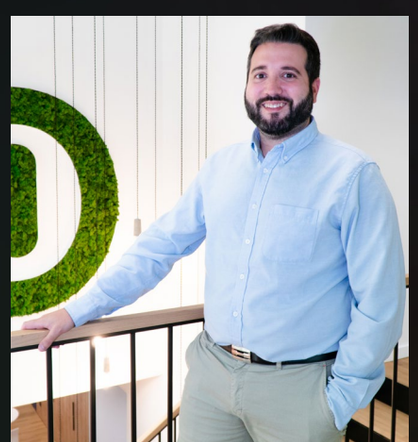
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Enero 2022 - nº 48

Tecnologías de ciberseguridad que no debes perder de vista en 2022



‘Lo importante no es tanto la solución o producto, sino el proveedor’ (Roberto González, Grupo Primavera)

‘Galaxy es la gran apuesta de CyberRes para devolverle el brillo a Arcsight’ (Ramsés Gallego, CyberRes)

HelpSystems ha tomado la importante decisión de enfocarse en ciberseguridad (Paolo Cappello, HelpSystems)

Ciberseguridad, ¿un mercado infravalorado?

ITTrends METAVERSO: el espacio virtual que liderará la nueva revolución digital

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

it Digital Security

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

it Digital MEDIA GROUP

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

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

Tecnologías de ciberseguridad que no debes perder de vista en 2022

Este año veremos más ataques. El ransomware se volverá más osado; el phishing más perfeccionado; el modo de trabajo será híbrido; los datos, el activos más buscado por los ciberdelincuentes; la gestión de vulnerabilidades, inabordable; seguiremos preocupados por el IoT, y por la movilidad, y por todo lo que se marcha a la nube sin que podamos evitarlo; seguiremos añadiendo IA a todo lo que podamos, sin saber en realidad si hacemos sistemas más inteligentes o solo más espabilados. Y seguirá habiendo escasez de profesionales, demasiadas herramientas que gestionar y una consolidación que va a un ritmo más lento del esperado. En cuanto a tecnologías, ¿cuáles habremos de tener en cuenta? Os lo contamos en el tema de portada de este número.

Entre los protagonistas de #ITDSEnero destacamos a Roberto González, CIO y CISO de Grupo Primavera, para quien hay que prestar más atención a la prevención, y quien asegura que la virtualización, junto con sistemas de seguridad basados en IA, van a ser puntos clave para el próximo año.

Ramsés Gallego, responsable de CyberRess, una unidad de negocio independiente de Micro Focus, y Paolo Cappello, Managing Director of International de HelpSystems, son los otros protagonistas de este este número. Entre otras cosas dice el primero que CyberRes tiene una oferta holística, completa y coherente, mientras el segundo destaca que con HelpSystems One están intentando hacer la vida un poco más fácil a los administradores.

La actualidad llega marcada por un informe en el que se asegura que el 93% de las redes empresariales son vulnerables a brechas de seguridad, y un resumen sobre el valor del mercado de ciberseguridad.

