún ahora.

Me estoy refiriendo a la ley antimonopolio Sherman de 1890, que hizo el legislador americano tras la segunda revolución industrial y la llamada "Guilded Age" del capitalismo norteamericano, cuando monopolios, duopolios y oligopolios eran lo habitual, fuera en el petróleo o en la fabricación de automóviles. Esa ley, que sigue vigente, no pudo romper a IBM en 1983, cuando dominaba la computación, ni a Microsoft entre los años 1992 y 2002, cuando la compañía de Bill Gates tenía absoluto dominio de los sistemas operativos (Windows) y, el motivo para "romperla" fue que al considerar Microsoft que su browser, Explorer, era una característica más del sistema operativo Windows y, por tanto, no se podía separar, la conclusión es que Explorer acababa embebido en todos los ordenadores de HP, Lenovo, Acer, Dell… y los competidores de Explorer, como Netscape y Altavista, acabaron por desaparecer con un "sayonara, baby" (=en japonés, "hasta luego, Lucas").

De los 189 procesos legales antimonopolio abiertos en EEUU entre 1890 y 2020, utilizando la Ley Sherman, solo uno salió adelante en el sector de las Tecnologías de la Información. Se trató de AT&T, dividida por jueces y legisladores en las llamadas "Baby Bells", siete compañías que cubrían un territorio geográfico. ¿Por qué salió adelante aquel proceso antitrust? Porque AT&T fue un monopolio estatal y en la época de Ronald Reagan aquello era anatema.

En estadística hay una norma no escrita que siempre se cumple: "el porcentaje mayor gana al porcentaje menor". Dado el historial de éxito de los procesos antimonopolio contra empresas tecnológicas (un caso positivo, AT&T, versus 188 que quedaron en nada), no es descabellado pensar que, al menos en Estados Unidos, el statu quo de las empresas tecnológicas se quede como está.

Enlaces de interés…

- The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google
- The Myth of Capitalism: Monopolies and the Death of Competition
- AI Superpowers: China, Silicon Valley, and the New World Order
- China's Disruptors

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos itUser

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother