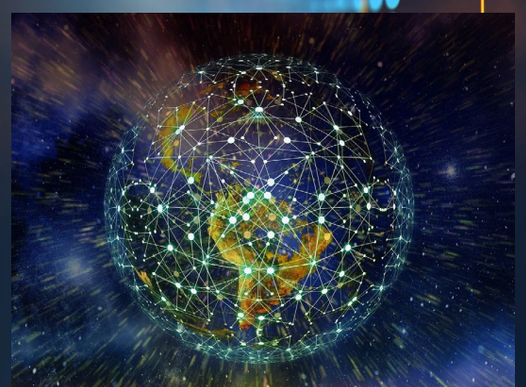
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Septiembre 2021 - nº 44

El vertiginoso crecimiento del negocio ciber

‘Las tecnologías ayudan, pero no son la clave’ (Luis Ballesteros, WiZink)



Sangfor, la empresa china de innovación que quiere atraer a la pyme española

Lecciones aprendidas para la transformación del puesto de trabajo

Microsegmentación, clave para la seguridad empresarial

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

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

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

El vertiginoso crecimiento del mercado ciber

La pandemia no sólo nos cambió la vida, sino que disparó los ciberataques, cambiando el panorama de ciberamenazas. El ransomware es el líder indiscutible en la falta de sueño de los responsables de seguridad, seguido de cerca por los ataques a la cadena de suministro. La ciberseguridad está de moda, y no solo entre los ciberdelincuentes. Durante los primeros seis meses del año las inversiones en este mercado aumentaron hasta acumular 51.000 millones de dólares en 593 transacciones, cifras que han superado las de todo 2020.

Además, este número de IT Digital Security incluye la entrevista a Luis Ballesteros, CISO de WiZink Bank, para quien las capacidades de liderazgo y de comunicación, tanto con la alta dirección como con proveedores, partners y colegas, son algunas de las habilidades que debe tener un buen responsable de ciberseguridad. También hablamos con José Luis Paramio, CISO de Userlytics, quien tiene claro que no puede vivir sin un gestor de vulnerabilidades y que si los clientes no son exigentes, las empresas no van a invertir en seguridad.

Os resumimos un Encuentro ITDS centrado en el puesto de trabajo y patrocinado por Citrix y Ozono Tech en el que participaron un total de siete responsables de ciberseguridad con los que analizamos los retos a los que se enfrentan y qué medidas se adoptarán para una siguiente fase en la que predominará un modelo de trabajo flexible.

Hace unas semanas pedíamos a nuestros lectores que respondieran a una breve encuesta sobre microsegmentación. Los resultados y están disponibles y, aunque no arrojan demasiadas sorpresas, dejan claro que esta tecnología es clave para mejorar la seguridad empresarial.

La actualidad llega marcada por la llegada al mercado español de Sangfor, una empresa china de soluciones de infraestructura de TI, especializado en computación en la nube y seguridad de redes con una amplia gama de productos; Overa Activity, una solución que analiza el puesto de trabajo para saber, entre otras muchas cosas, cuáles son las aplicaciones más utilizadas y las menos productivas, así como disponer de métricas de uso y rendimiento de dispositivos; por último resumimos los resultados de un estudio que desacredita algunos mitos comunes en torno a la seguridad móvil.

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

itds

Sumario

Actualidad

Entrevistas

Encuentros ITDS

No solo IT

Índice de anunciantes

Revistas Digitales

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
RESPUESTA	**DETECCIÓN**

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Sangfor, la empresa china de innovación que quiere atraer a la pyme española

Sangfor es una empresa de origen chino, con 20 años de historia y casi ocho mil empleados; cotiza en la Bolsa de Hong Kong, genera más de un millón de dólares de facturación anuales y tiene presencia en 60 países. Hace dos años y medio la compañía fijó su atención en Europa abriendo oficinas en Italia, donde ya se trabajan con más de 450 clientes, y más recientemente en España.

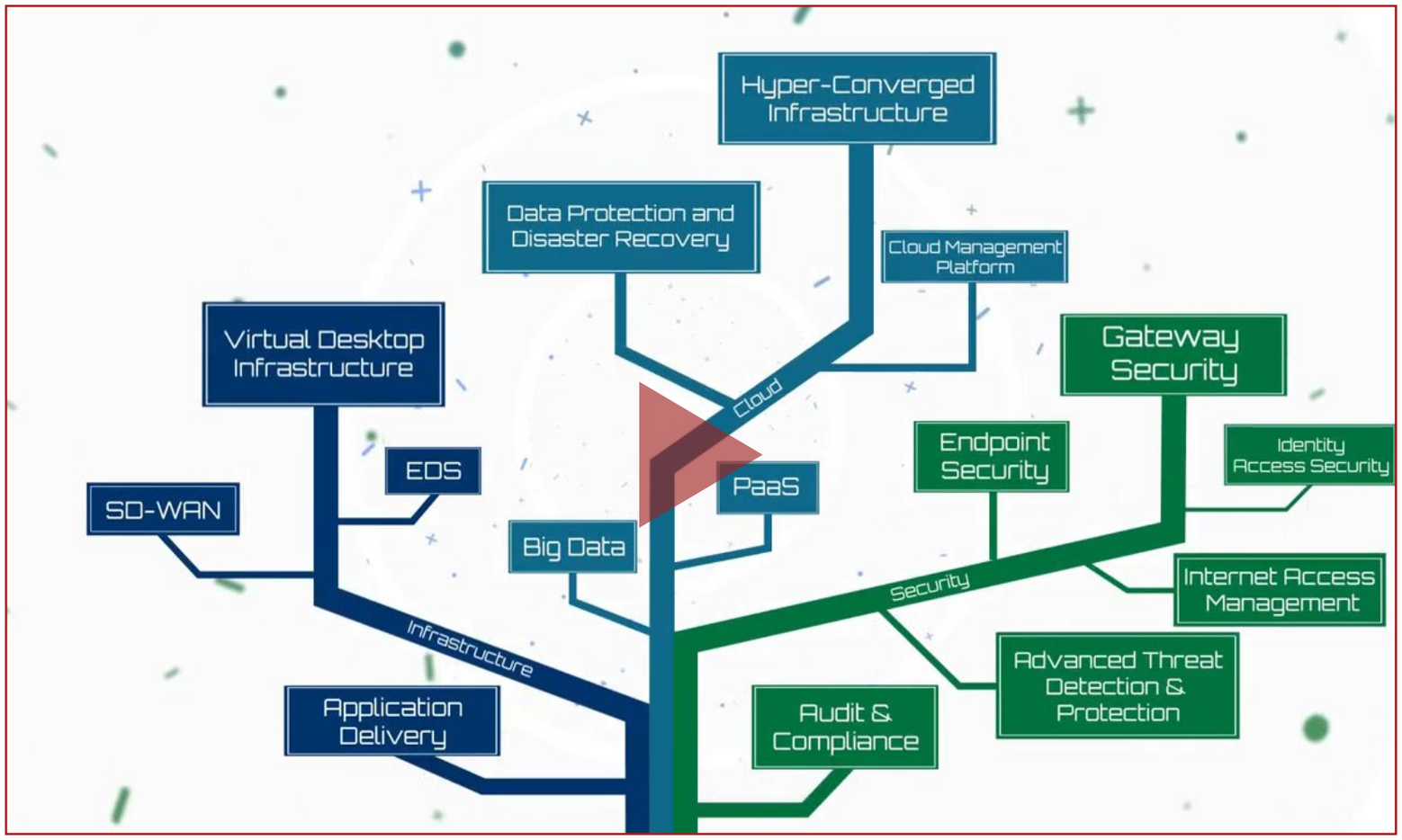
José Ramón Crespo y Alberto Carrillo, country manager y responsable preventa respectivamente, son los encargados de expandir la propuesta tecnológica de la compañía, un proveedor de soluciones de infraestructura de TI, especializado en computación en la nube y seguridad de redes con una amplia gama de productos que incluyen: infraestructura hiperconvergente, infraestructura de escritorio virtual, firewall de próxima generación, administración de acceso a Internet, optimización WAN, SD-WAN y muchos otros.

"Tanto Alberto como yo estamos encantados con las capacidades tecnológicas de la compañía", asegura José Ramón Crespo, quien suma experiencia en canal de distribución (Towers IT e Ingeam Micro) así como en Ivanti, y con gran conocimiento de las tecnologías de virtualización, monitorización, ciberseguridad y BackUp. Capacidades que se unen a las de Alberto Carrillo, quien tras su paso por Ermestekl, Econocom y, más recientemente Nutanix, le habilitan para hablar de hiperconvergencia y las últimas tendencias del mercado.

Asegura Crespo durante una reunión online, en la que la primera pregunta está dirigida a saber a qué se dedica Sangfor exactamente, que la propuesta permite competir con grandes nombres y aprovecha su capacidad para llegar a mercados más pequeños. Se menciona a VMware en virtualización o a Citrix en VDI y se asegura que "en hiperconvergencia somos un vSAN [VMware] barato y con capacidades muy superiores as a Nutanix en muchos aspectos", puntualizando que las propuestas tienen que tener en cuenta las necesidades reales de los clientes y que la oferta de hiperconvergencia, muy

"Tenemos un hándicap importante, y es que somos de origen chino"

José Ramón Crespo, Country Manager Spain & Portugal, Sangfor Technologies



¿QUIÉN ES SANGFOR? **CLICAR PARA VER EL VÍDEO**

Sangfor es un proveedor de soluciones de infraestructura de TI, especializado en computación en la nube y seguridad de redes con una amplia gama de productos

valoradas en el mercado entry-level “es bastante más sencillo que el de otras muchas ofertas del mercado”.

Uno de los productos de la compañía machea casi en el 100% el offering de VMware, desde la parte de hipervisor más sencilla hasta los productos más avanzados, lo que, en opinión de Alberto Carillo, permite a Sangfor entrar en un sector dominado por la presencia de VMware pero con una propuesta que se acerca más a las empresas de menor tamaño

“Sangfor es una empresa de innovación e infraestructura con más de 1.500 patentes”, responde José Ramón Crespo cuando le preguntamos a qué se dedica Sangfor. En la parte de ciberseguridad la compañía se centra en la seguridad perimetral, el endpoint y el SD-WAN. Respecto a esto último asegura Alberto Carrillo que tiene Sangfor un mensaje “muy potente” y una amplia oferta que permite dar cobertura tanto a oficinas con más de 2.000 personas u oficinas muy pequeñas.

Reivindica Alberto Carillo la responsabilidad de los fabricantes con las empresas pequeñas que de verdad no se pueden permitir tener herramientas de seguridad “y que lo que hacen al final es alimentar a los ciberdelincuentes, capaces después de realizar ataques más avanzados contra los objetivos que son pymes”.

El mercado es muchísimo más grande en la parte de infraestructura porque la competición es menor, el presupuesto que el cliente está dispuesto a pagar es más elevado, y los márgenes son más altos, asegura Alberto Carrillo.

En opinión de José Ramón Crespo, “no podemos evitar que nos ataquen, pero sí minimizar

"Sangfor tiene un mensaje muy potente y una amplia oferta que permite dar cobertura tanto a oficinas con más de 2.000 personas u oficinas muy pequeñas"

Alberto Carrillo, SE Manager Iberia, Sangfor Technologies

los daños", lo que lleva a Sangfor no sólo a ofrecer herramientas que son capaces de detectar y detener un incidente lo antes posible, sino a contar con una solución de Backup, "de forma que en la misma consola vamos a tener ese firewall perimetral, esa protección antimalware y antiramsonware, y una solución de backup que nos permite recuperarnos del daño que nos pueden hacer".

"Tenemos un hándicap importante, y es que somos de origen chino", reconoce José Ramón Crespo cuando le preguntamos por las previsiones de la compañía. Se añade la poca presencia que Sangfor tiene en Europa, que además de Italia y España se encuentra abriendo oficinas en Francia y Alemenia, y que planea abrir un CPD en la región.

En el mercado pyme, más sensible al precio, "podemos hacer muchas cosas", así como en las empresas de origen asiático con presencia en nuestro país.

Por otra parte, asegura el directivo de Sangfor sentirse "muy sorprendido" por la reacción que la compañía está teniendo en los países latinoamericanos, de donde cada día recibe peticiones de información "porque prefieren hablar con España que con China y porque en muchos países prefieren tecnología china a americana".

Volviendo a las previsiones, explica José Ramón Crespo que lo importante "no es tanto la facturación como hacer ruido y empezar a tener una base de clientes, como está pasando en Italia", donde ya cuentan con logos conocidos como la Universidad de Calabria y están teniendo mucha entrada en administración pública local y ayuntamientos, "donde también son muy sensibles al precio".

Al respecto la compañía lanzaba hace unas semanas la promoción 'Working from home'. Vigente hasta el 31 de octubre la promoción ofrece una experiencia de trabajo en remoto segura totalmente gratis para las compañías con menos recursos. Concretamente la promoción pone a disposición de los clientes su versión del Firewall de aplicaciones de próxima generación (NGAF) con un límite de hasta mil usuarios. Las empresas que lo necesiten podrán adquirir esta solución sin ningún tipo de coste, incluyendo el perimetral, las licencias de los Endpoint Secure y de los VPN y SSL, que facilitarán el acceso a la oficina con SSL sin puertos adicionales.

La promoción explota una actualización de producto realizada por la compañía que afectó tanto a la gama virtual de su hipervisor como a la gama de appliances físicos y, sobre todo,

a la de appliances virtuales cuya beta se liberó a finales de julio. Explica Alberto Carrillo que “poner un firewall perimetral con protección de ransomware” no es algo que se haga a nivel Enterprise, pero sí a nivel pequeña empresa donde además se producen un número elevado de ataques.

También se ve impulsada la propuesta Working from Home por el hecho de que la vuelta a las oficinas parece estar retrasándose y que son muchas las empresas que tienen que hacer frente a un modelo híbrido para el que no están preparadas.

Respecto al canal de distribución se opta por Esprinet como el mayorista que lleve al mercado el offering de Sangfor, siendo V-Valley quien se encargará de la parte de seguridad. Se trabaja también en “algún tipo de acuerdo, o bundleización con algún potro mayorista de hardware específico”, que trabajarán con Esprinet y V-Valley para llevar al mercado alguna solución conjunta.

Enlaces de interés...

- Sangfor
- El ransomware sigue su escalada: cómo actuar si eres una pyme
- El Clúster de Ciberseguridad de Madrid presenta el proyecto Pyme 3DSecure

Compartir en RRSS

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com

Overa Activity:
análisis inteligente del puesto de trabajo donde quiera que esté

Ozona Tech, una compañía española de origen gallego con casi 20 años de experiencia en el mercado en el área de la consultoría y la integración tecnológica, es una gran experta en el mercado del Digital Workplace y responsable de Overa Activity, un producto concebido como una plataforma de análisis inteligente del puesto de trabajo que permite conocer al detalle todo lo que sucede con los dispositivos y usuarios durante el trabajo en remoto, lo que ayuda a conocer usos, prácticas de riesgo, e incluso necesidades de formación.

El trabajo en remoto no es nuevo. Hace tiempo que los portátiles, tablets y smartphones han creado una fuerza de trabajo móvil que, si bien solo unos pocos podían disfrutar inicialmente se ha ido generalizando. La pandemia aceleró el proceso y nos encontramos ahora discutiendo no sólo cuando volveremos a las oficinas, sino quiénes y cuántos.

Uno de los retos que ha planteado el teletrabajo ha sido que se pudiera acceder a las herramientas corporativas con la misma experiencia de usuario, y las mismas capacidades y beneficios se estuviera donde se estuviera. Una vez superado surge uno nuevo. Nos lo cuenta Ramón Ares, director general de Ozona Tech, quien explica que lo que ahora se quieres es tener la misma capacidad de gestión y la misma capacidad de conocimiento del trabajo y actividad de empleado remoto que la que se tienen con los empleados a los que se puede ver porque están en la oficina.

Esta inquietud y un caso concreto de un cliente que tenía una importante fuerza de trabajo deslocalizada en Asia llevó hace cinco años a Ozona Tech a desarrollar una herramienta que permitía conocer lo que estaba pasando con aquellos empleados; esa herramienta, que monitoriza dispositivos, aplicaciones y la infraestructura que los soporta, ha pasado de ser “una herramienta que usábamos en nuestros clientes como un valor añadido de nuestros servicios como empresa de integración” a un

producto comercial bautizado como Overa Activity, que sigue evolucionando.

Tipología de cliente

"Hay muchos elementos de Overa Activity que ayudan a los clientes que se acercan a conocer la herramienta a decidirse por ella, independientemente del tamaño o de la actividad", explica Ramón Ares cuando le preguntamos por la tipología de cliente a la que va dirigida la solución.

A algunos les interesa más la capacidad de la solución de realizar una gestión integral del teletrabajo pudiendo saber "qué hacen mis trabajadores, cómo pueden mejorar su experiencia de usuario, etcétera", pero también es una herramienta de monitorización IT con la que gestionar el parque de dispositivos y optimizar el uso del software; desde la perspectiva del Departamento de Recursos Humanos, Overa Activity ayuda en la creación de entornos de trabajo en equipo para usuarios deslocalizado o permite gestionar la salud digital de los empleados. En definitiva, "hay una variedad tan grande de motivos y beneficios, que los clientes descubren que Overa Activity les proporciona nuevas vías de mejora que no habían considerado", asegura el director general de Ozona Tech.

Planteamos a Ramón Ares si los empleados no se sienten vigilados por una solución como Overa Activity, que monitoriza desde el tiempo de conexión a las herramientas utilizadas o los ficheros sobre los que se trabaja. Responde que no, y asegura que la clave está en el Panel del Empleado,

> Overa Activity permite, entre otras muchas cosas, saber cuáles son las aplicaciones más utilizadas y las menos productivas, así como disponer de métricas de uso y rendimiento de dispositivos

que garantiza al mismo ser el primero que conoce la información. Asegura además que "las empresas que tenemos como clientes no buscan conocer al detalle información de una persona, sino cómo se utiliza la informática de todos los empleados".

Planteamos también que, ya que la herramienta es capaz de saber los archivos con los que trabajan los empleados, pudiera alertar sobre, por ejemplo, una fuga de información. Responde el directivo que "la tecnología nos permite llegar profundamente a donde queremos" y que su finalidad es monitorizar dispositivos, aplicaciones e infraestructura para recopilar datos y estadísticas de uso.

Beneficios de Overa Activity

Francisco González Hermida, director de Innovación y uno de los desarrolladores de la plataforma, es el encargado de contarnos las ventajas, beneficios y casos de uso de Overa Activity.

Menciona entre otros la posibilidad de visualizar patrones de conectividad, incluso cargas o picos de actividad en las propias infraestructuras analíticas de rendimiento. Asegura también que muchos clientes han solicitado plantillas que permiten realizar un estudio del comportamiento de determinados procesos en distintos modelos de máquinas. La solución permite además crear “un diagrama temporal de explotación de los propios dispositivos; un control en tiempo real de todos los endpoints conectados a nuestras infraestructuras corporativas; un control en la propia ejecución de los procesos y la vigilancia de los consumos de esos procesos”.

Habla Francisco González de unos módulos que revisan el software que está instalado en las máquinas, y comprueban si los sistemas operativos están actualizados o no, lo que permite “enviar una alarma a sistemas indicando que hay determinados dispositivos que no tienen los hotfixes necesarios para el cumplimiento de la seguridad”, y que también se puede hacer un alarmado de aplicaciones clasificadas como potencialmente peligrosas.

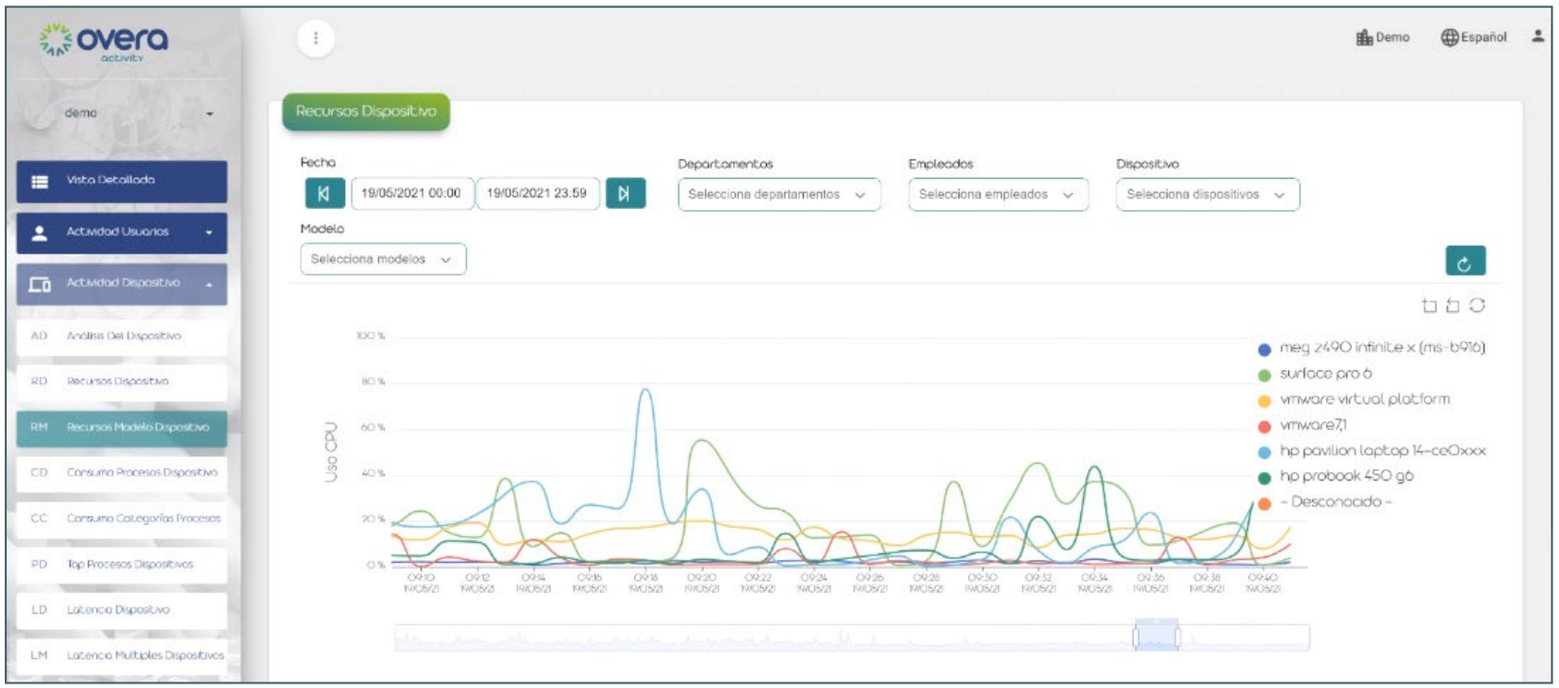
Desde la perspectiva de recursos humanos, otra característica muy interesante de Overa Activity es la catalogación de las páginas web visitadas. Esta información, junto con otra relacionada con la productividad del usuario, llega a la empresa en forma de indicadores de cómputo y se cifra de dos maneras: reversible o irreversible dependiendo de si la empresa quiere hacer una auditoría de seguridad o no. Explica González Hermida que son detalles que se analizan con los distintos departamentos de la empresa para realizar una implantación de la solución u otra distinta.

"El modelo de negocio es suscripción por usuario independientemente de los dispositivos que tenga"

Ramón Ares, director general, Ozona Tech

Muy interesante es la capacidad de la solución para realizar la comparación del consumo medio de los distintos procesos del sistema operativo para detectar cuándo un proceso puede estar suplantado, de forma que en un momento dado se podría identificar un posible proceso de minería de datos, por ejemplo.

Las opciones que ofrece Overa Activity no son sólo las mencionadas. El departamento de desarrollo no ha dejado de añadir opciones a la solución,



Como fuente de información para herramientas SIEM o EDR explica Francisco González que Overa Activity “dispone de una gran cantidad de mecanismos de integración”. Una de las ventajas “es que está construido con arquitectura basada en micro servicios y con las tecnologías más recientes del mercado, lo que significa que cualquier integración se puede realizar de una manera muy sencilla”. Añade el director de innovación de Ozona Tech que, de base, la solución ofrece “una serie de APIs personalizadas basadas en diferentes mecanismos de autenticación y de autorización, lo que nos garantiza poder hacer integraciones bidireccionales con cualquier tipo de herramienta”.

en ocasiones a partir de las peticiones de los propios clientes, con el objetivo de “facilitar una serie de técnicas y una serie de conceptos para que sistemas tenga el control de lo que está pasando en sus infraestructuras”.

Por cierto que en el corazón de Overa Activity coexisten dos algoritmos de inteligencia artificial basados en machine learning, que examinan la experiencia de usuario en determinadas competencias, lo que “nos permite identificar si en un determinado proceso el usuario está interactuando de una manera incorrecta”

Overa Activity se nutre de agentes colocados en endpoints basados, por el momento, en Windows, Linux y Android. iOS estará disponible en los próximos meses. En cuanto al famoso BYOD (Bring Yoour Own Devices), se establecen medidas para que sólo se extraiga información cuando la actividad realizada en el dispositivo esté relacionada con el trabajo.

"Overa Activity está construido con arquitectura basada en micro servicios y las tecnologías más recientes del mercado"

Francisco González Hermida, director de Innovación, Ozona Tech

Overa Activity ayuda a conocer usos, prácticas de riesgo, incluso necesidades de formación de los empleados

Y no solo esto, porque Overa Activity también posee un bus de eventos interno, “lo que significa que podemos ofrecer reactividad en tiempo real”, así como un sistema incorporado de automatización de workflow integrado “que nos permite una serie de automatizaciones de tareas diarias.

Oportunidad y modelo de negocio

“El modelo de negocio es suscripción por usuario independientemente de los dispositivos que tenga”, explica Ramón Ares. Llegados a este punto, habría que plantearse su Overa Activity es más una solución que mejora la productividad o una solución que mejora la seguridad, y cómo quiere promocionarla Ozono Tech.

Sin duda la oportunidad está en la productividad, y si bien aporta muchas opciones a la hora de mejorar la seguridad de las empresas, “no tenemos la ambición de convertirnos en una herramienta del segmento de la seguridad”, asegura el directivo.

Enlaces de interés...

- Cinco imprescindibles para crear un entorno seguro para los datos en cloud

Incide Ramón Ares en que el enfoque de Overa Activity es la productividad, así como la gestión de todo lo que está alrededor del mundo del teletrabajo. Añade que como expertos en implantación del Digital Workplace dieron un paso más; “profundizamos en cómo se usan las herramientas que implantamos porque era necesario conocerlo para que fueran útiles, y todo se ha potenciado con la llegada de Francisco González y su equipo, que han aportado toda la capacidad de desarrollo y han integrado todo el conocimiento que había dentro de la casa en torno al puesto de trabajo para que tengamos una herramienta que es tecnológicamente muy avanzada”.

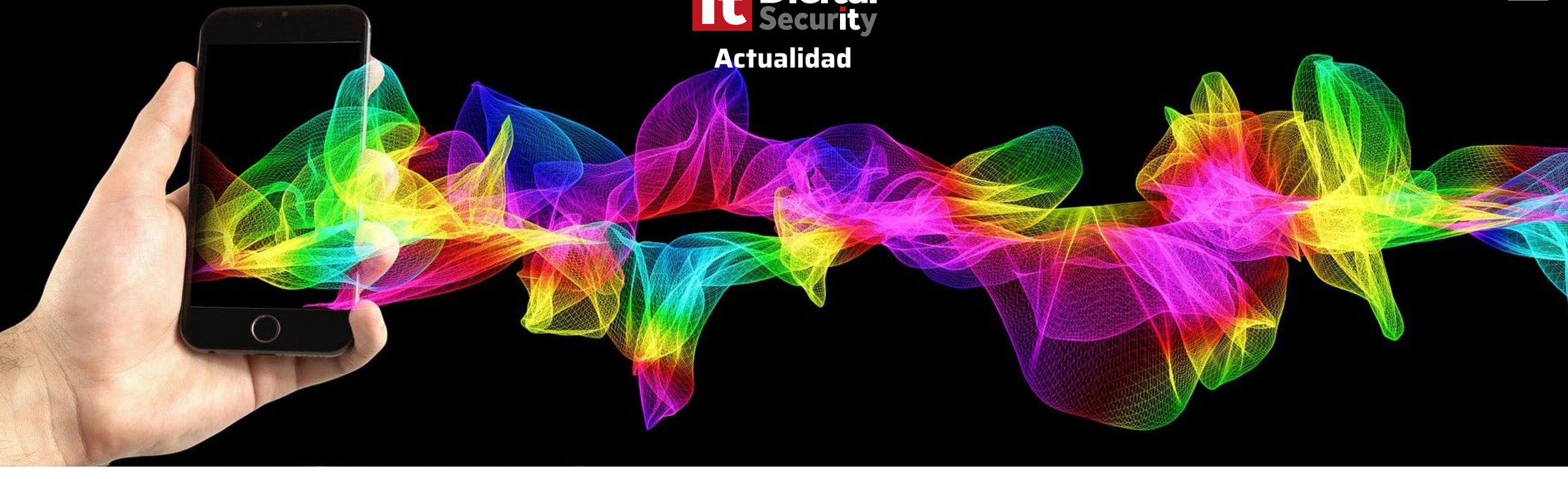
El siguiente paso es que dentro de tres o cuatro años los clientes de Overa Activity puedan comparar los datos que genera la herramienta, esos indicadores, “con los de otras empresas de su misma actividad o tamaño”, una información a agregada comparativa con otras empresas “que va a tener un gran valor”.

Compartir en RRSS

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN

ENTRUST



Los cinco mitos de la seguridad móvil que todo CISO debería conocer

Appdome, una compañía centrada en la seguridad de aplicaciones móviles sin código ni prevención de fraudes, ha publicado recientemente una encuesta global centrada en cómo los responsables de ciberseguridad pueden satisfacer las expectativas de los usuarios sobre seguridad móvil en 2021.

La encuesta proporciona información completa sobre las expectativas de seguridad, malware y defensa contra amenazas de los usuarios de dispositivos móviles en Estados Unidos, Europa, América Latina y Asia.

Los datos de la encuesta, realizada a más de 10.000 usuarios de dispositivos móviles de Estados Unidos, Europa, América Latina y Asia, no sólo ofrecen una visión poco común de la voz del consumidor, sino que desacredita algunos mitos comunes, información que los equipos de seguridad encargados de proteger a los usuarios de las aplicaciones móviles deberían tener en cuenta.

Entre otros datos, el informe recoge qué amenazas móviles temen más los consumidores, qué aplicaciones esperan que tengan el mayor nivel de seguridad o los cambios en las expectativas de los consumidores para la seguridad de las aplicaciones móviles como resultado de la COVID-19.

Los consumidores exigen la máxima seguridad en las aplicaciones móviles, incluidas las de banca

MITO 1. Los consumidores se sienten cómodos con las estrategias de seguridad “buyer beware” de las aplicaciones móviles

Realidad: los consumidores esperan que el editor proporcione un nivel muy alto de seguridad y protección de la aplicación móvil en la aplicación móvil.

- El 73% de los consumidores dejarían de usar una aplicación móvil si los dejara desprotegidos contra ataques.
- El 74% de los consumidores dejarían de usar una aplicación móvil si su aplicación fuera violada o pirateada.
- El 46% de los consumidores les diría a sus amigos que dejen de usar una aplicación si su aplicación fue violada o pirateada.

MITO 2. Los consumidores están dispuestos a renunciar a la seguridad para obtener mejores funciones en la aplicación móvil.

Realidad: la mayoría de los consumidores valoran la seguridad y la protección contra malware tanto o más que las funciones.

- El 38% de los consumidores dicen que se preocupan más por la seguridad cuando usan aplicaciones móviles.
- El 37% de los consumidores dicen que se preocupan más por las funciones de las aplicaciones móviles.
- El 25% de los consumidores se preocupa más por la seguridad y las funciones, por igual.

MITO 3. La protección contra las brechas en la red y la nube debe ser la principal prioridad.

Realidad: los consumidores se preocupan más por las amenazas en el dispositivo a nivel de la aplicación y descartan las amenazas en la nube de la red.

- El 62% de los consumidores temen que alguien piratee su aplicación, por lo que es el No. 1 amenaza de aplicación móvil.
- El 56% de los consumidores temen las amenazas de malware en su dispositivo, lo que lo convierte en la segunda amenaza de aplicaciones móviles.
- El 32% de los consumidores temen las amenazas de la red en la nube, lo que la convierte en la séptima amenaza de las aplicaciones móviles.

MITO 4. Proteger las credenciales de usuario y el inicio de sesión en el backend es suficiente para satisfacer a los consumidores.

Realidad: los consumidores clasifican las amenazas como el malware y la piratería por encima de la pérdida de credenciales por violaciones de backend.

- Más del 55% de los usuarios de Android e iOS temen que el malware robe datos de su aplicación como la principal amenaza.
- El 40% de los consumidores de todos los grupos de edad temen la falta de protección de las credenciales, lo que la convierte en la cuarta amenaza más destacada para los usuarios.

MITO 5. La seguridad de las aplicaciones móviles solo es relevante si la aplicación móvil se encuentra en una industria regulada.

Realidad: los consumidores exigen la máxima seguridad en las aplicaciones móviles, incluidas las de banca

- El 36% de los consumidores esperan que las aplicaciones de banca móvil tengan el más alto nivel de seguridad.
- El 33% de los consumidores dice que “todas las aplicaciones de transacciones” deben tener el nivel más alto de seguridad.
- El 16% de los consumidores dice que las aplicaciones de monedero electrónico / pago deberían tener el nivel más alto de seguridad.
- El 12% de los consumidores dice que las aplicaciones minoristas y de entrega de alimentos deberían tener el nivel más alto de seguridad.

Tras publicar los resultados del informe, Tom Tovar, CEO de Appdome ha destacado que la opinión del consumidor cambia el guión en el debate ‘seguridad versus características’, “dejando en claro que la seguridad de las aplicaciones móviles y la protección contra malware están a la par con otras características críticas en la experiencia de las aplicaciones móviles y son demandadas por todos los consumidores que descargan y usan un aplicación móvil”.

Enlaces de interés...

- Cómo los CISO pueden satisfacer las expectativas de los consumidores en materia de seguridad móvil en 2021
- La seguridad móvil y de los dispositivos IoT, las áreas más vulnerables de las empresas - 20 ABR 2021
- La seguridad de los pags, lo que más valora el consumidor online

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTION DE LOS RIESGOS

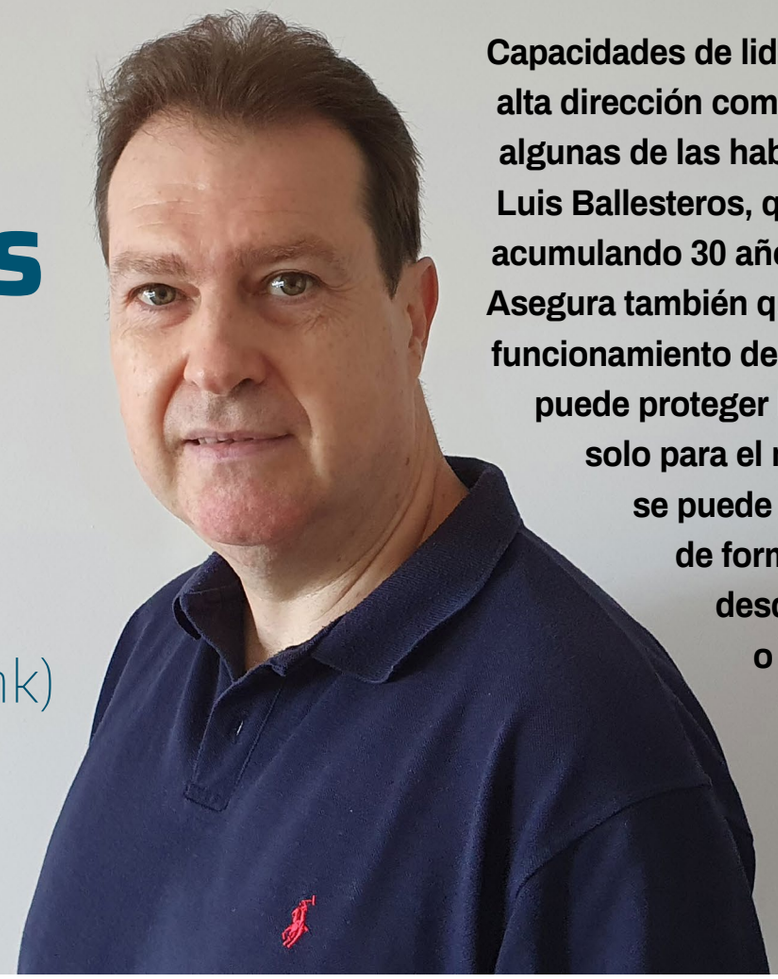
Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

‘Las tecnologías ayudan, pero no son la clave’

(Luis Ballesteros, WiZink)



Capacidades de liderazgo y de comunicación, tanto con la alta dirección como con proveedores, partners y colegas son algunas de las habilidades que debe tener un buen CISO. Lo dice Luis Ballesteros, quien protege WiZink Bank desde sus inicios, acumulando 30 años de experiencia en el mundo de la banca. Asegura también que hay que tener amplios conocimientos del funcionamiento de la empresa a la que se sirve, porque no se puede proteger lo que no se conoce; que se debe educar no solo para el mundo digital sino en ciberseguridad; que no se puede renunciar al cloud, pero que hay que adoptarlo de forma segura; que ciberdelincuentes existen desde el mismo momento en que se crea Internet o que aquellas tecnologías que hacen uso de inteligencia artificial para realizar análisis de comportamiento en la red y detectar actividades anómalas serán imprescindibles.

Rosalía Arroyo

Luis Ballesteros es el CISO de WiZink, un banco digital experto en financiación al consumo con presencia en España y Portugal. Ofrece a sus clientes un amplio abanico de soluciones de financiación digitales, así como productos de ahorro que buscan impulsar el potencial financiero de las personas de manera responsable y realista. La entidad posee también la plataforma digital de adquisición de vehículos de ocasión Lendrock, así como la plataforma de pagos y financiación flexible en tiendas online, Aplazame.

La banca es el sector al que Luis Ballesteros ha dedicado la mayor parte de su carrera profesional. A los 23 años en Citibank se suman los dedicados a Bancopopular-e y WiZink, donde ejerce como CISO desde sus inicios.

Para Ballesteros tener conocimientos en el área de tecnología y seguridad de la información es una de las cualidades que debe tener un buen CISO; “lo suyo sería tener por lo menos una certificación de reconocido prestigio para asegurar conocimientos en controles y evaluación de riesgos de ciberseguridad”, como la certificación en el CISA o el CISM; añade la necesidad de contar con experiencia en normativas aplicables, tanto regulación específica que pueda tener el sector al que cada cual se dedique, “como otras regulaciones de referencia como puede ser la NIS y estándares internacionales como puede ser la ISO 27001 de seguridad de la

"Los ciberataques están en permanente evolución y lo que tenemos claro es que no se puede parar de mejorar"

información y la ISO 22301 de continuidad de negocio". Por otra parte, "es fundamental" tener buenos conocimientos del funcionamiento y organización de la empresa a la que se tiene que proteger, cómo está organizada internamente y cómo son las prácticas habituales, "porque no se puede proteger algo que no se conoce" y porque "por muchas normas que queramos poner los de seguridad, si la gente que tiene que hacer de verdad el trabajo no está concienciada, no entiende qué tiene que hacer, las hará mal, no por mala fe sino por desconocimiento, y pondrá en riesgo a la compañía".

Junto con el conocimiento, enumera Luis Ballesteros "una serie de habilidades que probablemente no son específicas de este puesto, pero que sí son necesarias". Asegurando que "nosotros estamos para ayudar al negocio a conseguir sus objetivos sin renunciar a la seguridad" menciona el directivo que es necesario contar con una gran capacidad analítica y tener mente abierta para analizar nuevas iniciativas y soluciones, lo que, a su vez, lleva a la necesidad de "ser curioso y con ganas permanentes de aprender". Otras cualidades de un buen CISO es contar con capacidad de liderazgo y de comunicación, tanto con la alta dirección como con proveedores, partners y colegas; "es muy importante transmitir a los empleados, desde el primero hasta el último, cuál es el motivo de las políticas o controles de seguridad que ponemos. Explicarles bien no sólo lo que tienen que hacer, sino cómo tienen que hacerlo y por qué tienen que hacerlo".

Interés por la seguridad

Hablando del mayor interés que parecen estar prestando las empresas a la ciberseguridad, dice Luis Ballesteros que el mundo cibernético no deja de ser una extensión del mundo físico y que los ciberdelincuentes existen desde el mismo momento en que se crea Internet, "pero no cabe duda de que esto ha evolucionado y está evolucionando muchísimo en los últimos años, porque el propio uso de Internet y el propio uso del mundo cibernético ha evolucionado muchísimo".

Asegura el CISO de WiZink Bank que "en lo primero que se fijaron los ciberdelincuentes a la hora de intentar sacar dinero fue en los bancos, y por eso somos un sector muy maduro y que llevamos preocupados por la ciberseguridad muchos años". Que el número de ataques no deje de incrementarse ha hecho que toda la sociedad, todas las empresas, grandes y pequeñas, independientemente del sector, estén cada vez más concienciadas, lo cual no quita, en opinión de Luis Ballesteros, que todavía haya "recorrido de mejora en cuanto a que

"Para nosotros el trabajo en remoto era una estrategia de continuidad de negocio que ahora se ha convertido en una estrategia BAU (Business as Usual), que implica que esta infraestructura tenga también su alta disponibilidad y que sea resiliente"

es importante fortalecer la educación en ciberseguridad en las escuelas y que esto forme parte de del temario oficial, porque Internet ha corrido mucho, todo el mundo utiliza las redes sociales, todo el mundo utilizado tienen un móvil, y es importante que desde que somos pequeños se eduque a la gente no solo para el mundo digital sino en ciberseguridad".

La fuerte regulación a la que se ve sometido el sector bancario, con normativas específicas como la PSI-DSS, "ha sido una palanca, no sólo dentro, sino también con proveedores" para adoptar medidas de ciberseguridad, asegura el directivo de Wizink Bank, que desde hace años realiza evaluaciones de seguridad a proveedores e incluye cláusulas en sus contratos para asegurar que los proveedores gestionan bien la información; "desde el momento en que las regulaciones, empezando por GDPR, nos exigen que tenemos que tener cláusulas en los contratos, que tenemos que auditar a los proveedores, etc., se facilita muchísimo la tarea porque ya no es algo que mi empresa quiera hacer, sino que se tiene que hacer por regulación, con lo cual yo diría que hoy ha sido una palanca fenomenal".

Cloud

El cloud, o mejor dicho, las ofertas as-a-service, revolucionaron el mercado hace unos años. Esa revolución, que se aceleró en tiempos de pandemia, aún continúa y es la pieza principal de la llamada Transformación Digital. Preguntamos a Luis Ballesteros si la adopción de la nube en el sector bancario ha sido más lenta, más precavida. "Precavida sí que es, pero no podemos renunciar al cloud", asegura.

La banca está yendo al cloud porque “no puede ser de otra manera. Es una solución más que proporciona muchísimos beneficios para la empresa. En algunos casos no sólo beneficios al nivel del propio servicio, sino en muchos casos también beneficios desde el punto de vista de ciberseguridad”, asegura Luis Ballesteros, añadiendo que “no debemos engañarnos” y pensar que cuando se adopta la nube van a desaparecer los problemas.

Para el CISO de WiZink Bank el cloud no es ni más ni menos seguro, y destacada como punto importante “la parametrización y la personalización que nosotros hagamos del servicio” porque son muchos los incidentes de seguridad que se producen no tanto por culpa del proveedor de cloud sino porque se han dejado las contraseñas por defecto, o por tener un acceso directo sin doble factor de autenticación, etc.

Alrededor de la nube crecen los servicios gestionados. Considera Ballesteros que son imprescindibles y comenta que excepto dos o tres empresas muy grandes que pueden tener todo internalizado, “no tiene sentido que demos los servicios internamente”, entre otras cosas “porque no tenemos gente. Es imposible tener un equipo grande, súper especializado y mantenerlo totalmente al día. Si queremos ser eficaces y eficientes, las dos cosas, es necesario contar con equipos especializados que nos ayuden”, asegura el CISO de WiZink Bank añadiendo que las empresas siguen siendo responsables de cómo se gestionan sus datos y por tanto “es fundamental que haya un equipo de seguridad dentro de la compañía que gobierne los servicios y que haga de puente entre la compañía y los propios equipos especializados en seguridad, con los que hay que trabajar muy de cerca para transmitir cuáles son los problemas de nuestra compañía, en qué sector estamos y que todas las alertas y toda la vigilancia se personalice para el sector y la empresa que están dando servicio”.

Pandemia

¿Qué se ha aprendido de la pandemia? “Que el teletrabajo va a formar parte del modelo de trabajo de muchas empresas”, dice Luis Ballesteros. Asegura

el directivo que el trabajo en remoto, que ya existía antes de la pandemia, se utilizaba de manera puntual y no de manera masiva y simultánea, y que en el caso de WiZink Bank "la adopción fue bastante sencilla porque nosotros no teníamos puesto físico en la oficina personalizado. Todos los empleados teníamos portátil y teléfono móvil y cuando ibas a la oficina te sentabas en el sitio que vieras libre, por lo que ya todos teníamos acceso remoto y las medidas de seguridad adecuadas. Lo único que tuvimos que hacer fue reforzar esa infraestructura en cuanto a capacidad".

Respecto a las lecciones aprendidas desde el punto de vista de seguridad, "no hemos tenido nada reseñable en cuanto a que ha funcionado todo bien desde el punto de vista de seguridad desde el primer momento"; y si hablamos de continuidad de negocio "para nosotros el trabajo en remoto era una estrategia de continuidad de negocio", que ahora se ha convertido en una estrategia BAU (Business as Usual) que implica que "esta infraestructura tenga también su alta disponibilidad y que sea resiliente".

Sobre el teletrabajo, dice Luis Ballesteros que es un modelo que funciona y que tiene muchos puntos positivos, tanto para las empresas como para los empleados, aunque "no creo que sea la panacea", por lo que será habitual que las empresas busquen modelos híbridos.

Tecnologías

Le preguntamos a Luis Ballesteros por las tecnologías de ciberseguridad que toda empresa debería tener, ese mínimo del que nadie puede prescindir. Responde el CISO de WiZink que "antes que las tecnologías, te diría que lo que toda empresa debería tener es un marco de ciberseguridad. Las tecnologías ayudan, pero no son la clave. La clave es tener el marco de ciberseguridad que haga la orquestación de todas las herramientas".

"Es muy importante transmitir a los empleados, desde el primero hasta el último, cuál es el motivo de las políticas o controles de seguridad que ponemos"

Gobierno, Securización o Protección, Detección y Resiliencia son los cuatro grandes dominios del marco de ciberseguridad de WiZink Bank, cada uno de los cuales tiene varios subdominios en los que se identifican diferentes herramientas tecnológicas.

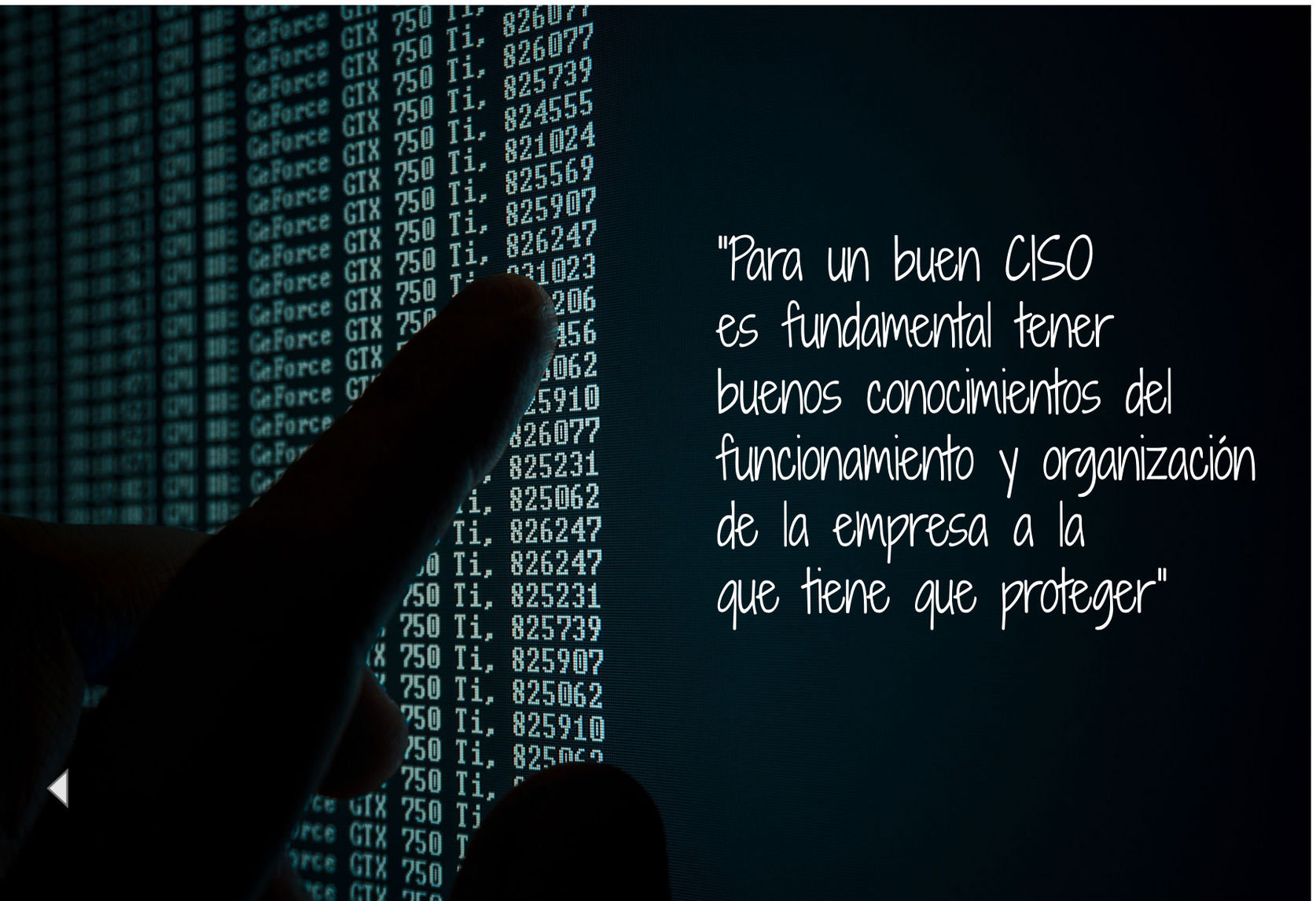
Cada año la compañía realiza un análisis de ciberseguridad "para analizar en qué situación estamos, cómo están evolucionado las ciberamenazas, y en definitiva, establecer un pipeline de ciberseguridad para el año siguiente". Esto permite realizar, en base a riesgo, una propuesta de mejora continua, "porque los ciberataques están en permanente evolución y lo que tenemos claro es que no se puede parar de mejorar".

Si tiene que mencionar alguna tecnología que será relevante, menciona Luis Ballesteros aquellas "que hacen uso de inteligencia artificial para realizar análisis de comportamiento en la red y detectar actividades anómalas" para poder detener el ataque cuanto antes. Además, con el incremento de servicios en nube, identifica Ballesteros también como imprescindibles las tecnologías que ayuden a implementar modelos de concepto Zero Trust y arquitectura SASE (Secure Access Service Edge).

Ciberseguridad en 2021

Que las ciberamenazas seguirán evolucionando es algo que va a ocurrir sí o sí "y tenemos es que estar alertas y preparados para adaptarnos y reaccionar rápidamente", asegura el directivo, que identifica una serie de tendencias que continuarán en los próximos meses, como que ciberdelincuentes y naciones estado continuarán desarrollando nuevas formas de ataque, se continuarán lanzando ataques de ingeniería social utilizando COVID-19 como base o que los trabajadores en remoto seguirán siendo objetivo de ataques de ingeniería social.

Añade que veremos más ataques de ransomware con doble extorsión, que continuarán evolucionando los ataques a móviles, se incrementarán ataques a IoT, los ataques a la cadena de suministro y las operaciones de ciber espionaje utilizando APT Advance Persistant Threats).



Enlaces de interés...

- Anatsa, un troyano bancario con gran impacto en la Unión Europea
- La Policía alerta de una modalidad de fraude bancario mediante SMS y llamadas telefónicas
- Guía para el éxito en la gestión de accesos privilegiados

Compartir en RRSS

it Digital Security

CAMINANDO HACIA ZERO TRUST

EVENTO ONLINE, 26 DE OCTUBRE DE 2021

EL MODELO DE SEGURIDAD QUE SE IMPONE EN LA EMPRESA

‘Si los clientes no son exigentes, las empresas no van a invertir en seguridad’

(José Luis Paramio, Userlytics Corporation)

Userlytics Corporation es una empresa dedicada, entre otras cosas, a realizar estudios de mercado cuyos clientes quieren comprobar la experiencia de usuario en nuevos prototipos de aplicaciones. El activo a proteger más importante, que no el único, de la compañía es la base de datos de testers que permite ofrecer a los clientes grupos definidos para realizar las pruebas, una base de datos que protege con celo José Luis Paramio, CISO de la compañía que durante años se dedicó al pentesting y pasó diez años en Japón.

Rosalía Arroyo

Le preguntamos por la evolución de la figura del CISO y responde asegurando que depende del tipo de empresa a la que preste sus servicios.

Dice también que la evolución del CISO va de la mano de la evolución de las tecnologías, como la aparición de los contenedores, del machine learning o el internet de las cosas; así como de la evolución de las necesidades y de las soluciones que ayudan

"Igual que estamos viendo el aumento del ransomware también veremos su caída, y entonces aparecerá otra cosa"

a protegerlo todo, de forma que “según avanza la tecnología avanza la necesidad del CISO y evoluciona su figura. Pero creo que la ciberseguridad en realidad no tiene un papel cantante en todo esto, sino que va a remolque de la evolución de la tecnología”. ¿No sientes que os ponen en primer plano? “Sí, estamos en primer plano. Estamos de moda. Pero nosotros no decidimos hacia dónde evoluciona la seguridad. Nosotros nos adaptamos”.

En esa tarea de adaptación dice haber visto morir muchas tecnologías que parecía que iban a quedarse para toda la vida, “y siempre se me viene a la cabeza Flash. Hay tecnologías que ahora parecen inmutables, que parece que son el presente y nadie se atrevería a decir que no son el futuro, pero llegarán otras que les sustituirán y no sabría decirte cómo va a quedar todo, aunque todos miramos de reojo a los ordenadores cuánticos”.

En un mercado saturado de fabricantes, soluciones y propuestas ¿cómo escoger? “El CISO siempre tiene una limitación, que es el presupuesto”, responde José Luis Paramio. Explica que hay una parte fácil: según las características de una empresa se tienen una serie de necesidades y una serie de productos que las cubren; “a partir de ahí se produce un descarte por presupuesto” por lo que el número de opciones ya se reduce, y se añaden factores humanos, como “que alguien de tu empresa o tú mismo te fíes más de un proveedor, o tengas un contacto, o llegue una oferta más agresiva… o pruebas, te equivocas y al año siguiente, cuando acaba la licencia, te vas a la competencia”.

“El grado de sensibilización depende del grado de exigencia de tu cliente”, responde José Luis Paramio cuando le preguntamos por el grado de sensibilización de las empresas por la ciberseguridad. Añade que “si tus clientes no son exigentes, la empresa no invertirá en ciberseguridad; y si tus clientes son exigentes, la empresa va a invertir”. Dice también el CISO de Userlytics que también deben tenerse en cuenta las necesidades tecnológicas de cada caso.

Servicios Gestionados

Respecto a los servicios gestionados, dice Paramio que son más útiles para empresas pequeñas, pero demasiado caros para ellas. “Y digo que son útiles porque al final te dan todo el servicio de ciberseguridad sin necesidad de crear un departamento de ciberseguridad ni contratar personal. Pero son demasiado caros. Una pyme en realidad no se lo puede permitir y sin embargo sería la empresa perfecta como objetivo para estos servicios”, reflexiona, para después añadir que, en su opinión, un servicio gestionado empieza a ser interesante cuando se necesita un SOC.

Seguimos hablando del SOC y añadimos Zero Trust a la ecuación. Para José Luis Paramio ambos términos, o lo que representan, son compatibles, “pero los conceptos son antagónicos. Por un lado voy a crear una red en la que no confío ni en mí mismo porque sé que están dentro, y por el otro voy a proteger el perímetro”.

"Lo más importante es la formación en seguridad que des a tus empleados"

"Nosotros no decidimos hacia dónde evoluciona la seguridad. Nosotros nos adaptamos"

Opina también el CISO de Userlytics que "la nube mata el SOC. Todo el que tenga servidores en Amazon o en Digital Ocean, ¿para qué necesitaría un SOC? Probablemente Amazon y Digital Ocean ya tienen su propio SOC y están monitoreando sus data centers constantemente. Puedes contratar con tu propio SOC y añadirlo, como un doble firewall, pero en realidad si alguien entra en uno de esos servidores no tienes más que restaurar la máquina virtual. Entiendo que el SOC es interesante para empresas muy grandes y necesidades muy concretas".

La nube

Sobre el cloud, dice José Luis Paramio que tenerlo todo en la nube es una tendencia; "todos los servicios nuevos que se ofertan, y cada vez hay más, y más interesantes, se ofertan como un servicio en la nube". En este tipo de entornos hay que proteger las credenciales por un lado, y cómo hace uso de los datos el usuario por otro lado, dice el directivo añadiendo que no es lo mismo un usuario que solo tenga acceso a su email, que un usuario que tenga acceso a un CRM, de forma que "según la importancia del dato que vaya a manejar ese usuario, la seguridad que lleva detrás es diferente".

Cuando le preguntamos por las tecnologías de seguridad que deberían ser imprescindibles en cualquier empresa nos pide José Luis Paramio que nos imaginemos una que no tiene presupuesto para seguridad, "en ese caso yo recomendaría ir a la nube y hacer uso de un autenticación multifactor en todos los servicios, como mínimo. Y si fuera posible, gestionar el login con un servicio de single sign-on; un SIEM de fuente abierta; un gestor de vulnerabilidades, el que pudiera; y gestionar un DLP. Nada muy elaborado pero muy útil y con lo que vas a vas a proteger el 80% por ciento de tu empresa. Ahora bien –añade, de aquí lo más importante es la formación en seguridad que des a tus empleados".

Asegura el directivo que en definitiva se trata de aplicar el sentido común, aprender de las catástrofes de los demás para reforzar tu seguridad y la formación al empleado, "y si tienes el apoyo de la dirección, miel sobre hojuelas".

Tecnologías de futuro

"Yo no puedo vivir, por ejemplo, sin un gestor de vulnerabilidades. Dado que somos una aplicación web, no puedo vivir sin un DAST, Dynamic Application Security Testing. Y un SAST, Static Application Security Testing, también es una tecnología increíblemente útil", explica José Luis Paramio.

"El CISO siempre tiene una limitación, que es el presupuesto"

Añade que sería deseable una asociación o alianza de empresas que estén enfocadas en el SAST, DAST, Vulnerability Assessment, SIEM, SOC, "sería deseable". Opina que los antivirus no tienen mucho interés a día de hoy, o por lo menos no la importancia que tenían, y que pasa algo parecido con los firewall, aunque siguen siendo necesarios.

Por otra parte, "estoy notando una tendencia a la seguridad hardware", asegura el CISO de Userlytics, apuntando a anuncios realizados por HP [Wolf] o Apple relativos a la implementación de seguridad en el propio dispositivo o algunos de los requisitos de Windows 11, tanto a nivel de procesador como módulos seguridad TPM.

Finalmente hablamos de cambios que pudiera haber en lo que queda de año relativos a la ciberseguridad. "Creo que ninguno. Yo diría que casi ni en 2022", dice, para añadir que igual que estamos viendo el aumento del ransomware también veremos su caída, "y entonces aparecerá otra cosa".

Enlaces de interés...

- 'Las empresas tienen que tener en mente la protección del ciclo de vida del dato' (Manuel Barrios, Solvia)
- 'No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla' (Alejandro Sánchez es el CISO de SEAT)
- 'Los CISOs nos hemos dado cuenta de que la preparación al final del día compensa' (Fermín Serna, Citrix)
- 'No estamos en el momento de que sólo contratando tecnología podamos estar protegidos' (Judit Closa, habitissimo)
- 'El cloud no se hace responsable de la seguridad' (Toni García, LETI Pharma)
- 'Si puedo envenenar un data lake o hacer que un algoritmo funcione mal, tendré más influencia para la extorsión' (Rik Ferguson, Trend Micro)

Compartir en RRSS

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™

Microsegmentación, clave para la seguridad empresarial

Elaborado por:

itResearch

Para:

zscaler

Microsegmentación, clave para la seguridad empresarial

'LAS TÉCNICAS DE MICROSEGMENTACIÓN TIENEN QUE SER ALTAMENTE AUTOMATIZADAS' (MIGUEL ÁNGEL MARTOS, ZSCALER)

CLICAR PARA VER EL VÍDEO

La microsegmentación es un método para crear zonas seguras en centros de datos y despliegues en la nube que permite a las empresas aislar cargas de trabajo entre sí y protegerlas individualmente. Su objetivo es hacer que la seguridad de la red sea más granular.

La segmentación de la red no es nueva. Las empresas han confiado en firewalls, redes de área local virtuales (VLAN) y listas de control de acceso (ACL) para la segmentación de la red durante años. Con la microsegmentación, las políticas se aplican a cargas de trabajo individuales para una mayor resistencia a los ataques.

La granularidad que ofrece la microsegmentación es esencial en un momento en que la mayoría de las organizaciones están adoptando servicios en la nube y nuevas opciones de implementación, como contenedores, que hacen que la seguridad perimetral tradicional sea cada vez menos relevante.

Y es que a pesar de los diferentes tipos de protección [firewalls, IPS, etc] los ataques están logrando penetrar el perímetro y las infracciones continúan ocurriendo. El problema principal es que una vez que un ataque sobrepasa el perímetro de la red, existen pocos controles laterales para evitar que las amenazas se extiendan. La mejor manera de resolver esto es adoptar un modelo de seguridad microgranular más estricto con la capacidad de vincular la seguridad a las cargas de trabajo individuales y la agilidad para aprovisionar políticas automáticamente.

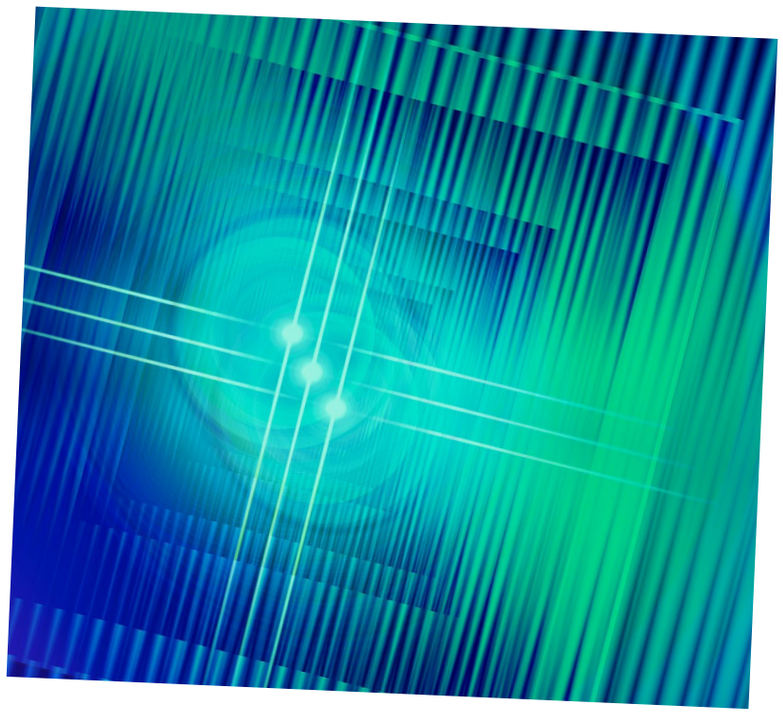
Se prevé que el mercado de microsegmentación alcanzará los 2.700 millones de dólares para 2025, con un crecimiento medio anual del 23.4% durante 2020-2025. Algunos de los factores que están impulsando este mercado son una mayor conciencia para proteger el entorno de la nube, el aumento del coste de los ciberataques y un mayor aumento del uso de aplicaciones, dispositivos conectados y dispositivos móviles, según datos de Industry ARC.

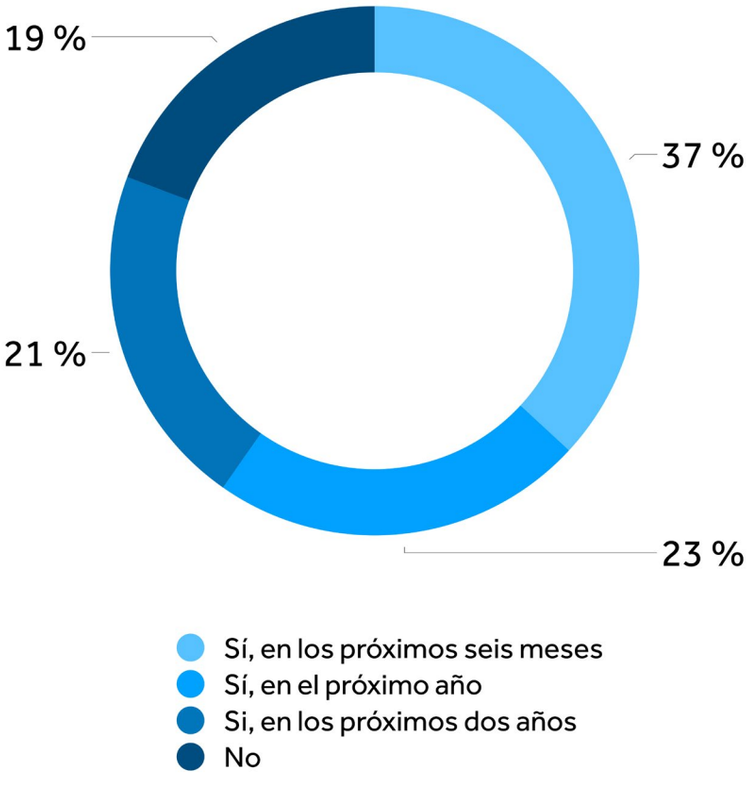
IT Digital Security, en colaboración con Zscaler, ha realizado una encuesta entre profesionales españoles durante los meses de junio y julio de 2021 para conocer la visión que los profesionales de las empresas tienen acerca de la microsegmentación, qué viene a solucionar, que beneficios aporta, qué características deben tener las soluciones que lo permitan o cómo impacta en la seguridad.

Microsegmentación, clave para la seguridad empresarial

"Si bien el concepto de microsegmentación en la superficie es fácil (hay que crear segmentos separados para microservicios), ponerlo en su lugar a menudo parece demasiado complejo, más aún con las conexiones internas. Sin embargo, uno de los mayores beneficios de la microsegmentación es la facilidad de escalar y cambiar las políticas. Al utilizar esta estrategia como base, su empresa ahora tiene la agilidad necesaria para realizar cambios internos (en empleados, dispositivos, cargas de trabajo y aplicaciones) para reaccionar a las necesidades comerciales cambiantes. Con la microsegmentación y la confianza cero, se crea la seguridad y la flexibilidad necesarias para el mundo actual".

Carlos Asún, CISO, Food Delivery Brands





¿Está considerando implementar microsegmentación como parte de su estrategia de seguridad para el datacenter?

Como decíamos, la microsegmentación es una forma de crear zonas seguras en los centros de datos y despliegues cloud que te permiten aislar cargas de trabajo y protegerlas individualmente, de forma que cuanto más pequeños son los segmentos, más se reduce la superficie de ataque y por tanto menor el riesgo para las empresas.

Según la encuesta realizada por IT Digital Security, la empresa española está más que dispuesta a adoptar microsegmentación como parte de su estrategia se seguridad para el centro de datos, aunque lo harán a diferentes velocidades.

Del 80,6% que consideran la adopción, la mayor parte, un 36,8% implementarán la microsegmentación en los próximos seis meses, un 22,8% la considera en el próximo año y un 21% en los próximos dos años.

Un 19,2% no considera la implementación de la microsegmentación asociada a la seguridad.

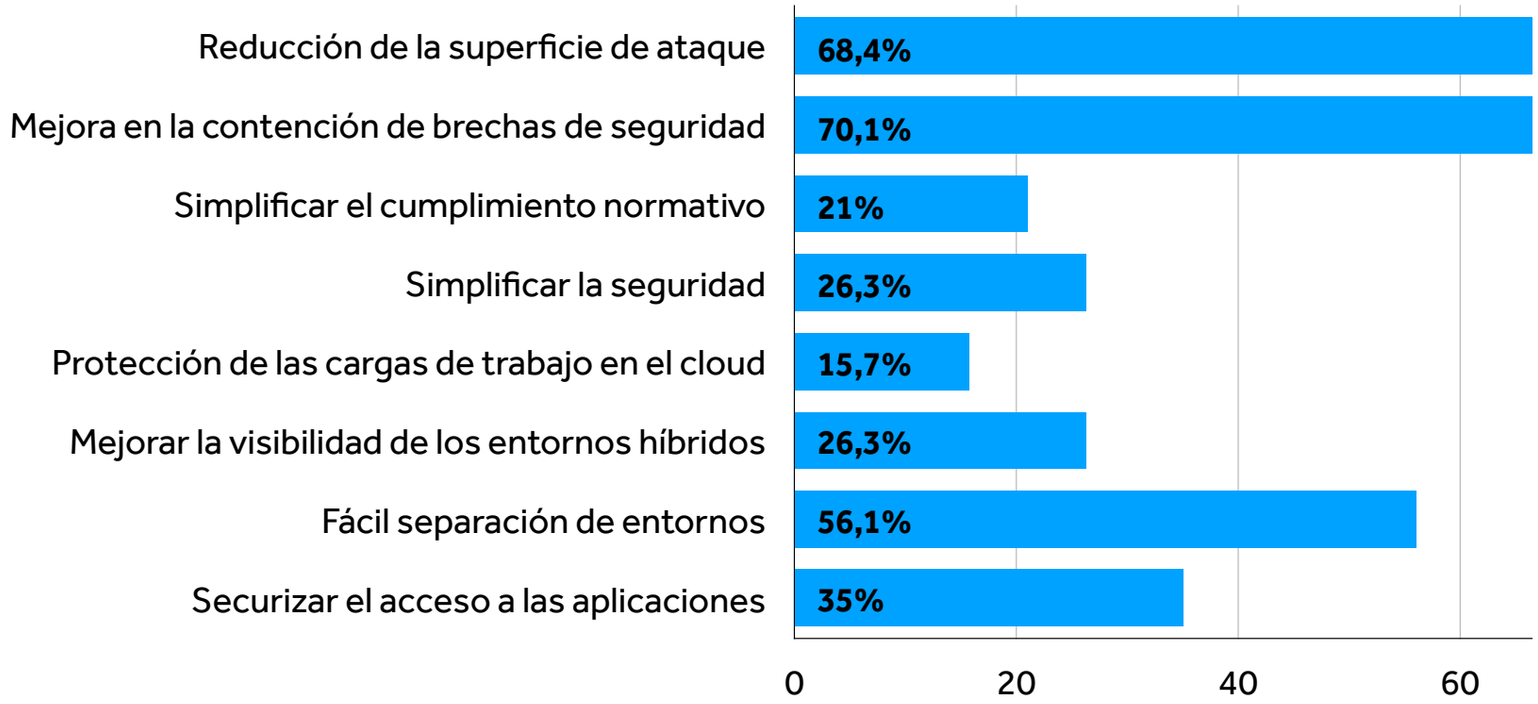
¿Qué objetivos cree que puede lograr con un proyecto de microsegmentación?

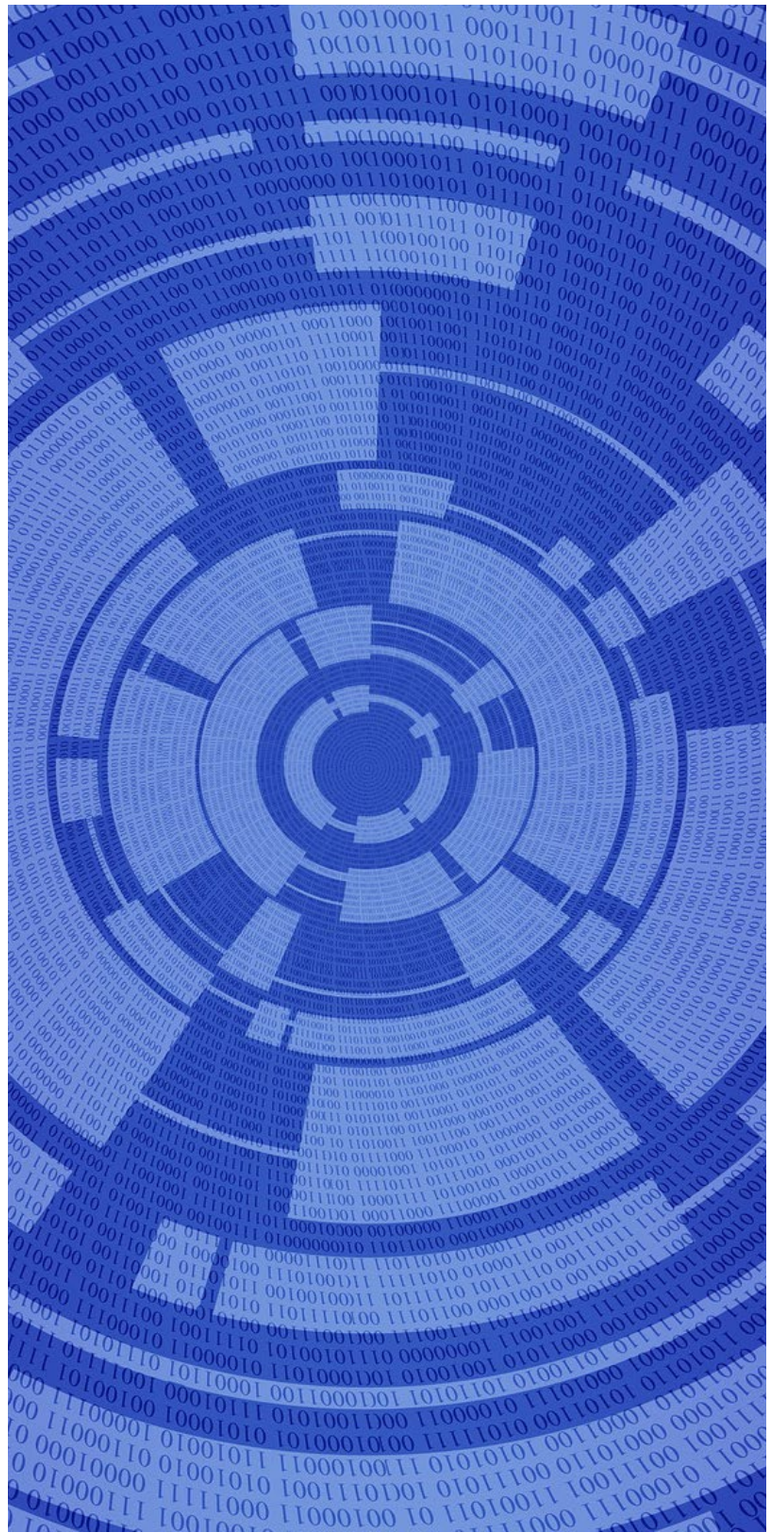
La microsegmentación ofrece a las empresas un mayor control sobre la comunicación este-oeste, o comunicación lateral que se produce dentro de las empresas. Un tráfico que ya no pasa por las herramientas de seguridad centradas en el perímetro. Si se producen infracciones, la microsegmentación limita la posible exploración lateral de las redes por parte de los ciberdelincuentes.

La mejora en la contención de las brechas de seguridad es, para el 70,1% de los encuestados, el principal objetivo que persiguen en un proyecto de microsegmentación, seguido de la reducción de la superficie de ataque (68,4%). La fácil separación de entornos es el tercer objetivo más destacado para un 56,1%, que también valoran positivamente la posibilidad de securizar el acceso a las aplicaciones (35%) mediante la microsegmentación.

El objetivo menos valorado de los propuestos es la protección de las cargas de trabajo en el cloud (15,7), así como la posibilidad de simplificar el cumplimiento normativo (21%).

Existe un empate entre simplificar la seguridad y la mejora de la visibilidad de los entornos híbridos (26,3%) como posibles objetivos de un proyecto de microsegmentación.





¿Cuáles son las principales características que debería tener una solución de microsegmentación para hacer viable su despliegue?

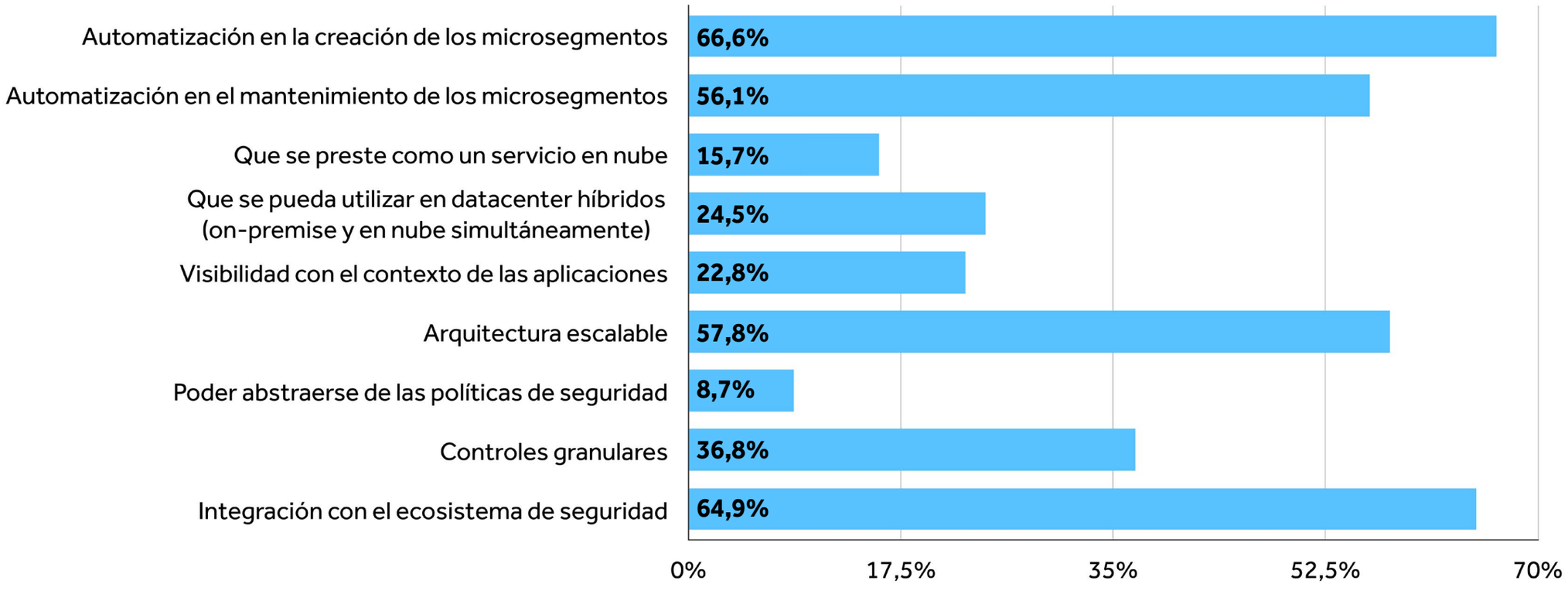
La microsegmentación permite políticas de seguridad más flexibles y precisas que se pueden asignar hasta el nivel de carga de trabajo. Estos controles minuciosos aseguran que los atacantes se enfrenten a menos debilidades potenciales para explotar, incluso cuando aumenta el número teórico de posibles puntos de ataque.

Las tres características más valoradas que debe tener una solución de microsegmentación según los encuestados son: la automatización en la creación de los microsegmentos (66,6%); su integración con el ecosistema de seguridad (64,9) y la automatización en el mantenimiento de esos microsegmentos creados (56,1%).

También se toma en consideración que sea una arquitectura escalable (57,8%) e incluso que se puedan aplicar controles granulares (36,8%).

Similares respuestas han tenido el que una solución de microsegmentación pueda ser utilizada en datacenter híbridos (on-premise y en nube simultáneamente) y que ofrezca visibilidad con el contexto de aplicaciones, para un 24,5% y un 22,8% de los encuestados respectivamente.

A pesar del interés que despierta el as-a-service, que se preste como un servicio en nube ha sido escogido por un 15,7% de los encuestados como una de las características que debería tener una solución de microsegmentación para hacer viable su despliegue. La opción que menos interés ha despertado es el que pueda abstraerse de las políticas de seguridad (8,7%)



Microsegmentación, clave para la seguridad empresarial

"La Microsegmentación ayuda a aislar los diferentes entornos que tenemos en una empresa permitiendo avanzar en el paradigma de Zero Trust o desconfianza total. Aislar los sistemas nos permite NO proporcionar accesos que quizás antes teníamos que realizar una segmentación más compleja a nivel de red, sin embargo, ahora, con la microsegmentación nos facilita esta labor y podemos aislar de forma eficiente cada uno de los entornos. No quiero dejar de comentar que la microsegmentación también permite una monitorización más sencilla, con lo que facilita encontrar posibles fallos más rápidamente".

Jose María Pulgar Gutierrez, CISO Responsable Oficina Técnica Seguridad de la Información, Bosonit

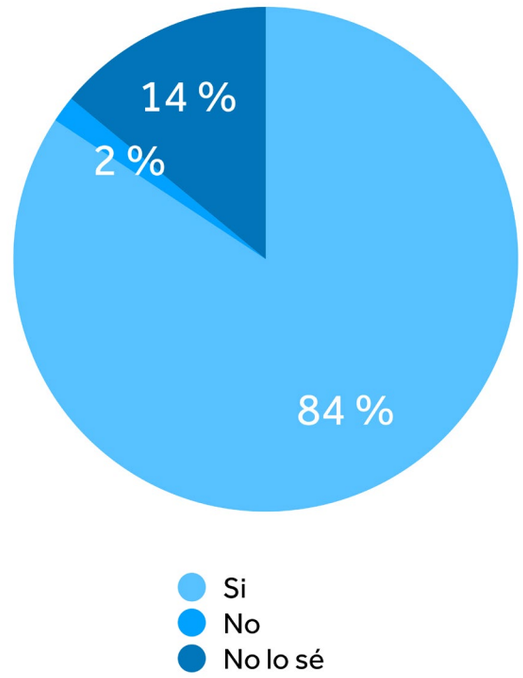
¿Cree que la microsegmentación le puede ayudar a implementar o extender su estrategia Zero Trust?

Rotunda es la afirmación de que la microsegmetación ayuda en la implementación de una estrategia de Zero Trust. Así lo consideran el 84,2% de los encuestados.

Un 14% no lo tienen claro, mientras que un mero 1,7% no creen que la microsegmentación ayude a extender un marco de seguridad que requiere que las organizaciones autentiquen y autoricen a todos los usuarios y dispositivos dentro y fuera del perímetro antes de permitir el acceso a aplicaciones y datos.

La microsegmentación es un método para crear segmentos de red de forma lógica y controlar completamente el tráfico dentro y entre los segmentos. Proporciona la capacidad de controlar las cargas de trabajo en un centro de datos o un entorno de múltiples nubes con controles de políticas granulares y restringe la propagación de amenazas laterales en el centro de datos.

Uno de los principios clave de un enfoque de confianza cero es nunca confiar y siempre verificar primero. La microsegmentación a nivel de host permite a los equipos de seguridad aislar entornos y segmentar cargas de trabajo y aplicaciones distribuidas. Una vez segmentadas, las políticas de seguridad detalladas se pueden aplicar en función de un enfoque de confianza cero.



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 Digital Security
Encuentros ITDS

Lecciones aprendidas para la transformación del puesto de trabajo

citrix

ozona tecnologia

Septiembre 2021

itds

Encuentros ITDS

LA VISIÓN DE LAS EMPRESAS LA VISIÓN DE LA INDUSTRIA IT

Lecciones aprendidas para la transformación del puesto de trabajo

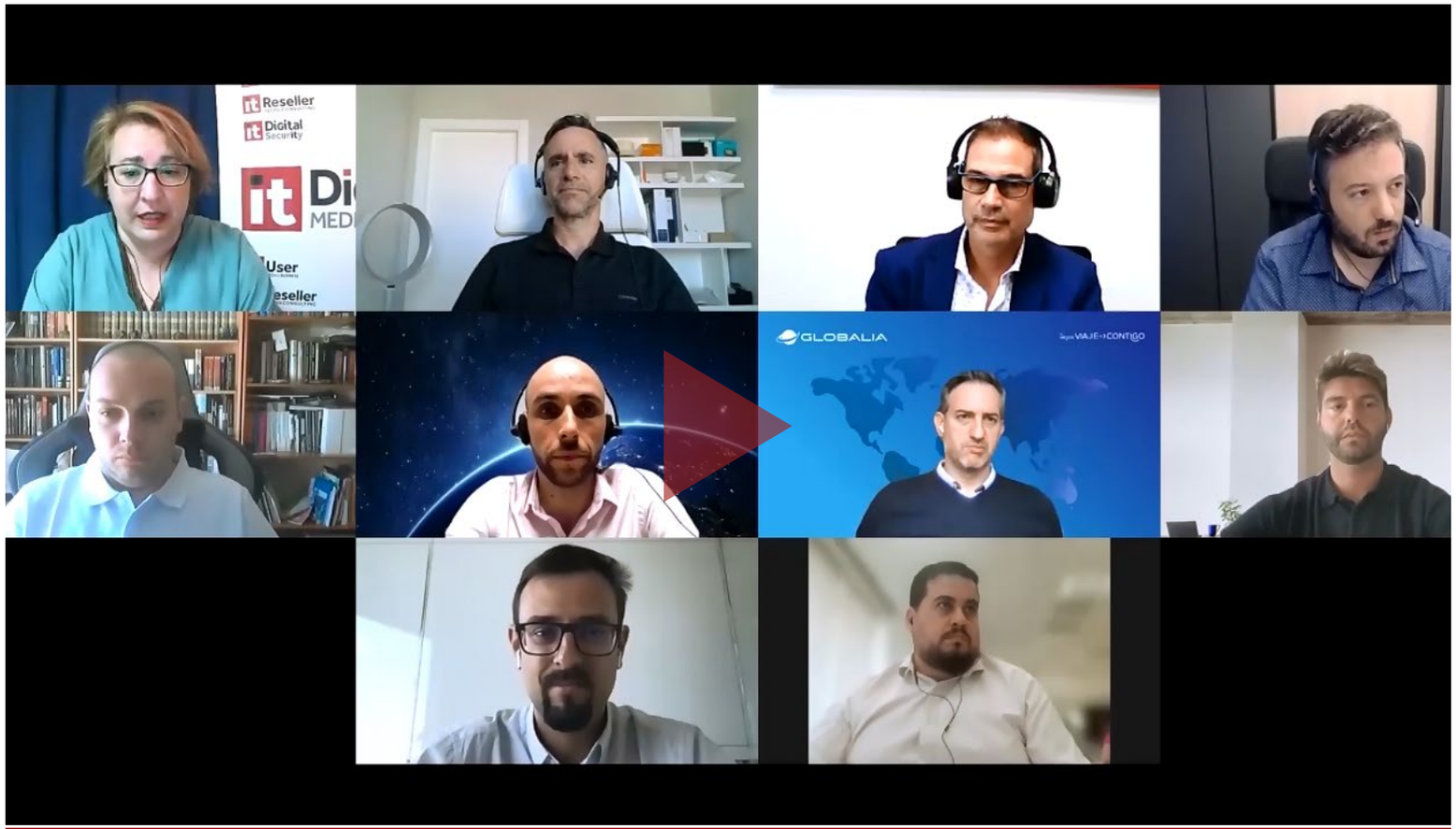
Hace ya más de un año que las empresas, empujadas por una amenaza llamada COVID, entraron en una nueva realidad que ha llevado a la imperiosa necesidad de digitalizar puestos de trabajo, migrar aplicaciones a la nube, automatizar procesos o echar mano de la IA.

El puesto de trabajo no está en la oficina, sino donde esté el empleado y el perímetro de seguridad, tan cuidadosamente delimitado en aquellos primeros tiempos del firewall, lejos de desaparecer se ha extendido hasta cada hogar. Esta nueva situación ha sido un reto para los responsables de TI y ciberseguridad de las empresas, y una oportunidad para los ciberdelincuentes que han

itds

Encuentros ITDS

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



ENCUENTROS ITDS
PUESTO DE TRABAJO REMOTO

CLICAR PARA VER EL VÍDEO

desplegado más ransomware y más phishing que nunca con demasiado éxito.

Con el objetivo de analizar la situación a la que se enfrentan los responsables de ciberseguridad de las empresas y qué medidas se adoptarán para una siguiente fase en la que predominará un modelo de trabajo flexible hemos reunido, con el patrocinio de Ozona Tech y Citrix, a un grupo de CISOS empezando por Pedro Mª Galdón Conejo, CIO y CISO de EMASA (Empresa Municipal Aguas de Málaga, S.A.); Daniel Zapico Palacio, CISO de Globalia; Iván Sánchez, CISO de Sanitas; Javier Sánchez Salas, CISO de HAYA Real Estate; Joan Massanet, CTO y CISO, Maximice Events Group; José Luis Paramio, CISO de Userlytics Corporation y Carlos Valerdi, CIO y CISO en Enso Energy.

Arrancaba el evento Marcos Paredes González, CTO y Cofundador de Ozona Tech, quien tras dar la bienvenida a los ponentes destacaba que, junto con Citrix, lleva muchos años habilitando el tele-trabajo y que “nuestro discurso, nuestra propuesta de valor y nuestras soluciones han tenido que ir evolucionando para contemplar cada vez más la parte de seguridad”.