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

Índice de anunciantes

itds

Sumario

Actualidad

Entrevistas

Revista IT Trends

No solo IT

Securizando organizaciones en cualquier lugar

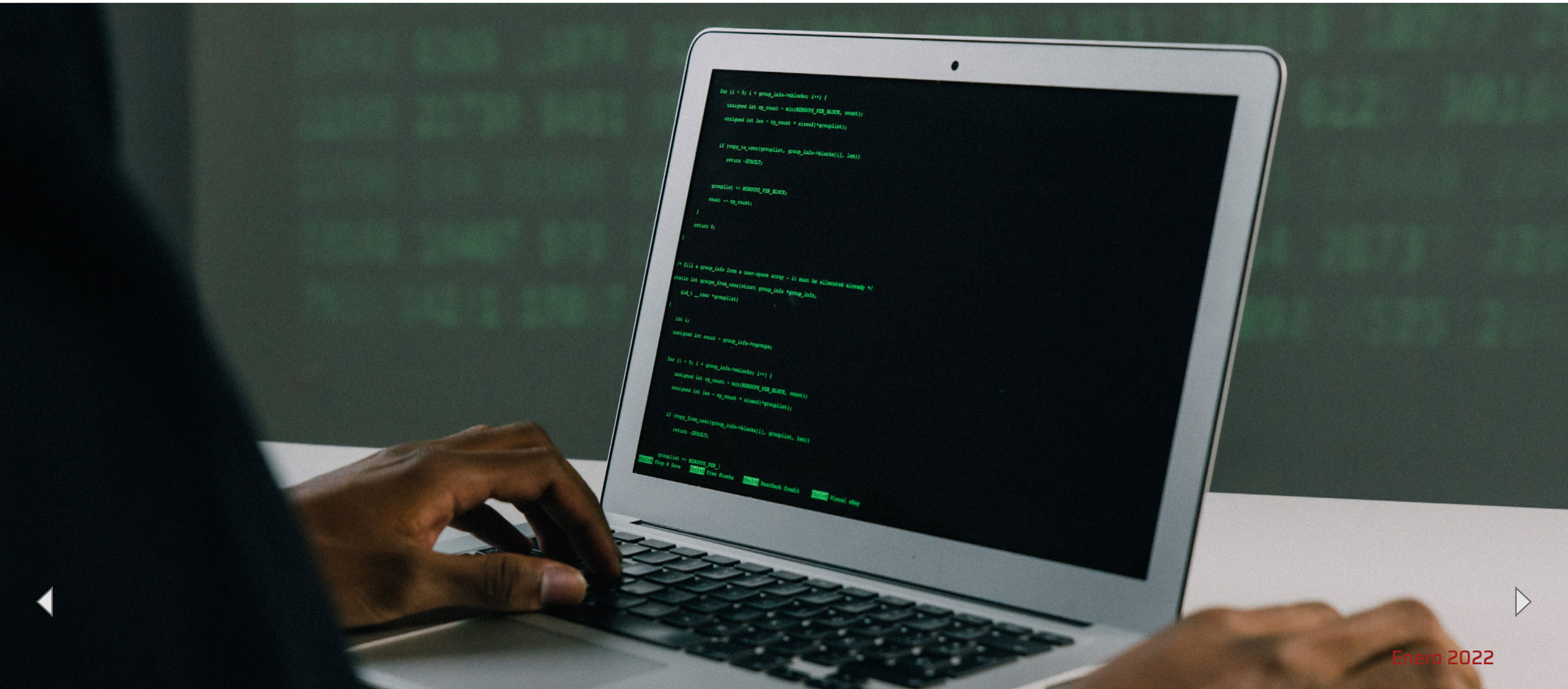
cualquier localización,
cualquier dispositivo,
cualquier recurso

Más información en **sophos.com/es-es/**

SOPHOS
Cybersecurity evolved.

Ciberseguridad, ¿un mercado infravalorado?

Se espera que el de ciberseguridad sea un mercado de 345.000 millones de dólares para 2026, creciendo desde los 218.000 millones estimados de 2021.



La ciberseguridad es un campo cada vez más importante en el mundo actual. Entre otras tendencias, los cambios hacia la nube pública, el trabajo desde casa y la Internet de las cosas han ampliado las superficies de ataque disponibles para los ciberdelincuentes. Como tal, las corporaciones son más vulnerables que nunca, lo que lleva a múltiples incidentes de ciberseguridad de alto perfil este año. Por ejemplo, en el ataque a Colonial Pipeline los ciberdelicuentes exigieron casi cinco millones de dólares en rescate y generaron el pánico entre la población.