LA VISIÓN DE LAS EMPRESAS

"Debemos replantearnos la tecnología y las herramientas"

Pedro Galdón, EMASA

EMPRESA MUNICIPAL DE AGUAS DE MÁLAGA, S.A., Pedro Mª Galdón, CIO y CISO

"El teletrabajo se tuvo que adoptar con mucha celeridad y para mucha gente que no tenía costumbre de teletrabajar", dice el CISO de EMASA (Empresa Municipal Aguas de Málaga, S.A.), asegurando que el nuevo modelo de trabajo que plantea tener a los empleados en casa de manera generalizada y de forma permanente, ha llevado a que "hayamos perdido el control de la fortaleza" y que la situación derivará en un entorno flexible "que nos permita realmente utilizar el teletrabajo para lo que debe ser, no como una situación de emergencia, sino como algo que de verdad facilite la labor a la gente que tiene que trabajar".

En su doble rol de CIO y CISO, Pedro Galdón reconoce la necesidad la formación y concienciación no sólo de los empleados, sino de los propios programadores, que en ocasiones piensan en la seguridad "como el barniz que le va a dar alguien a lo que ellos que han hecho, pero que no va con ellos".

Sobre el "hazlo seguro, pero que no se note", plantea Galdón cómo después del 11S todo el mundo asumió que para subirse a un avión tenía que pasar una serie de controles, o que con la pandemia se asume que, por seguridad, se tienen que hacer una serie de cosas que antes no se hacían y que no son realmente cómodas, "y sin embargo, cuando nos toca a los CISOS nadie quiere asumir que la seguridad lleva una serie de incomodidades. Que si yo me voy de mi casa y tengo que echar la alarma, tengo que dedicar cinco segundos a ello, pero la gente no quiere que le pida un doble factor de autentificación para entrar en una aplicación. Esa molestia, que directivos y usuarios asumen en otros ámbitos no la quieren asumir en el término de ciberseguridad".

En un mercado que ha pasado de teletrabajo para unos pocos a extenderse a toda la empresa en poco tiempo "tenemos que repensar la tecnología", dice el CISO de EMASA. Explica que lo que valía para un grupo reducido ha valido en un momento de emergencia "porque se trataba de dar soluciones rápidas y que la gente se pudiera ir a casa". Pero cuando todo indica que el teletrabajo se va a consolidar como una herramienta de flexibilidad, conciliación y productividad, "creo que debemos replantearnos tecnologías y herramientas para que sea algo más transparente para el usuario, y más seguro".

MAXIMICE EVENTS GROUP, Joan Massanet, CTO y CISO

Reconociendo que el teletrabajo tuvo que ser implantado “con una celeridad extraordinaria” dice Joan Massanet, CTO y CISO de Maximice Events Group, que es fundamental intentar controlar lo que hacen los empleados, pero que también representa un gran reto vigilar la cadena de suministro porque, en ambos casos “no es algo que puedas controlar”.

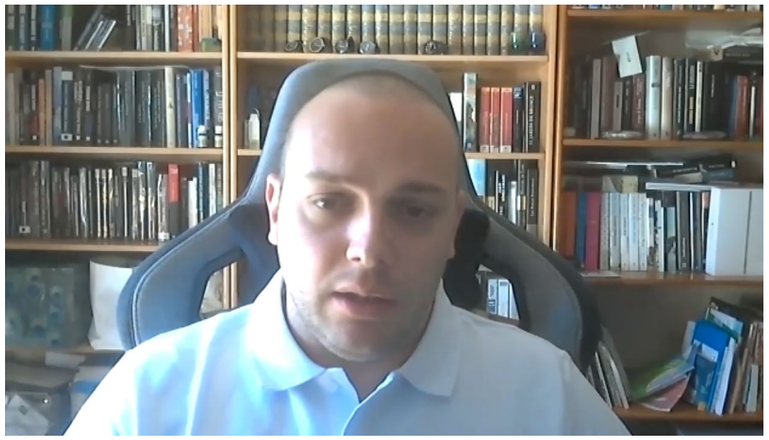
Sobre la heterogeneidad de los entornos IT y de ciberseguridad de las empresas, reclama Joan Massanet un mayor compromiso por parte de los fabricantes por la inteoperabilidad “porque nos encontramos en un punto bastante crítico y todos tenemos que ir de la mano”. Los productos, asegura, tienen que hablarse entre ellos para que podamos tener “una visibilidad de lo que está ocurriendo realmente en nuestra empresa”.

Menciona durante su intervención el CISO de Maximice Events Group la necesidad de que los responsables de ciberseguridad aprendan a hablar el lenguaje del usuario y, en términos más generales, que las empresas aprendan a convertir la adopción de medias y certificaciones de seguridad en un argumento de venta frente a los clientes, que en el caso de su compañía pueden ser Porche, SEAT o Ferrari.

> "El contar con los servicios fundamentales basados en cloud, hace que no importe que los empleados estén en casa o en la oficina"
>
> Joan Massanet, Maximice Events Group

Explicando que el uso que Maximice Events Group hace de la VPN no es tanto un tema de conexión a la empresa en sí como un control de lo que están haciendo los usuarios, y reconociendo que es una tecnología cada vez tiene menos tendencia, y que en entornos cloud no tiene sentido, dice Joan Massanet que en Maximice Events Group la VPN es algo que se activa en todos los ordenadores que están fuera de la oficina cuyo tráfico es obligado a pasar por un firewall.

En cuanto al nuevo modelo de trabajo mixto, el contar con todos los servicios fundamentales, como el ERP o correo electrónico, basados en cloud, hace que no importe que los empleados estén en casa o en la oficina desde el punto de vista de seguridad aplicando, eso sí, doble factor de autenticación o políticas de ubicación restringidas.



USERLYTICS CORPORATION, José Luis Paramio, CISO

El confinamiento no cambió mucho la forma de trabajar en Userlytics Corporation, donde ya existía antes de la pandemia una cultura de teletrabajo instaurada. Para José Luis Paramio, CISO de esta compañía, el reto al que se enfrentan los responsables de ciberseguridad tras la pandemia está

"Mi empresa ha convertido la seguridad en un argumento de venta más"

José Luis Paramio, Userlytics Corporation

relacionado con "las necesidades y exigencias de nuestros clientes según avanza el interés por la ciberseguridad". Explica el directivo que las preguntas y requisitos de los nuevos clientes en torno a la seguridad antes de firmar un acuerdo son cada vez más altos y requieren inversiones.

"Mi empresa ha convertido la seguridad en un argumento de venta más, y una diferenciación con respecto a la competencia", asegura José Luis Paramio, quien añade que esto ha llevado a adoptar medias y certificaciones que han hecho que "seamos más seguros como empresa".

Respecto a cómo afronta Userlytics el modelo de trabajo híbrido, apuesta José Luis Paramio por no tener "absolutamente nada en local" y aplicar una serie de medidas, como es limitación de conexión de memorias USB, discos externos…. Todo ello "escrito por políticas y aceptado por empleados". Explica que la dispersión, no sólo geográfica, sino horaria, hace que eso sea "el mejor Zero Trust para nosotros" y que al ser la propia compañía un servicio en nube hace que sea "coherente que nos basemos en la nube".

Añade también José Luis Paramio que poco a poco se está volviendo a la oficina, un lugar donde lo único que se tiene es un router y un firewall, lo que hace que, desde el punto de vista de la seguridad "la diferencia entre trabajar en casa y trabajar en la oficina sea ninguna en nuestro caso".

Considera el CISO de Userlytics que su gran fortaleza, "la mejor herramienta que tengo" es la implicación de la dirección de la compañía en la ciberseguridad; "cuando yo voy a pedirle a un usuario que por favor haga esto o lo otro, las palabras salen de mi boca, pero él escucha la voz de mi jefe".

ENSO – ENERGY ENVIRONMENT AND SUSTAINABILITY, Carlos Valerdi, CIO y CISO

"Creo que el reto más grande al que nos estamos enfrentando es entender que nuestro perímetro ya no termina en las puertas de la compañía, sino que se extiende hacia todos los usuarios que están dentro de nuestra corporación", dice Carlos Valerdi,

"Posiblemente tendremos que ser mucho más estrictos de lo que estamos siendo hoy"

Carlos Valerdi, Enso Energy

CIO y CISO en Enso Energy. Añade que la concienciación, y que las personas entiendan que cuando están trabajando en remoto corren mucho más riesgo y pueden poner en riesgo a la compañía, es fundamental.

Dice Carlos Valerdi que "el usuario tiene que sentir lo que es realmente la seguridad y adoptarla para su vida personal y laboral", no solo porque los responsables de ciberseguridad puedan terminar siendo "una caja negra" y a veces no se entiende muy bien cuál es nuestra función, sino porque en un futuro posiblemente "tendremos que ser mucho más estrictos de lo que estamos siendo hoy". Asimismo considera vital que las personas dentro de la compañía entiendan cuál es la función del CISO y se den cuenta de que "no somos el área de servicios que acompaña al negocio, sino que somos parte del negocio".

El año pasado Enso Energy pasó por un proceso de venta y una segregación tecnológica importante que, en opinión de Valerdi, "posibilitó el despliegue de muchas herramientas necesarias para para enfrentarnos a lo que se están dando en el mundo

y lo que nos espera en un futuro" y apostar por un entorno flexible que pasó por la adopción de un entorno cloud. La labor no fue fácil debido a la casuística de la empresa, donde por un lado se operan y mantienen plantas de energía y además se cuenta con una empresa que hace ingeniería, de forma "hay que enfrentar cada realidad y tiene que haber una línea base de política y de gobernanza".

La migración, realizada en plena pandemia, se planteó como una oportunidad para posicionarse de cara al futuro adoptando tecnologías punteras como el XDR (Extended, Detection and Response) y "estar en otra línea de defensa, mucho más preparado para lo que venga", asegura Carlos Valerdi.

"Hay que ir hacia un punto de acceso único"

Daniel Zapico, Globalia

GLOBALIA, Daniel Zapico Palacio, CISO

Para Daniel Zapico, CISO de Globalia, el trabajo en remoto ha pasado de considerar un dispositivo corporativo conectado a una VPN a poder trabajar con una tablet en una cafetería o aprovechando un viaje en tren, y el reto es "que eso se pueda hacer de forma segura y sencilla para el usuario". Añade que "el concepto VPN está desfasado" y que habría que ir hacia un punto de acceso único, donde se tengan todas las aplicaciones y al que pueda acceder cualquier dispositivo, de forma que ya solo tengas que preocuparte de garantizar la identidad.

Sobre la consolidación tecnológica que para muchos debería producirse después de un año de adopción tecnológica acelerada para hacer frente a la pandemia, dice Daniel Zapico que, "a pesar de que tiene todo el sentido", es algo que "va a tardar muchísimo" y que puede resultar imposible debido a la existencia de entornos legacy que son "intocables". Es más, para el CISO de Globalia más que una consolidación lo que se está produciendo es una divergencia en la que además de los entornos tradicionales se tienen entornos cloud y además de los dispositivos gestionados, el BYOD; "la clave es cómo hacer que aun estando en ese modelo de divergencia, que cada vez va más, la percepción desde el punto de vista usuario final sea lo contrario".

Reconociendo que en Globalia el impacto del teletrabajo no fue tanto tecnológico como de volumen, explica Daniel Zapico que ya se contaban con herramientas implantadas antes del teletrabajo. Destaca la ayuda que aportó el XDR por su capacidad de aportar visibilidad y añade que, aunque todo el mundo considera que el trabajo remoto empeora la postura de seguridad "en mi opinión para algunas cosas es hasta bueno porque cuando tus equipos no están conectados a la misma red corporativa y entra un ransomware, la propagación lateral se limita sustancialmente y tienes más tiempo de reaccionar que si te ocurre dentro de tu propia

infraestructura. Que no es que se resuelva el problema, pero te da una ventaja".

¿Hacia dónde tenemos que ir? "Yo quiero llegar a un punto en el que me dé igual que un usuario esté dentro de las instalaciones o que esté en su casa, que esté accediendo con un dispositivo corporativo o con uno personal", dice Daniel Zapico, proponiendo un portal que sea la base de un modelo Zero Trust "en el que incluso estando el dispositivo comprometido, yo sigo protegiendo mi dado, mi identidad y las aplicaciones que utilizo".

SANITAS, Iván Sánchez, CISO

Para Iván Sánchez, CISO de Sanitas, el modelo de negocio en el mercado sanitario "ha cambiado completamente". El despliegue de plataformas de telemedicina ha reducido las visitas a los centros médicos si bien ha supuesto un rato a la hora de desplegar estos nuevos sistemas en tiempo récord

"El proxy en la nube tiene que ser parte de cualquier agenda"

Iván Sánchez, Sanitas

y con la seguridad adecuada, por lo tanto el primer reto al que ahora se enfrenta es "asentarlo todo". El segundo reto es "encajar todo eso en un modelo sostenible económicamente, porque atacar es mucho más barato que defender, y debemos hacer entender muy bien la necesidad de inversión en estos nuevos entornos respecto la inversión en entornos on-premise". Un tercer reto es "la gestión del incidente en un modelo de trabajo remoto".

Para el CISO de Sanitas un entorno de tecnología heterogéneo es complejo de gestionar, lo que está llevando a las empresas hacia el camino de la consolidación tecnológica. La adopción del cloud y el tener en cuenta temas relacionados con la experiencia de usuario son también tendencia en Sanitas, según explica el CISO de la compañía, quien además asegura que las soluciones basadas en cloud "han acelerado muchísimo la adopción de un nuevo modelo de seguridad" y que el reto es cómo mantenerlo todo porque "lo que está claro es que no vamos a volver a lo anterior de ninguna manera".

Para Iván Sánchez, el proxy en la nube es una solución que "tiene que ser parte de cualquier agenda". Explica el directivo que es algo que la compañía ya tenía desplegado cuando se inició la pandemia y cuyo caso de uso inicial fue "quitarnos infraestructura on-premise y apostar por un modelo escalable". Asegura el CISO de Sanitas que fue "una fantástica decisión" porque cuando los empleados se fueron a casa se pudo mantener en control de la navegación

del usuario, la categorización de las webs, aplicar bloqueos en tiempo real, etc.

También es fundamental una solución EDR, que también se tenía desplegada en Sanitas, y aumentar la apuesta por la concienciación.

El modelo Zero Trust, entendido como un modelo basado en la identidad, el dispositivo y un contexto adaptativo que tiene en cuenta desde dónde y cómo se conecta el usuario, es relevante para el responsable de ciberseguridad de Sanitas, que habla en todo caso de la complejidad de su adopción en un entorno como el de su compañía donde hay muchísimo personal que no está ligado a un dispositivo o localización concreta.

HAYA REAL ESTATE, Javier Sánchez Salas, CISO

"Nuestro reto de post-pandemia ha sido el usuario, hacerle entender que tenemos que hacer un frente unido a la seguridad", y saber que si los medios que se ponen para proteger a la empresa no son fáciles y transparentes para los usuarios "vamos a fracasar", dice Javier Sánchez Salas, CISO de HAYA Real Estate.

Asegura el directivo que este es el año de la consolidación, de homogeneizar "todos los procedimientos que hemos abordado durante 2019-2020, incluida la nueva forma de trabajar", porque "no nos vale nada establecer modelos de emergencia, si luego no los aterrizas".

"Hemos conseguido un modelo de acceso único e invisible para el usuario", asegura Javier Sánchez. El producto, que se ha desarrollado internamiento, permite que cualquier usuario puede acceder a cualquier aplicativo de negocio a través de un portal. Explica Javier Sánchez Salas que la clave es un gestor de identidades y que el portal facilita que, independientemente se esté dentro de la red de HAYA o no, "el acceso sea el mismo". Para el usuario es transparente en tanto en cuanto que los mecanismos de autenticación son los mismos, y es dentro del propio portal de acceso donde se monitoriza cómo se conecta o deja de conectar cada usuario".

"A mí me da igual que el empleado trabaje desde casa, desde la oficina o incluso desde la playa. Lo que tenemos que hacer nosotros es tener los medios preparados para que, en caso tener que conectarse desde fuera, trabaje igual que si estuviera en la oficina", dice Javier Sánchez Salas, añadiendo que debido a lo comentado durante su intervención no le impacta el modelo de trabajo híbrido que está por venir, algo que considera que afecta más al departamento de recursos humanos.

"Hemos conseguido un modelo de acceso invisible para el usuario"

Javier Sánchez Salas, HAYA Real Estate

LA VISIÓN DE LA INDUSTRIA IT

"Tener una experiencia homogénea es imprescindible para un modelo de trabajo flexible"

Marcos Paredes, Ozona Tech

OZONA TECH, Marcos Paredes González, CTO y Cofundador

Marcos Paredes González, CTO y Cofundador de Ozona Tech, aseguraba durante su intervención que, junto con la necesidad de ponérselo fácil al usuario y concienciarle de que es el principal punto de entrada de malware en las compañías, también supone un reto el ofrecer soporte en entornos de trabajo remoto o intentar mitigar "esas incidencias que puedan ocurrir en cualquier lugar".

La experiencia de años dedicado a habilitar el teletrabajo permite a Marcos Paredes asegurar que el modelo Zero Trust se está imponiendo y que "las políticas deben ser homogéneas y el usuario tiene que sentir que trabaja en un solo entorno".

Dice Marcos Paredes que el puesto de trabajo híbrido, flexible, se empieza a asumir como definitivo y que en función del nivel de madurez en el momento del confinamiento las empresas están en una fase o en otra. Asegura el directivo de Ozona Tech que los que llegaron con cierto grado de madurez y de desarrollo, lo han tenido muy fácil porque simplemente incrementaron el volumen, y que, además de en la seguridad, "esas empresas ahora están pensando en la experiencia de usuario, porque es imprescindible para un modelo flexible que la experiencia sea homogénea".

En lo que parece haber consenso, dice también Marcos Paredes, es hacia dónde se va: un punto único de acceso y tenerlo todo en remoto. "Conéctate desde donde quieras, como quieras, con el dispositivo que quieras y te voy a pedir, eso sí, un reto: tu contraseña. Si sospecho que estás en un entorno no habitual, te pongo un reto a mayores, pero adaptado a tu riesgo", explica el directivo.

En esta transición hacia una solución de trabajo flexible en la que el usuario acepte las medidas de seguridad de buen grado, menciona también Marcos Paredes que "la monitorización de la experiencia del usuario es fundamental". Asegura el directivo que "poder medir cuál es la experiencia de uso, cómo los usuarios hacen uso de sus dispositivos, de las aplicaciones, de las de las herramientas que la compañía pone para desarrollar su trabajo, es fundamental" y que ya que lo que no se puede medir, no se puede mejorar, es importante "que el usuario tenga información de cómo está usando los sistemas en dos vertientes, una en cuanto a productividad y otra en prácticas de riesgo".

CITRIX, Luigi Semente, Sales Specialist

Asegurando que el concepto de trabajo flexible se está imponiendo y que es algo que se verá reflejado en los convenios corporativos de una de cada dos empresas españolas antes de finales de 2021, asegura Luigi Semente, Sales Specialist de Citrix, que el puesto de trabajo ha pasado de ser algo táctico a ser algo estratégico.

Dice también Luigi Semente que ahora "la ciberseguridad es un aliado de negocio", y menciona que uno de los retos a los que se enfrentan los CISOs es "cómo garantizar una seguridad consistente y coherente a todos los usuarios, desde lo que se conectarán desde una red corporativa, a quienes lo harán desde una red de Internet, o desde un dispositivo personal. Cómo voy a garantizar que mis datos y mis aplicaciones, que ya están en todos lados, están protegidas". Un segundo reto el cómo dar visibilidad a todos los diferentes elementos, los activos corporativos; "cómo controlar los datos sensibles cuando un usuario se está conectando desde cualquier sitio".

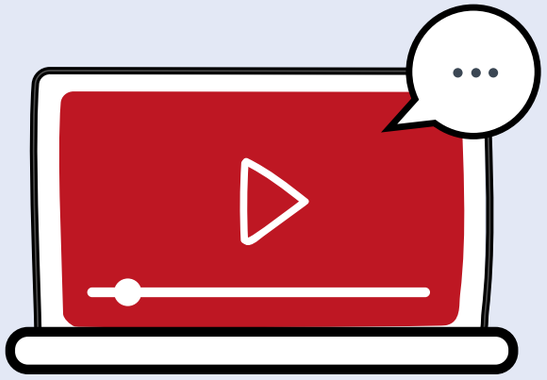
En este proceso hacia el puesto del trabajo del futuro, un puesto de trabajo flexible y seguro, dice Luigi Semente que "el rol del proveedor y de los integradores es clave". Habla de detectar y analizar los activos corporativos que se necesitan proteger porque, existiendo muchísima tecnología y funcionalidades, "a veces compramos un Ferrari para estar atascados en la M-40 en hora punta".

Asegura el ejecutivo de Citrix que el mercado español ya ha recorrido la mitad del cambio hacia ese puesto de trabajo flexible, bien gracias a tecnologías de virtualización de escritorio o VPNs, pero que hay que ajustar todas esas características.

Respecto al uso de VPN, asegura que su uso depende del ecosistema; en un entorno tradicional que permite que los datos, las aplicaciones y los usuarios permanezcan dentro de un perímetro de seguridad bien definido, puede valer, no así cuando nos adentramos en el mundo de los servicios, las herramientas colaborativas y los usuarios conectándose desde redes que en muchos casos no se pueden controlar. Ha llegado el momento, asegura, "de empezar a evolucionar el modelo". it

El papel de la ciberinteligencia en la seguridad empresarial

La ciberinteligencia es el futuro de la ciberseguridad en un momento en que los ciberataques se suceden sin freno y las amenazas son desconocidas y sofisticadas. En este IT Webinar te enseñaremos cómo la ciberinteligencia ayuda a la seguridad empresarial desde tres puntos de vista: en la superficie de ataque pública; en la Darkweb; y analizando y correlando eventos.



#ITWEBINARS

Atención pública al ciudadano: hacia una relación de 360 grados

En este encuentro se reunirán diferentes portavoces de la Administración Pública para debatir sobre las distintas propuestas y formas de generar una atención proactiva y digital con un ciudadano que avanza en un futuro digital y los retos que tiene el sector público para construir y estrechar ese vínculo con los habitantes de sus municipios.

Conectando y entendiendo a la empresa sin fronteras

En plena era cloud, descentralizada, de trabajo remoto, la conectividad se da por hecho. No así una buena experiencia. SD-WAN se afianza mientras 5G se abre camino, la computación se marcha al Edge y el IoT sigue avanzando sin freno y a lo grande. ¿Qué opciones tienes para gestionar una empresa cuyo perímetro está cada vez más diluido y potenciado por las nuevas tecnologías de conexión? Acompáñanos en este Encuentro IT Trends para saber a qué retos se enfrentan las empresas “borderless”.

REGISTRO

El vertiginoso crecimiento del mercado ciber

La ciberseguridad está de moda, y no solo entre los ciberdelincuentes. Durante los primeros seis meses del año las inversiones en este mercado aumentaron hasta acumular 51.000 millones de dólares en 593 transacciones, cifras que han superado las de todo 2020.

La pandemia no sólo nos cambió la vida, sino que disparó los ciberataques, cambiando el panorama de ciberamenazas. El ransomware es el líder indiscutible en la falta de sueño de los responsables de seguridad, seguido de cerca por los ataques a la cadena de suministro. Por cierto que sobre estos últimos advertía recientemente la agencia de ciberseguridad de la Unión Europea, ENISA, diciendo que las protecciones de ciberseguridad más tradicionales ya no son eficaces para defenderse de este tipo de ataques.

El gran momento del mercado de ciberseguridad se produce bajo la sombra del éxito de los ciberdelincuentes, que están haciendo un gran año. Desde los ataques de ransomware a la red de transporte de petróleo de Colonial Pipeline a los ataques a la cadena de suministro contra las empresas de gestión remota como SolarWinds y Kaseya, los ciberdelincuentes han recaudado decenas de millones en pagos de empresas cuya ciberseguridad ha fallado. Defender es mucho más caro que atacar y el de la ciberdelincuencia es un mercado organizado que también invierte en cloud y en inteligencia artificial.

La necesidad de ciberseguridad y de tecnologías emergentes capaces de detectar y detener los ataques más avanzados es más real que nunca y el mercado se prepara para ello. Las valoraciones de ciberseguridad siguen siendo algunas de las más altas entre cualquier subsector de TI y las fusiones y adquisiciones de ciberseguridad acumulan 189.000 millones de dólares en 1.583 acuerdos desde 2012.

Durante los primeros seis meses de este año se han producido casi tantos acuerdos como en todo 2020: 163 contra 178. Además, el valor de los mismos ha sido mucho mayor: 39.500 millones frente a los 9.800 millones del mismo periodo del año anterior, o los 20.500 millones de todo 2020, según los nuevos datos de Momentum Cyber.

Las adquisiciones de empresas/activos públicos sumaron 19.100 millones en los primeros seis meses del año, lo que representa el 47% del valor total

de las transacciones realizadas. Además, los grupos de capital privado completaron 71 adquisiciones en el periodo por un total de 22.500 millones en valor de operación.

Lo que va de año acumula nueve acuerdos de fusiones y adquisiciones que han superado los mil millones de dólares, incluidos la compra de Proofpoint por parte de Thoma Bravo por 12.300 millones de dólares, una cifra que duplica el anterior acuerdo más grande de capital privado en el mercado de la ciberseguridad. También de alto valor fue la compra de Auth0 por parte de Okta, que pagó 6.400 millones, convirtiéndose en la tercera adquisición más grande dentro de mercado de ciberseguridad y que permite a Okta expandir sus ofertas de IAM y comenzar a atender a clientes enfocados en desarrolladores.

La compra de McAfee por un total de 4.000 millones pagados por STG permite a esta última combinar partes del negocio empresarial de McAfee con otra empresa en su cartera, RSA Security. STG es también protagonista de la compra de FireEye, por la que pagó 1.200 millones de dólares y está involucrada en el acuerdo Thycotic/Centrify, valorado en 1.400 millones de dólares y que permite ofrecer a estas compañías una completa oferta para los mercados de PAM, o gestión de cuentas privilegiadas, e IAM, o de gestión de accesos e identidades.

Inversiones

Según datos del estudio publicado recientemente por Momentum Cyber, los inversores dedicaron

> Se espera que lo que queda de 2021 sea aún más activo en lo que a salida a Bolsa de empresas de ciberseguridad se refiere

11.500 millones de dólares a las empresas de ciberseguridad en la primera mitad de 2021, frente a los 4.700 millones del mismo período del año anterior. Además, según los datos del informe, de las 430 transacciones realizadas en el primer semestre, 36 superaron los cien millones de dólares.

Por cierto que los 11.500 millones de dólares en el primer semestre del año supera el total de inversión realizado de los ocho años anteriores a 2020. Los datos muestran por otra parte que el número de acuerdos del segundo trimestre de 2021 disminuyó un 19% respecto al segundo trimestre de 2020, mientras que el volumen de acuerdos aumentó un 12%, lo que significa un aumento en el tamaño promedio de los acuerdos.

Y si echamos un poco la vista atrás, durante los últimos ocho trimestres, los inversores han acumulado inversiones por valor de 28.700 millones en ciberseguridad repartidos en 1.497 acuerdos.

El segundo trimestre de 2021 representa el décimo octavo trimestre consecutivo en capital invertido con 1.700 millones invertidos en abril (74

acuerdos), 1.900 millones invertidos en mayo (65 acuerdos) y 2.500 millones invertidos en junio (53 acuerdos).

El volumen de transacciones del segundo trimestre de 2021 estableció un récord, con el 41% del valor del trimestre generado solo de junio. El mes de junio de 2021 ocupa el segundo lugar como el mes de mayor recaudación por detrás de marzo de este año, cuando se recaudaron más de 65 millones de dólares de un total de 2.500 millones. Estos datos hacen que 2021 ya se perfile como uno de los años de financiación más importantes para la ciberseguridad.

¿Por qué?

Varias son las razones que están impulsando este mercado más allá de haberse colado en las noticias de los diarios. El ransomware, una gran palanca por su notoriedad, ha hecho que las empresas concentren sus esfuerzos en conseguir una mejor seguridad y visibilidad.

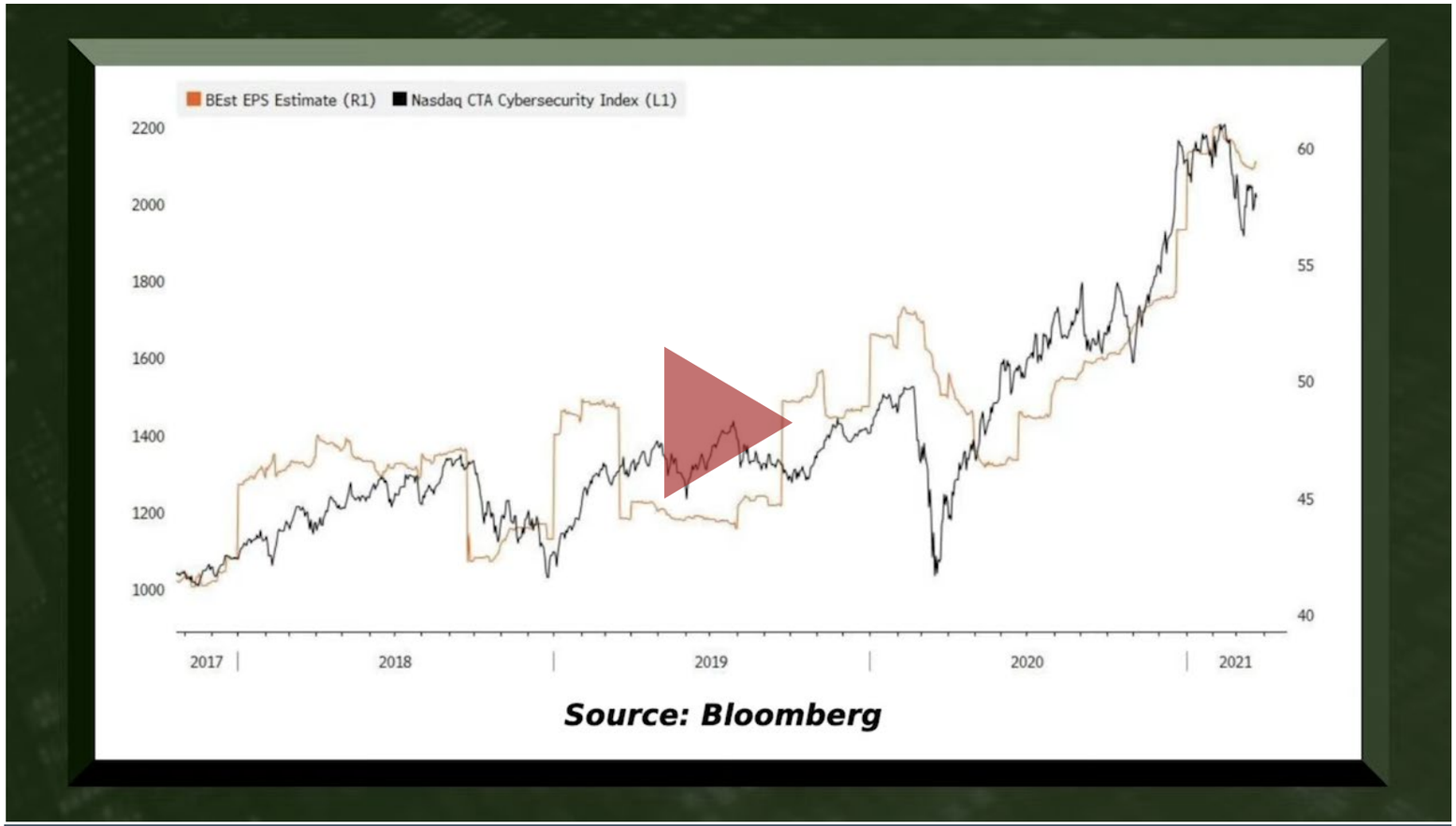
La pandemia también ha sido de gran ayuda al impulsar el trabajo en remoto y la adopción de la nube, lo que ha obligado a las empresas a revisar las tecnologías de seguridad implantadas, lo que a su vez ha impulsado las ventas. Según el informe, la empresa de seguridad promedio está negociando entre cinco y seis veces los ingresos el año pasado, lo que genera confianza en las juntas directivas, más predispuestas a invertir y poner la vista en competidores o empresas complementarias para crecer de manera inorgánica.

El mercado de Gestión de Identidades y Accesos (IAM) está creciendo una media anual del 14,5%

Otro factor que está impulsando el mercado es el auge de las SPAC (special purpose acquisition company), o empresas de adquisición de propósito especial, que son empresas creadas para mantener fondos para inversiones posteriores. Tres de los 10 principales acuerdos en ciberseguridad en los primeros seis meses de este año se han producido a través de empresas que se fusionaron con SPAC, frente a cero acuerdos el año pasado.

Las SPAC, que tienen la capacidad de agregar predicciones de rendimientos futuros en sus

El ransomware, una gran palanca por su notoriedad, ha hecho que las empresas concentren sus esfuerzos en conseguir una mejor seguridad y visibilidad



CYBERSECURITY STOCKS, DÉCADAS DE CRECIMIENTO

CLICAR PARA VER EL VÍDEO

documentos de inversión, aparecieron en Estados Unidos en la década de 1990, país en el que han tenido un creciente protagonismo, particularmente a partir de 2020.

Lo habitual es que una SPAC sea lanzada por un promotor, normalmente procedente de sector de inversiones de capital, que asume la gestión empresarial del proyecto. El primer paso es recaudar dinero a través de una oferta pública de venta e invertirlo inicialmente en una cuenta de depósito al tipo de mercado libre de riesgo. En un plazo determinado (alrededor de 24 meses), la SPAC trata de realizar una o varias adquisiciones de otras empresas. La decisión final sobre la adquisición se toma en la junta general de accionistas: si la mayoría de los accionistas vota a favor, se ejecuta la compra; en caso contrario, la SPAC se disuelve y los fondos recaudados se devuelven a los accionistas. Si no se realiza ninguna adquisición en el plazo acordado, la SPAC también se disolverá y los accionistas recibirán de nuevo el dinero con intereses depositado en la cuenta de garantía bloqueada.

Jugando en Bolsa

Una OPI, u Oferta Pública Inicial, es el proceso por el cual una empresa privada empieza a cotizar en una bolsa de valores, poniendo sus acciones a disposición del público en general para su compra. Pero es importante comprender que uno de los propósitos de una oferta pública inicial es permitir que los primeros inversores de la empresa retiren sus inversiones.

Hay que pensar en las OPI como el final de una etapa en el ciclo de vida de una empresa y el comienzo de otra. Hay varias razones para que una empresa busque una oferta pública inicial, como recaudar capital, de forma que los ingresos se puedan utilizar para expandir el negocio, financiar la investigación y el desarrollo o pagar deudas.

Por otra parte, salir a bolsa en una OPI puede proporcionar a las empresas una gran cantidad de publicidad.

En lo que va de año hay que destacar la salida a bolsa de tres empresas de ciberseguridad, dos realizadas en el mes de abril y una en el mes de junio.

La de KnowBe4 fue la primera OPI de 2021. La compañía proporciona un marco de concientización sobre seguridad que permite a las empresas evaluar, rastrear y mitigar la amenaza constante de las redes sociales y los ataques de ingeniería. Concienciación de seguridad, Orquestación, Automatización y respuesta, Gobernanza, Riesgo y Cumplimiento se encuentran entre las características de su plataforma. La compañía, que ahora cotiza en el Nasdaq lanzó 9,5 millones de acciones a un precio

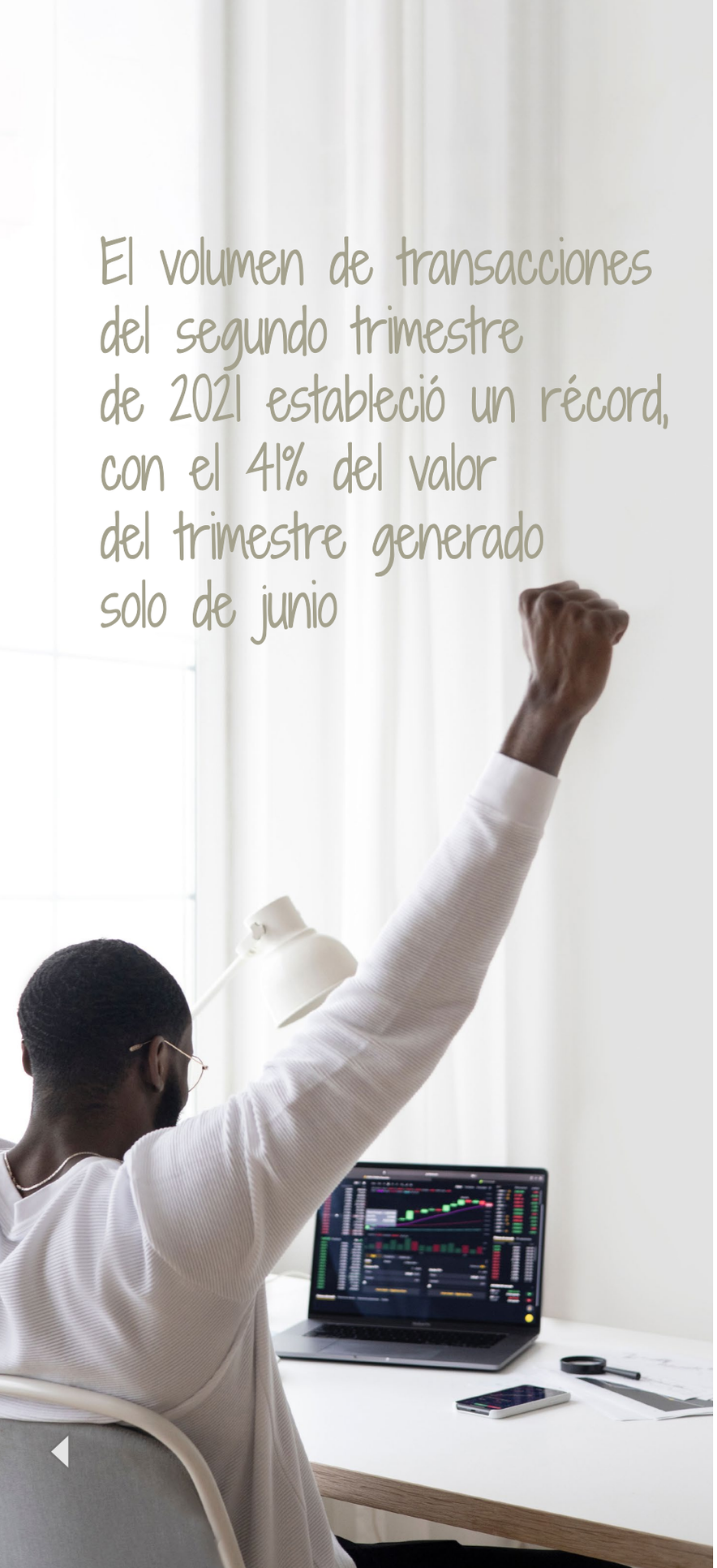
Las empresas privadas mejor financiadas

Las 15 empresas privadas mejor financiadas del mercado de ciberseguridad han recaudado un total de 8.900 millones desde su fundación. Hay que destacar la entrada de Transmit Security en el top 15 gracias a una ronda de inversión de 543 millones de dólares el pasado mes de junio, la mayor inversión en ciberseguridad hasta la fecha.

- **Tanium –** 980 millones de dólares
- **Rubrik –** 927 millones de dólares
- **OneTrust –** 920 millones de dólares
- **Netskope -** 744 millones de dólares
- **Lacework –** 600 millones de dólares
- **Snyk –** 549 millones de dólares
- **Transmit Security –** 543 millones de dólares
- **Forter –** 525 millones de dólares Truly – 491
- **Druva –** 475 millones de dólares
- **Ledger –** 465 millones de dólares
- **Acronis –** 426 millones de dólares
- **Plume –** 423 millones de dólares
- **Signoyd –** 421 millones de dólares
- **Stackpath –** 396 millones de dólares

Hay otras 123 compañías que han superado los cien millones de dólares en financiación caa una, sumando más de 24.000 millones de dólares, y entre las que cabría citar a Exabeam (393 millones), Lookout (375,2 millones), Vectra (352,7 millones), Illumia (332,5 millones) o CATO (332 millones).

El volumen de transacciones del segundo trimestre de 2021 estableció un récord, con el 41% del valor del trimestre generado solo de junio



inicial de 16 dólares el título, lo que le permitió recaudar 152 millones de dólares

La segunda OPI del año fue la de Darktrace, centrada en utilizar la Inteligencia artificial al servicio de la seguridad. La tecnología de autoaprendizaje de la empresa detecta, investiga y responde de forma autónoma a las ciberamenazas, incluidas las amenazas internas, el ransomware, los riesgos del trabajo remoto, la pérdida de datos y las vulnerabilidades de la cadena de suministro. La compañía, que cotiza en la bolsa de Londres, recaudó casi 200 millones de dólares poniendo en el mercado más de 57 millones de acciones a un precio inicial de 250 peniques la acción.

El protagonista de la tercera OPI de 2021 es SentinelOne, empresa pionera en el mercado de EDR (Endpoint, Detection and Response). La Compañía unifica la prevención, detección, respuesta y remediación dentro de una plataforma que identifica el comportamiento malicioso en múltiples vectores y elimina las amenazas a través de una respuesta integrada impulsada por inteligencia artificial. De las tres, ha sido la OPI más grande al poner en el mercado 35 millones de acciones a un precio de 35 dólares, lo que le permitió recaudar, en la Bolsa de Nueva York, 1.225 millones de dólares.

A finales de agosto de 2021 las acciones de las tres compañías se colocaban en los 24, 56 dólares las KnowBe4; 627 peniques las de Darktrace, y 61,01 dólares las de SentinelOne.

Por otra parte se espera que lo que queda de 2021 sea aún más activo en lo que a salida a Bolsa de empresas de ciberseguridad se refiere. Cybereason, Exabeam, Netskope o Tanium son algunos de los protagonistas esperados.

Sectores

Dentro del mercado de ciberseguridad, los sectores con más actividad en lo que se refiere a fusiones y adquisiciones son los de consultoría de seguridad, con 41 acuerdos; servicios gestionados, o MSSP, con 31; Risk & Compliance (17), seguridad del cloud (13) y seguridad de infraestructuras y de red (11).

En cuanto al valor de estas adquisiciones, es la seguridad del cloud el sector que lidera el ranking con un montante de 12.626 millones de dólares y ejemplos como el acuerdo de Proofpoint. Le sigue el de Gestión de seguridad y accesos, con 8.808 millones y Auth0, Thycotic y Centrify como los grandes protagonistas, y el de Seguridad de Infraestructuras y red, que suma 4.955 millones de dólares en adquisiciones realizadas en el primer semestre del año.

A la hora de invertir los sectores con mayor actividad cambian y es el de riesgos y cumplimiento el de mayor actividad, con 64 acciones, seguido del sector de seguridad del dato, donde se han realizado un total de 60 inversiones; SecOps / Incident Response con 47 acciones o gestión de accesos e identidades (IAM), con 43 inversiones.

Según datos del informe de Momentum Cyber, el sector de gestión de identidades y accesos acumuló inversiones de capital por valor de 1.758 millones

de dólares, seguido del de seguridad cloud con 1.410 millones de inversión, Risk & Compliance (1.314 millones), Seguridad del dato (1.297 millones) y seguridad de las transacciones y el fraude (1.164 millones).

SASE y DevSecOps, grandes impulsores

Desde que Gartner publicó su informe "El futuro de las redes de seguridad está en la nube" en agosto de 2019, que acuñó el concepto de SASE como la clave para el futuro de las redes y la seguridad, ha habido un rumor constante y creciente a su alrededor. SASE – Secure Access Service Edge no es un producto o servicio que se pueda adquirir directamente de un proveedor, sino un nuevo modelo para brindar servicios de red y seguridad, una evolución relevante de las tendencias que han sido claves en los últimos años, como security-as-a-service o network-as-a-service, y uno de los grandes impulsores del mercado de seguridad.

La transformación digital estaba ganando impulso antes de la pandemia, pero eran muchas las organizaciones que se encontraban en primeras tempranas y se vieron obligadas a acelerar. De repente, las aplicaciones en la nube y SaaS (software como servicio) se volvieron cruciales para la productividad.

Si bien las aplicaciones de nube y SaaS permiten la productividad, existe una variedad de preocupaciones de seguridad que vienen con su uso, combinadas con las implicaciones de seguridad de esencialmente destruir la red y confiar en la Internet

Principales inversores en ciberseguridad en el primer semestre de 2021

INVERSOR	EMPRESAS INVERTIDAS	SECTORES DE INVERSION
Insight Partners	Plume, Transmit Security, Wiz	Seguridad de Aplicaciones, Seguridad cloud, Seguridad del dato, Risk & Compliance
Sequoia Capital	Forter, Salt, Wiz	Seguridad cloud, Seguridad del dato, Risk & Compliance, SecOps y respuesta ante incidentes
Cyberstarts	Axis Security, Fireblock, Transmit Security	Threat Intelligence, Blockchain, Seguridad cloud, SecOps y respuesta ante incidentes
GGV Capital	Orca, Qingteng, VDOO	SecOps y respuesta ante incidentes, IAM, Seguridad Cloud, IoT
TenEleven Ventures	Axis Security, Cyware, NetSPI	Seguridad cloud y de aplicaciones, Threat Intelligence, SecOps y respuesta ante incidentes
Fama Ventures	Cygilant, Query.ai, Sevco	Threat Intelligence, Risk & Compliance, Seguridad Cloud, SecOps y respuesta ante incidentes
Vertex Ventures	Axonius, Cymulate, OwnBackup	SecOps y respuesta ante incidentes, Seguridad del dato, Risk & Compliance, IAM
Sapphire Ventures	Feedzai, OwnBackup, Uptycs	Seguridad Cloud, Seguridad del dato, SecOps y respuesta ante incidentes, Seguridad del fraude y las transacciones
Accel	Snyk, Socure, Vectra	Seguridad de aplicaciones, Seguridad del Dato, Seguridad de red e Infraestructuras, Seguridad de la mensajería
Coaute Mangement	Fireblocks, Lacework, Synk	Blockchain, Seguridad Endpoint, IAM, Seguridad Cloud

La pandemia también ha sido de gran ayuda al impulsar el trabajo en remoto y la adopción de la nube, lo que ha obligado a las empresas a revisar las tecnologías de seguridad implantadas

pública como la columna vertebral de la infraestructura de la empresa. Sencillamente, las soluciones de seguridad heredadas y las herramientas de configuración y monitorización de redes no tienen la escalabilidad y la automatización necesarias.