Si el ciberdelito fuera un país, ya tendría un PIB de alrededor de 6.000 millones de dólares, y se espera que esta cifra crezca un 15% anual hasta 2025, cuando alcanzaría los 10.500 millones. En cambio, la industria de la ciberseguridad en sí solo tiene un valor de 167.000 millones de dólares en la actualidad, menos de un 3% de la valoración de mercado de ciberdelito. Y su crecimiento medio anual previsto es del 10,9%, lo que implica que crecerá más lentamente que la industria del ciberdelito.

Según los analistas, esta baja valoración se debe a que la ciberseguridad representa actualmente solo el 5,7% del gasto en TI. Sin embargo, la mayoría de los expertos recomiendan que este número esté en el rango del 10 al 15%, considerando el daño financiero y de reputación que generalmente se inflige a las empresas que son víctimas de ciberataques.

Antes de finalizar el año, los analistas Dan Ives y John Katsingris, de Wedbush, una firma de

El ataque contra Colonial Pipeline fue "la gota que colmó el vaso" y lo que impulsó que muchas empresas reevaluaran sus actitudes frente a la ciberseguridad

inversión con sede en Los Ángeles que en febrero de 2021 gestionaba 2.400 millones de dólares y unos 600 clientes aseguraron que el mercado de ciberseguridad podría estar infravalorado. Según estos analistas la “gran intensidad” del mercado de ciberseguridad no está recibiendo el respeto que se merece por parte de los inversores. Añaden además que “hay demasiados factores a favor de los proveedores de ciberseguridad para ignorarlos el próximo año”, refiriéndose a un panorama de amenazas que continúa acelerándose junto con el movimiento que empresas e instituciones públicas realizan hacia el cloud, multiplicando los vectores de ataque.

La situación, aseguran “ha creado una gran oportunidad para los proveedores de seguridad bien posicionados con el producto y la propuesta de valor adecuados”.

Entre las elecciones preferidas por los analistas en relación a empresas específicas mencionan a Zscaler, CyberArk Software, Varonis Systems, Sailpoint Technologies Holdings y Fortinet, todas ellas con calificaciones superiores a las de sus acciones. Además, Ives y Katsingris mencionan de manera específica a Palo Alto Networks y Tenable como las dos principales empresas de ciberseguridad para el próximo año; ambas también tienen calificaciones superiores a sus acciones.

Se refieren los analistas al ataque contra Colonial Pipeline como “la gota que colmó el vaso” y lo que impulsó que muchas empresas reevaluaran sus actitudes frente a la ciberseguridad. “Los ataques están aumentando a un ritmo asombroso y, en última instancia, creemos que este es otro catalizador de crecimiento del sector de ciberseguridad durante los próximos 12 a 18 meses”, aseguran, sin olvidarse del impulso que genera la Orden Ejecutiva de CiberSeguridad de la Administración de Biden.

También mencionan la mayor oportunidad que tienen las empresas que ofrecen seguridad cloud ya que “solo el 43% de las cargas de trabajo corporativas actuales se encuentran en entornos de nube”. Según los analistas la cifra crecerá hasta el 70% para 2025, lo que generará una oportunidad de mercado de más de 300.000 millones de dólares.

Enlaces de interés...

- La seguridad y el gobierno de los datos en cloud serán prioridad para las empresas en 2022
- El mercado de firewalls de SMS crecerá un 346% en cinco años
- Las empresas aumentarán su gasto en protección de sus bases de datos

Compartir en RRSS

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

El 93% de las redes son vulnerables a brechas de seguridad

Enero 2022

Según los datos de un estudio reciente publicado por Positive Technologies en base a los proyectos de pentesting realizados por la compañía durante la segunda mitad de 2020 y la primera de 2021, el 93% de las redes son vulnerables a una brecha de seguridad ya que un atacante externo podría violar el perímetro de la red de una organización y obtener acceso a recursos de redes locales. Según los investigadores de la compañía, esta cifra se ha mantenido alta durante muchos años, lo que confirma que los delincuentes pueden violar casi cualquier infraestructura corporativa.