Según Dell'Oro Group el mercado de SASE crecerá a más de 5.000 millones anuales para 2024, como resultado de su impulso establecido, acelerado por el cambio al trabajo remoto durante la pandemia. Los sectores de seguridad cloud y de red son los más beneficiados de este impulso.

La incorporación de la seguridad en el ciclo de desarrollo, o DevSecOps, también está generando enormes oportunidades "para vender aplicaciones de seguridad a los desarrolladores de software", dice el informe, que recoge un crecimiento medio anual del 29% entre 2020 y 2025, pasando de generar 1.800 a 6.500 millones de dólares.

Explica Momentum Cyber que el mercado de DevSecOps está muy fragmentado en múltiples soluciones puntuales que se conectan a fases específicas del SDLC (Software Development Life Cycle) y que "existe una gran oportunidad para consolidar a los proveedores de servicios e integrar horizontalmente sus soluciones en una única plataforma unificada.

Mercado IAM

Como se ha comentado, el sector de Gestión de Identidades y Accesos (IAM – Identity and Access Management) no sólo ha liderado las inversiones, sino que se ha colocado en segunda posición en cuanto al volumen alcanzado en fusiones y adquisiciones. Es uno de los segmentos donde más se está viendo un proceso de consolidación, con CyberArk adquiriendo Idaptive, Okta comprando ScaleFT y Auth0, Ping adquiriendo UnboundID y Symphonic, o Thycotic y Centrify uniéndose.

El mercado de Gestión de Identidad y Acceso crece una media anual del 14,5%, desde los 12.300 millones en 2020 a 24.100 millones para 2025, según datos de MarketsandMarkets.

El aumento en la demanda de soluciones de gestión de identidades, junto con las de control de accesos privilegiados PAM (Privilegede Access

Enlaces de interés...

- Noticias de las últimas adquisiciones del sector
- Momentum Cyber
- El mercado de ciberseguridad europeo alcanzará 22.670 millones de dólares en 2027
- La necesidad de mejorar la seguridad impulsa el mercado de servicios gestionados

Lo que va de año acumula nueve acuerdos de fusiones y adquisiciones que han superado los mil millones de dólares

Management), se ha visto impulsado por la necesidad de las organizaciones de proteger a los empleados en un modelo de teletrabajo adoptado de manera acelerada por la pandemia.

Dar a los empleados diferentes contraseñas para diferentes aplicaciones y redes genera un montón de llamadas al servicio de asistencia técnica. Con cada vez más servicios accedidos a través de la nube, la multitud de sistemas y aplicaciones que requieren autenticación para el acceso hace que la gestión de identidades se haya convertido en un elemento clave que debería estar en la agenda de todas las empresas.

Con los ciberdelincuentes buscando credenciales de acceso privilegiado que permitirían el movimiento lateral, la adopción de soluciones de doble o múltiple factor de autenticación (2FA - MFA) está creciendo. MFA requiere dos factores para acceder a los recursos que los empleados necesitan, ya sea en una Mac, una PC con Windows o un teléfono inteligente. Un factor podría ser una contraseña y otro podría ser una notificación de inserción móvil, SMS (texto), llamada telefónica o llavero. La simplificación del acceso mejora la productividad de los empleados y del personal de TI. Es muy eficiente y una capa adicional de seguridad.

Compartir en RRSS

La documentación TIC, a un solo clic

Identificación de ataques web

Los equipos de seguridad de las empresas se enfrentan a diferentes tipos de ataques de alto riesgo contra sus organizaciones. La pregunta es, ¿cómo pueden reconocer los cuatro tipos de ataques más peligrosos? Este documento ayuda a identificar los ataques tales como relleno de credenciales, uso indebido de una API, inyección de SQL y vulnerabilidades de la lógica de negocio.

La hoja de ruta de DevOps en materia de seguridad

Las compañías, buscando agilidad, flexibilidad y reducción de tiempos para llevar sus aplicaciones al mercado, han apostado por DevOps, pero ¿es esta decisión un buen paso cuando hablamos de seguridad? Este documento nos muestra que, cuando una organización gestiona bien DevOps, consigue reforzar la estrategia de seguridad en todos los aspectos.

Microsegmentación, clave para seguridad empresarial

Este estudio, realizado por IT Digital Security para Zscaler, aporta la visión que los profesionales de la ciberseguridad tienen acerca de la microsegmentación, qué viene a solucionar, qué beneficios aporta, qué características deben tener las soluciones que lo permitan o cómo impacta en la seguridad.

Tendencias tecnológicas de alto impacto para tu negocio

Las empresas se encuentran con una nueva oleada de recursos tecnológicos que les están permitiendo definir nuevos modelos de negocio, entender mejor a sus clientes o expandir los límites de su actividad. En este informe, hemos seleccionado las principales innovaciones tecnológicas que están transformando el mundo de los negocios tal y como lo entendemos hoy en día.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
SPAIN CHAPTER

CONCEPCIÓN CORDÓN FUENTES

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN
Es Ingeniera Informática por la Universidad de Málaga y Directora de Seguridad por La Universidad Pablo de Olavide de Sevilla (UPO). Tiene más de 32 años de experiencia en diferentes campos relacionados de la ciberseguridad y la protección de datos. Desde 1989 trabaja en la Empresa Municipal de Aguas de Málaga, EMASA, con responsabilidad en distintas áreas (Comunicaciones y Redes, Seguridad integral, Continuidad del Negocio, Infraestructuras Estratégicas, Gestión de Riesgos, Protección de Datos, Transparencia, Seguridad Física)
Miembro del Comité de Expertos Independientes para la elaboración de la Estrategia Nacional de Ciberseguridad 2019
Concepción Cordón Fuentes es, además, profesora colaboradora en varias universidades y Escuelas de Negocios y muy activa en ponencias, actividades y publicaciones relacionadas con la Ciberseguridad, Transformación Digital, Innovación, Protección de Datos y Equidad de género. Es miembro del Consejo de Women4Cyber Spain, el capítulo nacional dependiente de la Fundación Women4Cyber de la European Cyber Security Organization (ECSO).

Compartir en RRSS

Privacidad y Ciberseguridad: hasta que la ciberdelincuencia nos separe

Después de este período estival, y para ir entrando poco a poco en "faena", me he permitido el lujo de usar un estribillo de una de las canciones del verano, de "aquellos maravillosos y añorados veranos", donde se disfrutaba al aire libre al son de la música sin restricciones, bailando en las noches cálidas del periodo estival...

El tema en concreto es "El anillo", de Jennifer López, más conocida, por la repetición una y otra vez del estribillo, con el nombre "El anillo pa cuando..." (sin que esto quiera reflejar mis preferencias musicales, para lo cual hubiera escogido "Verso suelto", una de las últimas composiciones de "De Vuelta", el proyecto musical de nuestro colega Luis Fernández).

Antes del pegadizo estribillo, la frase completa y que me hizo reflexionar para escribir este artículo es:

"Ya lo tengo todo, pero, "el anillo pa cuando"...

Precisamente esto sintetiza justo lo que está ocurriendo en las organizaciones con la y Privacidad y Ciberseguridad: les hace falta un "compromiso formal", aceptado por los responsables de ambas áreas.

Privacidad y Ciberseguridad ya van de la mano, son inseparables, no deben entenderse como enemigas, si una gana la otra pierde

Los inicios

Es habitual encontrar en las entidades departamentos enteros, en mayor o menor medida, trabajando cada uno por su cuenta, como si estuviesen jugando en distintas competiciones, en ligas diferentes (estamos en época de fichajes..., y ya se han cerrado algunos de ellos muy sustanciosos...).

Así encontramos Planes directores de Seguridad, Análisis de Impacto del Negocio, Planes de Continuidad de Negocio, Compliance, Códigos Éticos, Políticas de Privacidad, Políticas de Clasificación y Tratamiento de la Información, Procedimientos de Gestión y Notificación de Brechas de Seguridad, Procedimientos de Gestión y Notificación de Ciberincidentes, Planes de Seguridad de Operador (PSO) y Planes de Protección Específicos(PPE) para aquellos organismos y empresas que han sido designados Operadores Críticos, Declaración de Aplicabilidad de medidas de seguridad para los Operadores de Servicios Esenciales (OSE), Certificaciones de conformidad con distintas normas nacionales e internacionales....

Al hilo de la letra de la canción, las entidades, con las herramientas anteriormente descritas, “pueden tenerlo todo...”, o casi todo, para implementar una adecuada Privacidad y Ciberseguridad, sin embargo, siguen sin proteger adecuadamente sus activos, el core de sus negocios, faltando una adecuada interacción entre ambas.

El compromiso

Ya es hora de que las empresas consientan esta unión entre la Privacidad y la Ciberseguridad, es el paso definitivo que deben dar, ya sean públicas o privadas, para conseguir una Seguridad Integral capaz de afrontar los desafíos de una sociedad digitalizada donde la información y los datos personales son los ejes que mantienen la rueda que hace girar al mundo.

Un mundo que, por otro lado, busca la sostenibilidad en una sociedad de economía circular, que intenta aprovechar al máximo los recursos, y por supuesto las sinergias entre los mismos.

Formalizando el compromiso

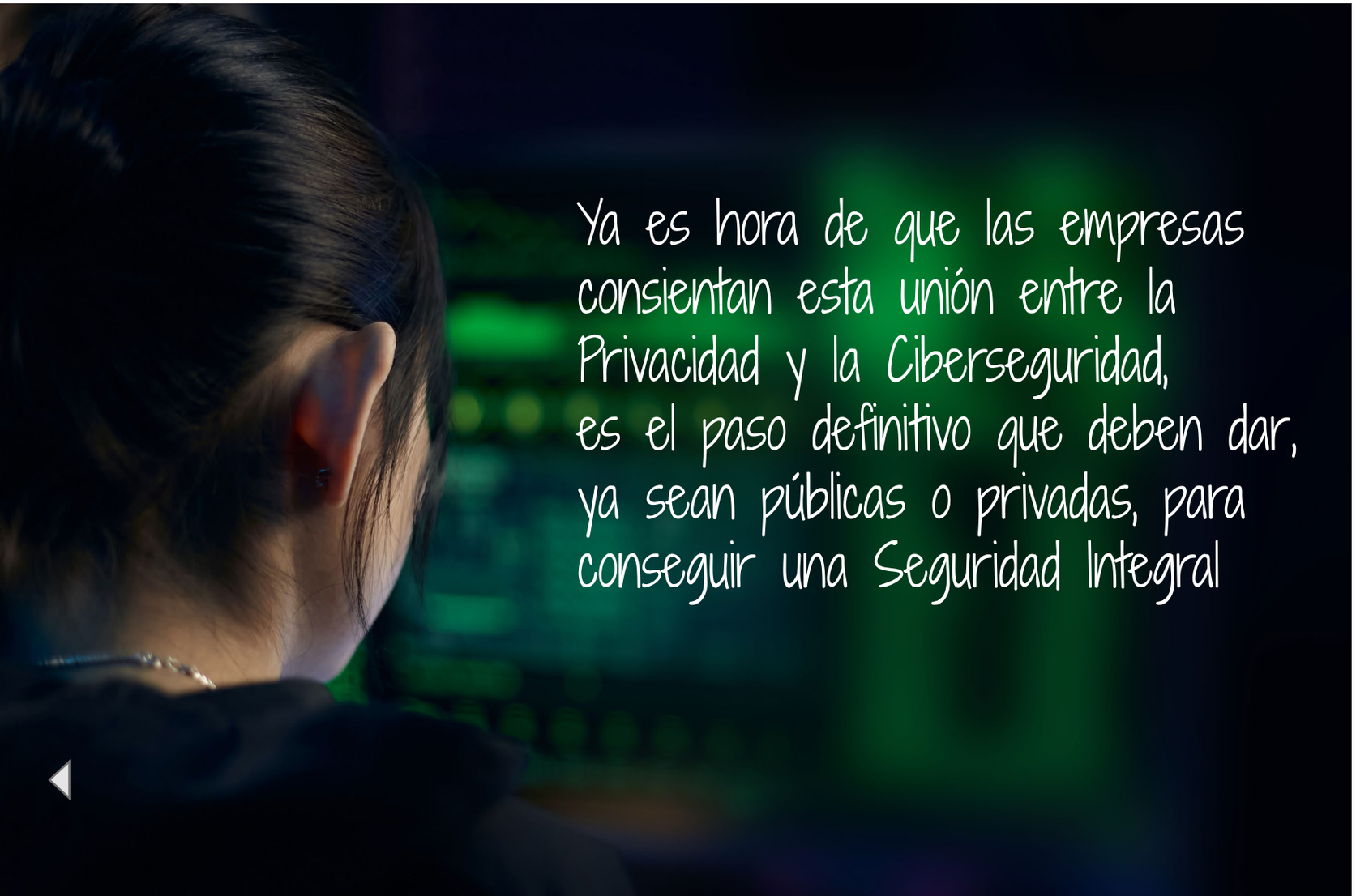
¿Qué nos impide aceptar esta interconexión?

En verdad tenemos “casi todo” para no poner obstáculos e ir formalizando este compromiso.

La pareja tiene mucho en común para que se entiendan y emprendan un camino único, acompañados, complementándose, protegiéndose mutuamente y haciendo fuerte y robusta su casa.

Además, el viento sopla a favor...

Con las últimas normativas establecidas tanto a nivel nacional como europeo, poco a poco se han ido engranando las piezas del ecosistema digital, acercando posturas entre ambos ámbitos.



En España, la legislación en la administración electrónica se consolidó con el Esquema Nacional de Seguridad (ENS) que ha resultado ser la herramienta perfecta para mejorar la seguridad de las TICs en la Administración pública, y cuya influencia ha ido creciendo, llegando hasta los proveedores que trabajan con las mismas, y al número de entidades y sistemas que están dentro del ámbito subjetivo de la ley. En breve se publicará el nuevo Esquema Nacional de CiberSeguridad, aprovechando la experiencia adquirida en estos años.

La normativa de Protección de Infraestructuras Críticas, ley PIC, del 2011, sentó las bases para dotar de seguridad a las infraestructuras críticas que soportan servicios esenciales, mejorando y aumentando los sectores de aplicación que la Directiva europea proponía, algo que ha sido relevante para agilizar la aplicación de otras directivas relacionadas y que actualmente también está siendo revisada.

En cuanto a la Privacidad, ya se avanzó bastante con el cambio de paradigma que el Reglamento General de Protección de Datos (RGPD) inculcó, centrándose en la “seguridad del dato personal”, con enfoque de gestión de riesgos para dotar de las medidas adecuadas en aras de una mejor protección de los datos personales, y, por ende, de la privacidad.

Así mismo, la que busca mejorar la seguridad de las redes y sistemas de comunicaciones de los servicios esenciales, se convirtió en España en la primera Ley de Ciberseguridad, RD-12/2018 propiamente dicha con su reciente reglamento de desarrollo, RD-43/2021. La NIS.2 ya está gestionándose.

Todas estas directivas culminaron a finales del 2019 con distintas estrategias europeas encaminadas al aseguramiento del ciberespacio, siendo sin duda, la Covid-19, la aceleradora para que se convenciese al más escéptico de los implicados, dirigiendo todas las miradas en la Ciberseguridad

como tabla de salvación de la sociedad debido a la “digitalización por inmersión” a la que el mundo entero se ha visto abocado.

Y en plena crisis, compañera inseparable de la Ciberseguridad ha sido la Privacidad, debido al considerable aumento de la información que navega entre las redes, con un alto porcentaje de datos de carácter personal.

Esto se debe no sólo al uso del teletrabajo, sino a la inmensidad de trámites que se han habilitado de manera telemática debido a la imposibilidad de movilidad de los ciudadanos por las restricciones impuestas por la crisis mundial.

Preparativos para el enlace

Una vez que tenemos el convencimiento de que esta unión ha de ser, debe serlo “para toda la vida”, por eso, hay que ponerse manos a la obra, estableciendo una estrategia a corto plazo e ir mejorándola progresivamente.

Quizás, tal y como ha pasado en el último año, el enlace se ha tenido que retrasar, a cambio hemos ganado en abundancia de instrumentos reguladores que poco a poco van diseñando las condiciones que se deben dar para que el maridaje sea perfecto.

De hecho, todas las normativas y estrategias están siendo revisadas y se ha acelerado su revisión.

El maestro de ceremonia

Este puede ser un punto de escollo importante, ya que sobre él recaerá toda la responsabilidad de

haber sabido dotar de una adecuada organización y estructura para conseguir el éxito.

Más allá del nombre que se le ponga, CISO, RSI, RSE, DPO, CIO, CMR, CTO..., debe ser alguien con visión estratégica, mando ejecutivo, habilidad de trabajo en equipo, que no le tiemble el pulso cuando tenga que poner encima de la mesa propuestas que sabe no van a gustar pero son necesarias, etc..., en definitiva, alguien (no tiene que ser figura única, pueden ser comités) que dirija y coordine todas las acciones necesarias para conseguir un único objetivo común, haciendo que todos remen en la misma dirección, aprovechando ese viento a favor.

El enlace

Privacidad y Ciberseguridad ya van de la mano, son inseparables, no deben entenderse como enemigas, si una gana la otra pierde. De esta manera es un "win to win", uno de los siete principios de la denominada Privacidad por Defecto (PbD) que el RGPD ha impulsado, llevándola a la máxima expresión con las metodologías que implementan Seguridad y Privacidad por Defecto y por Diseño, para que desde el principio de los procesos estén integradas la Privacidad y la Ciberseguridad.

Enlaces de interés...

- Nos preocupa la privacidad de los datos, pero los compartimos a cambio de servicios gratuitos - 29 JUL 2021
- La UE se propone avanzar en un enfoque armonizado de la seguridad y la privacidad

En este sentido concluyeron, siguiendo con los clásicos del verano, dos de los cursos impartidos por la Fundación de la Universidad de Málaga (FGUMA), uno dedicado a la Privacidad,, y otro sobre Ciberseguridad.

Ambos cursos perseguían el mismo fin: el bienestar del individuo en la sociedad digital.

Reflexión final

¿Qué debemos hacer, ciudadanos, organismos reguladores, empresas, estados, para llevar a buen término el que la Privacidad y la Ciberseguridad sean una pareja bien avenida y duradera, uniendo esfuerzos para combatir con el mayor de sus peligros, la ciberdelincuencia?

¡Apostemos por ello!!

Con las últimas normativas establecidas tanto a nivel nacional como europeo, poco a poco se han ido engranando las piezas del ecosistema digital, acercando posturas entre ambos ámbitos

it User
TECH & BUSINESS

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

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la CiberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

Compartir en RRSS

it Digital Security

Tribuna Ciberseguridad 4.0

El Amanecer de la Humanidad Digital III:

Sueño de Verano 2021, disrupción digital, genética y conciencia

El verano con sus noches cortas pero deliciosamente cálidas y sus cielos casi siempre sin nubes nos permiten disfrutar de las estrellas invitando a nuestra imaginación a volar en ese infinito universo que nuestros pobres ojos solo ven en un estrecho margen de frecuencias pero que los avances tecnológicos nos han hecho saber que tienen una belleza inconmensurable.

El verano, que con su esplendor nos invita a soñar sobre sobre lo mundano y lo divino, sobre lo simple y lo complejo produciendo ideas o especulaciones que nos pueden parecer exageradas cercanas incluso en los límites de la razón, pero que yo me resisto a no compartirlas aunque tal vez tengan más de deseo que de viabilidad.

Antes del verano, en el Amanecer de la Humanidad II hice una disquisición respecto a la Disrupción Digital Global y el impacto de cambio que tendrá en la humanidad en los próximos 80 años llevándonos a un siglo XXII donde todo o casi todo lo que conocemos ahora será diferente, muchas de las cosas habituales de ese nuevo siglo no las conocemos ni las podemos imaginar siquiera, muchas de las cosas habituales ahora habrán desaparecido y solo las recordaremos en los libros de historia y aquello que permanezca habrá cambiado tanto que si pudiéramos viajar en el tiempo no las reconoceríamos.

Estoy convencido que la gran disrupción digital en el siglo XXI hará que el amanecer de la Humanidad Digital será luminoso y hermoso, como el primer gran paso evolutivo de la Humanidad Digital hacia avances aún mayores en los siglos venideros.

En este sueño de verano, la gran disrupción digital no es más que un pequeño paso de un sueño aún más profundo y a más largo plazo que yo me he atrevido a denominar la Gran Disrupción Genética que como no podía ser menos ya está en marcha aunque muy poca gente aún la considere en todo su potencial

Septiembre 2021

Quiero creer que los nuevos ciudadanos que nacerán en sociedades en muchos casos ya incomprensibles para sus antecesores, serán capaces de evolucionar sistemas y organizaciones obsoletas

Este verano, en una tarde/noche cálida de ir saltando de link en link por el espacio virtual, se cruzó delante de mí una noticia perdida en la inmensidad de la información que diariamente se produce en la actualidad, la publicación de un libro con el nombre de **The Next 500 Years: Engineering Life to Reach New Worlds,** cuyo autor es Christopher Mason genetista y biólogo computacional que ha sido investigador principal y co-investigador de siete misiones y proyectos de la NASA. Un artículo corto, publicado en la revista QUO, extrae información de ese libro y describe "las fases para llegar a conseguir humanos biológicamente adaptados a otros mundos, que voy a replicar en este artículo:

- **Fase 1.** Ya completada, entre 2010 y 2020, es un estudio detallado del genoma humano.
- **Fase 2. 2020-2040:** desarrollo de la ingeniería genética, por ejemplo, con la inserción en las células humanas de un gen conocido por promover la protección contra la radiación en los tardígrados, criaturas microscópicas que destacan por su extraordinaria capacidad de recuperación.
- **Fase 3. 2041-2100:** mejorar nuestras defensas genómicas contra la radiación espacial. Este es el período, escribe Mason, en el que «todos los genes, células e incluso potencialmente los órganos de cualquier organismo pueden convertirse en un componente de una célula humana».
- **Fase 4. 2101-2150:** la comprensión del genoma humano hará que todo el que nazca tenga su ADN editado, con todas las mejoras conseguidas, entre ellas, la de estar preparados para un entorno radiactivo.
- **Fase 5. 2151-2200:** el transporte entre la Tierra y las bases espaciales estará disponible para quienes la deseen.
- **Fases 6. 2201-2250:** haremos que los humanos sean tolerantes a condiciones cada vez más extremas.
- **Fase 7. 2251-2350:** la gente vivirá en colonias marcianas completamente desarrolladas, los viajes interestelares intergeneracionales pueden ser

posibles y el ADN de las formas de vida recién descubiertas podría potencialmente ser secuenciado y utilizado para refinar aún más nuestros genomas.