Los datos también recogen que se tardarían dos días en penetrar una red interna y que una persona con información privilegiada obtendría el control total de la infraestructura en el 100% de las empresas analizadas.

El estudio se realizó entre organizaciones financieras (29%), organizaciones de combustible y energía (18%), gobierno (16%), industria (16%), empresas de TI (13%) y otros sectores.

En el 71% de los casos, el atacante podría afectar a las empresas de una forma considerada “inaceptable”. Por ejemplo, todos los bancos evaluados por la empresa de seguridad podrían ser atacados de una manera que interrumpiera los procesos comerciales y redujera la calidad de su servicio.

Según los datos del estudio, las credenciales comprometidas eran la mejor forma de acceder a una red corporativa, teniendo éxito en el 71% de los proyectos, y eso es porque la mayoría de los empleados usan contraseñas demasiado simples. En el 60% de los proyectos, la explotación de software con vulnerabilidades conocidas al que no se han aplicado los parches permitió al atacante infiltrarse aún más en la red de la empresa objetivo. En el 54% de los casos, la mala configuración de los dispositivos y el software provocó un mayor compromiso.

“LAS EMPRESAS NECESITAN MÁS INFORMACIÓN DE LO QUE ESTÁ OCURRIENDO EN SU INFRAESTRUCTURA EN TODO MOMENTO” (SOPHOS)

CLICAR PARA VER EL VÍDEO

Finalmente, en el 81% de los casos, obtener acceso a una cuenta de administrador de dominio pudo hacerse por un atacante con un nivel bajo de habilidades. Un atacante que tenga las credenciales con privilegios de administrador de dominio puede obtener muchas otras credenciales para el movimiento lateral a través de la red corporativa y el acceso a ordenadores y servidores clave. Las herramientas

Según el estudio de Positive Technologies, solo se tardarían dos días en penetrar una red interna

de administración, virtualización, protección o monitorización a menudo ayudan a un intruso a obtener acceso a segmentos de red aislados. Según el estudio, la mayoría de las organizaciones no tienen segmentación de la red por procesos comerciales, y esto permite a los atacantes desarrollar varios vectores de ataque simultáneamente.

Enlaces de interés...

- 8 de cada 10 empresas han sufrido incidentes por su ecosistema de proveedores
- Casi 3 millones de pymes en España están poco o nada protegidas contra hackers
- Un 9,2% de los trabajadores no se ven capaces de detectar un email malicioso

La mayoría de las organizaciones no tienen segmentación de la red por procesos comerciales y esto permite a los atacantes desarrollar varios vectores de ataque simultáneamente

Las evaluaciones de Positive Technologies encontraron que la mayoría de las industrias tenían importantes debilidades de seguridad. Siete de cada ocho empresas de los sectores industrial y energético fueron vulnerables a un “evento inaceptable” provocado por un atacante, señala el informe. Las malas prácticas de seguridad, incluso por parte de los profesionales de TI, crearon debilidades para que los atacantes las explotaran: nueve de cada 10 ingenieros, por ejemplo, tenían documentos de texto sin formato que describían parte de la red, junto con credenciales no cifradas.

WatchGuard Endpoint Security Solutions

Proteja sus dispositivos con confianza

Las soluciones nativas en la nube de WatchGuard Endpoint Security protegen a las empresas de cualquier tipo de ciberataques presentes y futuros mediante las soluciones Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR). Nuestra plataforma WatchGuard Endpoint Security ofrece una protección completa de EPP y EDR, así como servicios de búsqueda de amenazas y aplicaciones de confianza cero, suministrados a través de un único agente ligero y gestionados desde una única plataforma basada en la nube.