- **Fase 8. 2351-2400:** asentamiento en exoplanetas, en otros sistemas solares.
- **Fase 9: 2401-2500:** los seres humanos controlarán la edición del genoma, y les permitirá combinaciones con el de todo tipo de criaturas. Habremos dominado nuestra evolución.

Y algo aún más maravilloso de este proceso, "los humanos biológicamente adaptados para vivir en otros planetas tendrán también el control biológico de la felicidad".

Claro está que todos estos avances estarán también a disposición de la humanidad que decida permanecer en este nuestro primigenio planeta Tierra, así pues podemos pensar que el control biológico de la felicidad será uno de los más grandes logros de la Genética para la humanidad futura.

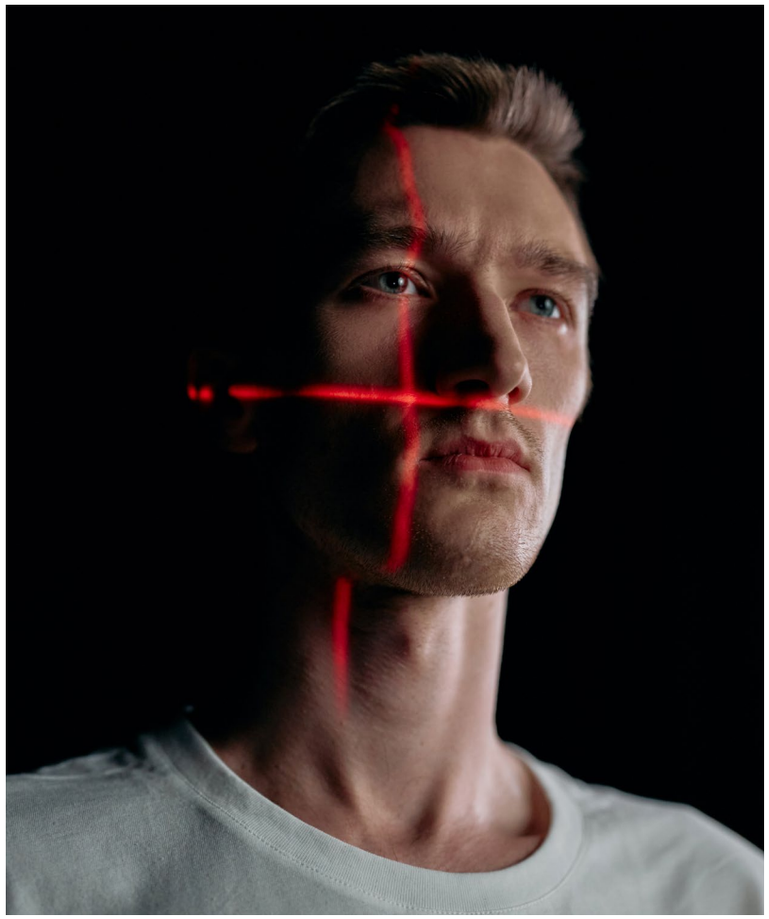
Sabemos por las experiencias pasadas que cuando una ciencia o tecnología avanza lo hace independientemente de la velocidad a las que avancen otras ciencias o tecnologías necesarias, pongamos el ejemplo cercano de aventura espacial, que nació del desarrollo de motores para impulsar cohetes y misiles balísticos que transportaban bombas a largas distancias, pero mediante el uso con fines pacíficos de estas tecnologías permitió el inicio de la era espacial de la humanidad sin apenas conocimientos de los efectos biológicos que los viajes espaciales tenían sobre los primeros astronautas.

Ocurre que mientras que las tecnologías de motores para impulsar naves espaciales va evolucionando en la actualidad con una velocidad lineal, la Genética ha tomado en el sigo XXI una velocidad exponencial, al igual que todo lo relacionados con lo digital, como la biología computacional.

Esto me hace pensar que el control de la edición de nuestro genoma y, por ende, el llegar a dominar nuestra evolución ocurrirá mucho antes del asentamiento de colonias en exoplanetas e incluso antes del establecimiento de colonias estables en planetas cercanos como Marte.

No veo cercana, ni siquiera en plazos de siglos, la evolución de motores que nos permitan impulsar naves a facciones considerables de la velocidad de la luz que es lo que se necesita para hacer viajes interestelares aunque tengan que seguir siendo intergeneracionales incluso a velocidades cercanas a la de la luz.

> Mientras que las tecnologías de motores para impulsar naves espaciales va evolucionando en la actualidad con una velocidad lineal, la Genética ha tomado en el siglo XXI una velocidad exponencial



Sabemos por las experiencias pasadas que cuando una ciencia o tecnología avanza lo hace independientemente de la velocidad a las que avancen otras ciencias o tecnologías necesarias

Tal vez la combinación de la Inteligencia Artificial con su crecimiento exponencial y la mejora genética de la Inteligencia Humana, también exponencial, en nuestros descendientes tenga la capacidad de encontrar los medios para conseguir motores interestelares cercanos a la velocidad de la luz para poder realizar esos viajes interestelares e intergeneracionales para llegar a otras galaxias en el siglo XXIII habiendo dominado ya nuestra evolución.

Qué maravilla poder soñar con haber llegado a dominar nuestra propia evolución como especie y tener el control biológico de la Felicidad.

Me he atrevido a pensar que cuando hayamos llegado a este grado de evolución, necesitaremos algo más, la evolución de la Conciencia Humana, que ya entrados en el siglo XXI podemos ver que evoluciona de manera lineal, siempre por detrás de los avances de las revoluciones industriales, de los cambios que se producen por tecnologías emergentes que rápidamente son dominantes, de ciencias como la genética y de disrupciones como las Digitales que crecen de manera exponencial.

Con el nivel de conciencia individual actual solo podemos aspirar a un nivel de Conciencia Colectiva de la Humanidad que no está a la altura del grado de desarrollo tecnológico y científico que ha alcanzado la humanidad en la tercera década del siglo XXI.

En mi sueño, donde los avances de la Sociedad Digital y la Genética han llevado la Humanidad a un grado de desarrollo donde la humanidad tendrá el control biológico de la felicidad y el dominio de nuestra evolución, solo es compatible con la evolución de la Conciencia Colectiva al mismo nivel de los otros avances de la Humanidad futura con su correspondiente evolución de las Conciencias Individuales. Quien y como hará posible la evolución de las Conciencias Individuales de las generaciones futuras, descendientes de bajo nivel que Conciencia Colectiva e Individual del que “disfrutamos en la actualidad”.

Enlaces de interés...

- Humanos modificados genéticamente vivirán en otros planetas en 500 años

Quiero creer que los nuevos ciudadanos que nacerán en sociedades en muchos casos ya incomprensibles para sus antecesores, serán capaces de evolucionar sistemas y organizaciones obsoletas y desarrollar nuevos modelos de participación ciudadana, nuevos modelos de reparto, nuevos modelos de organizaciones políticas donde los viejos paradigmas serán reemplazados por participación digital universal eliminando los viejos y caducos modelos de liderazgos individuales y, por supuesto, haciendo desaparecer no solo las democracias representativas sino también cualquier otro modelo pseudo-representativo como las dictaduras ideológicas, religiosas, económicas o simplemente individuales. No encuentro palabras para describir la Conciencia Colectiva e Individual del futuro que acompañe dignamente a la Humanidad Digital, Genética y neo Consciente que he soñado en este verano de 2021.

it Digital Security
Tribuna Marketing y Consumo

Reinventar la normalidad de los sistemas de pago

JOSÉ MANUEL NAVARRO

CMO MOMO GROUP

José Manuel Navarro Llena es experto en Marketing. Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

Compartir en RRSS

Una revisión de las tres últimas encuestas (2018-2020) realizadas por el Banco de España sobre el uso del efectivo a nivel nacional, revelan interesantes datos sobre el comportamiento de los ciudadanos en relación con la utilización de los medios de pago digitales (sobre todo con las tarjetas financieras). Podemos verlo en la tabla.

Aunque es evidente el descenso producido en las preferencias del uso de efectivo en los últimos años (desde un 80% en 2014 hasta un 39,5% en 2020), es en este último cuando se experimenta un diferencial a la baja realmente importante debido a los efectos que la pandemia de la Covid19 ha ejercido sobre los hábitos de consumo de las personas. El confinamiento y el miedo al contagio han impulsado la utilización de los medios de pago digitales y el comercio electrónico, aunque no se observa por ejemplo un paralelismo entre los 17,1 puntos de caída del efectivo y los 11,1 puntos de incremento de la tarjeta de débito (período 2018-2020), sobre todo si tenemos en cuenta que la costumbre de llevar dinero físico en el bolsillo (hasta 50€) se sigue manteniendo en un porcentaje muy alto (casi del 90%).

La aceleración de la economía hacia sistemas estrictamente digitales facilitará que se difuminen las tradicionales líneas divisorias entre la industria de pagos, el sector del comercio y las entidades financieras creando un ecosistema único

Es curioso contrastar, en los tres últimos años, el crecimiento en la aceptación del pago con tarjetas de crédito/débito (8% y 12%, respectivamente) por parte de los comercios, con el incremento de visitas a las sucursales bancarias más cercanas para solicitar cambio de efectivo (casi un 24%). Es posible que esto sea debido a que las compras de pequeños importes se mantengan en metálico, de ahí la necesidad de disponer de moneda fraccionaria, si bien la media de los pagos con tarjeta también ha descendido de 106€ a 52€. Aunque por los datos de las encuestas no es posible establecer el límite del precio por el que un consumidor prefiere pagar con tarjeta o con efectivo, o por el que un comercio acepta o no el pago con tarjeta (los mínimos han tendido a desaparecer por el ajuste a la baja de las comisiones de descuento que aplican las entidades financieras), podríamos imaginar que aquél se encuentra en los 50€; este dato podría favorecer posibles estrategias de precios por parte de los comercios minoristas, si se tienen en cuenta además los motivos de los consumidores para seguir usando el efectivo: mayor comodidad, les permite un mejor control del gasto, rapidez en la transacción y menor coste.

A estas razones habría que sumar la libertad, el anonimato y la universalidad del efectivo como medio de pago, el cual no depende además de tecnologías ni de infraestructuras dedicadas para cerrar una transacción. Por ello, el 26,4% de los pequeños comercios siguen prefiriendo cobrar en efectivo, el 40% de los consumidores no considera usar o incrementar el uso de los medios digitales en un futuro próximo y solo el 2,5% de la población declaró que habían dejado de usar el efectivo por motivos de higiene a causa de la pandemia (hecho que viene refrendado por el estudio publicado por el BCE, en el que evidencia que los billetes y monedas no son vector de transmisión de la enfermedad).

Hace tiempo que, desde diferentes foros especializados, se está vaticinando el final del efectivo e, incluso, se apunta 2030 como la fecha de su desaparición definitiva; este hecho estaría propiciado por las nuevas soluciones de pago, por la emisión

de moneda digital por parte de los bancos centrales y por la restricción a 1.000€ del límite máximo para compras en efectivo que establece la nueva Ley contra el Fraude Fiscal. No obstante, veamos de qué soluciones se está hablando para justificar su desaparición apoyándose en la idea de que la tecnología podrá generar, además, nuevas oportunidades de negocio mediante transacciones que mejoran la experiencia de cliente a través de la personalización del proceso de compra en un ecosistema que deberá ser omnicanal.

Las tendencias del mercado y la urgencia de su transformación digital sugieren soluciones que aúnen los intereses de comercios y consumidores priorizando la rapidez, eficacia, conveniencia y seguridad de los procesos de compra. En este sentido y gracias a las necesidades que ha revelado la situación de confinamiento, se están consolidando opciones que ya estaban operativas y otras que han surgido como respuesta a esas nuevas demandas y a las opciones que permite la Directiva Europea de Servicios de Pago (PSD2), tanto para la integración de los pagos minoristas en la UE como para la aplicación de medidas de autenticación reforzada:

- **Biometría.** Ya conocida y rodada por diferentes compañías para identificación y pago mediante reconocimiento facial, retiniano o dactilar, ahora se suma la voz para la verificación del pago y la asistencia en los procesos de comercio electrónico.
- **Sistemas contactless resueltos por las propias tarjetas NFC,** los monederos electrónicos (eWallet) y los dispositivos wearables. Son ya conocidos y su uso se ha disparado desde el primer momento de la pandemia.
- **Códigos QR (fijos y dinámicos).** Ha sido el método que más se ha popularizado como medio para acceder a información alojada en la nube y evitar el uso de soportes impresos, pero también se ha adoptado rápidamente para procesar pagos en comercio físico con aplicaciones móviles (Alipay y WeChat son los que más han extendido su

Variable	2018	2019	Dif. 19-18	2020	Dif. 20-19	Dif. 20-18
Uso de efectivo	53,0%	53,0%	0,0%	35,9%	-17,1%	-17,1%
Uso efectivo por edades						
> 64 años	70,8%	76,7%	5,9%	53,0%	-23,7%	-17,8%
55-64 años	53,6%	49,3%	-4,3%	25,3%	-24,0%	-28,3%
45-54 años	42,9%	30,9%	-12,0%	25,1%	-5,8%	-17,8%
35-44 años	39,0%	41,4%	2,4%	27,5%	-13,9%	-11,5%
25-34años	47,0%	47,1%	0,1%	30,8%	-16,3%	-16,2%
18-24 años	85,8%	82,2%	-3,6%	60,3%	-21,9%	-25,5%
Uso tarjeta de débito	43,0%	41,0%	-2,0%	54,1%	13,1%	11,1%
Billetes y monedas en el bolsillo (<50€)	89,0%	91,0%	2,0%	88,5%	-2,5%	-0,5%
No considera usar MP digitales en un futuro	80,0%	70,0%	-10,0%	40,0%	-30,0%	-40,0%
Uso de cajero automático para disposición efectivo	83,0%	74,0%	-9,0%	84,0%	10,0%	1,0%
Comercios que aceptan efectivo	99,2%	99,5%	0,3%	99,3%	-0,2%	0,1%
Comercios que aceptan tarjeta débito	81,0%	87,0%	6,0%	93,0%	6,0%	12,0%
Comercios que aceptan tarjeta crédito	74,0%	78,0%	4,0%	82,0%	4,0%	8,0%
Comercios que aceptan pago con móvil	--	40,0%	--	50,0%	10,0%	--
Comercios que acuden al banco a solicitar cambio	57,0%	49,0%	-8,0%	80,9%	31,9%	23,9%

Fuente: Banco de España. Encuesta nacional sobre el uso efectivo (2018, 2019, 2020)

Es indudable que los pagos digitales seguirán mejorando su eficiencia y, por tanto, creciendo en todos los ámbitos y geografías, aunque para ello deberán superar dos importantes barreras

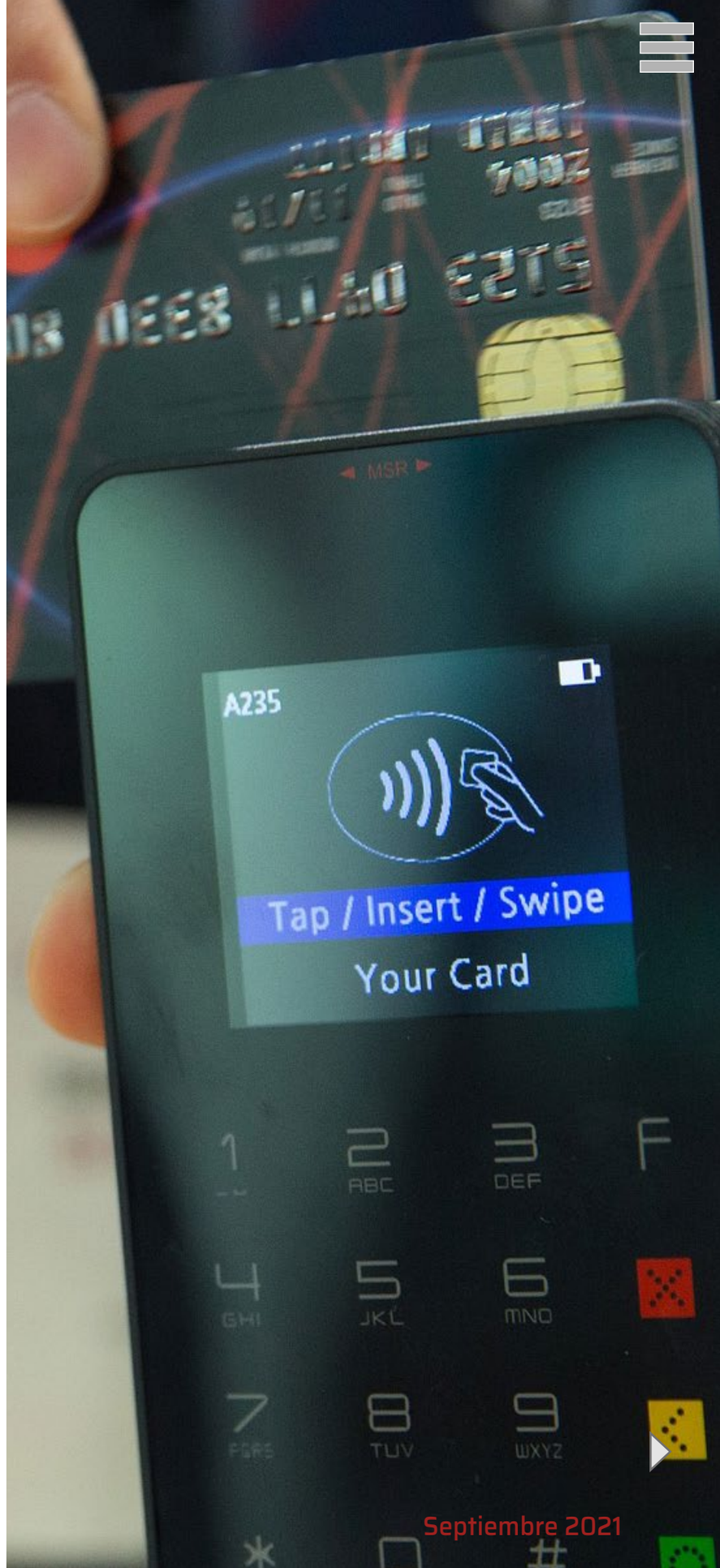
No estamos en el momento de augurar el futuro de cada modelo sino en el de construir el mejor escenario para que cada persona ejerza libremente la elección del sistema que más le convenga

implantación) y para completar algunas transacciones financieras.

- **Pagos P2P.** Es el método que mejor se ha posicionado para resolver el envío inmediato de dinero entre los usuarios de aplicaciones financieras móviles, pero también ha sido el que más ha crecido para resolver el cobro de las compras en pequeños comercios y de los servicios prestados por autónomos a particulares. El mejor ejemplo de su rápido crecimiento en España ha sido Bizum.
- **Pagos mediante enlace (MOTO y Pay-by-link).** La pandemia los ha extendido entre pequeños comercios locales y sin experiencia digital, pero el envío de los datos de pago a través de mail, sms o Whatsapp ha permitido el incremento de fraude en estas operaciones por su débil sistema de autenticación (no requieren PIN).
- **Social Payments.** Las redes sociales han sido el gran escaparate para muchos comercios para dar difusión a sus productos y servicios, pero también se han convertido en el canal principal para su venta con el sistema “one click”, sobre todo para marcas con dificultades para posicionarse en grandes marketplaces o para pequeñas empresas con sistemas de producción o distribución limitados.

La proliferación de nuevas soluciones es un síntoma claro de la rápida evolución de la tecnología para dar respuesta a lo que puede ser un nuevo escenario para la industria de los medios de pago tras los efectos de la pandemia en la conducta de los consumidores. Pero poner el foco exclusivamente en los sistemas electrónicos sin contacto o en ingeniosas soluciones de autenticación, puede resolver cuestiones como la seguridad, ubicuidad y versatilidad de las transacciones, pero no alcanza a los pagos en efectivo en cuanto a inmediatez y simplicidad. Atributos de lo que se ha denominado RTP (Real Time Payments), que reclaman la mayoría de las empresas para garantizar el cobro inmediato y el control de la información asociada al flujo de los fondos.

Es indudable que los pagos digitales seguirán mejorando su eficiencia y, por tanto, creciendo en todos los ámbitos y geografías, aunque para ello deberán superar dos importantes barreras: la adaptación de los sistemas heredados de la mayoría



Enlaces de interés...

- Encuesta uso efectivo en España, Banco de España
- El uso de efectivo no es un vector de transmisión de Covid-19
- W PSD2

de los comercios (grandes y pequeños) a los requerimientos de las nuevas fórmulas y medios de pago y, la segunda, equiparar las funcionalidades de anonimato y libertad de uso que tiene el efectivo. Derribar la primera barrera será cuestión de tiempo e inversión; la segunda sólo podría serlo por las criptomonedas, si bien éstas tienen otros aspectos en contra (falta de regulación, exigencia de conocimiento del funcionamiento de los mercados de valores y de habilidades en el uso de los entornos digitales basados en blockchain, alto riesgo de robo/pérdida de claves, alta volatilidad del mercado, refugio para blanqueo de capitales, elevados índices de fraude,…) que harán difícil un uso generalizado para compras y pagos entre particulares.

La aceleración de la economía hacia sistemas estrictamente digitales facilitará que se difuminen las tradicionales líneas divisorias entre la industria de pagos, el sector del comercio y las entidades financieras (convencionales y fintech) creando un ecosistema único que, no podrá evitarlo, tendrá que seguir teniendo en cuenta las transacciones en efectivo para equilibrar con sutileza la oferta y la demanda de los servicios de pago, para entregar al consumidor no ya la mejor experiencia de cliente, sino la más adecuada y acertada en el momento que toma una decisión de compra, precisa compartir gastos o realizar un envío de dinero. No estamos en el momento de augurar el futuro de cada modelo sino en el de construir el mejor escenario para que cada persona ejerza libremente la elección del sistema que más le convenga.