WATCHGUARD EPP

Endpoint Protection Platform

WATCHGUARD EDR

Endpoint Detection and Response

WATCHGUARD EPDR

Endpoint Protection Detection and Response

Threat Hunting Service

Zero-Trust Application Service

+34 917 932 531

spain@watchguard.com

www.watchguard.com

‘Sabemos que si somos capaces de encontrar los mejores productos en el mercado, y somos capaces de juntarlos, no hay posibilidad de que no tengamos éxito’

(Paolo Cappello, HelpSystems)

“En los últimos cinco años HelpSystems ha tomado la importante decisión de enfocarse en ciberseguridad”. Así comienza la entrevista con Paolo Cappello, Managing Director of International de HelpSystems, el responsable de liderar el crecimiento de una compañía que en los últimos dos años ha realizado una importante inversión en adquisición de empresas, muchas de ellas de seguridad (Digital Guardian, PhishLabs, Agari, Beyond Security, Digital Defense…).

Rosalía Arroyo

Hay dos áreas en las que la compañía está invirtiendo de forma predominante. Una es el ámbito del Data Protection, en la que “buscamos empresas que tengan algo más que ofrecer para unirlas y generar una oferta que quiere cubrir todo el ciclo digital de la información. Desde que la información se genera, clasificándola y entendiendo de qué información se trata, a definir quién puede acceder a esa información sino dónde puede ir esa información, extendiendo esta seguridad y la aplicación de la accesibilidad una vez que la información sale de la empresa”. En este sentido, cobran sentido adquisiciones como Titus, Boldon James para el área de clasificación, o la de Digital Guardian, la más reciente, que monitoriza el movimiento de los datos; la de Clearswift, centrada en la seguridad del email; las de GoAnywhere, GlobalScape y FileCatalyst en lo que tiene que ver con la seguridad en la transferencia de ficheros; la de Agari, que ayuda con el phishing y ataques BEC; la de PhishLabs, centrada en el Digital Risk Protection, que nos permite saber

"Si somos capaces de encontrar los mejores productos en el mercado, y somos capaces de juntarlos, no hay posibilidad de que no tengamos éxito"

lo que está pasando fuera de nuestra empresa; o Vera, que ofrecer gestión de la seguridad una vez que los ficheros han dejado la empresa para seguir gestionando quién tiene acceso a esa información.

Otra área que es foco para la compañía es todo lo que tiene que ver con Infraestructure Protection y que está orientado a todo lo relacionado con la gestión de vulnerabilidades. En esta área han sido claves las compras de Digital Defense o Beyond Security. Deja claro Paolo Cappello que "no nos quedamos en el escaneo de vulnerabilidades, sino que vamos más allá". En ese segundo paso entran en juego herramientas como las de Core Security para el tema de pentesting o Cobalt Strike, para la simulación de amenazas. La idea es poder testear que las defensas están bien organizadas y poder organizar todo el proceso de parcheo o de remediación de vulnerabilidades

Todas estas adquisiciones se armonizarán en una plataforma, HelpSystems One, que estará disponible en 2022 y que permitirá integrar las diferentes funcionalidades de todos los productos, ofreciendo una capa de coordinación e integración que simplifique la administración de la seguridad. "Con HelpSystems One estamos intentando poner la vida un poco más fácil a los administradores", asegura Paolo Cappello.

La estrategia de la compañía se ajusta a algunos de los grandes problemas del mercado. Uno de ellos es la complejidad que supone gestionar multitud de herramientas de seguridad. Habla también el directivo de HelpSystems de la "inflexibilidad del cloud", refiriéndose a que hay que tener en cuenta que la realidad es híbrida y que en estos entornos híbridos la seguridad se complica.

HelpSystems entra en el mundo de la seguridad con un amplio recorrido en otras áreas de

Diez adquisiciones en dos años

- Octubre 2021 — Digital Guardian
- Octubre 2021 — PhishLabs
- Mayo 2021 — Agari
- Mayo 2021 — Beyond Security
- Febrero 2021 — Digital Defense
- Enero 2021 — FileCatalyst
- Diciembre 2020 — Vera
- Junio 2020 — Boldon James
- Junio 2020 — TITUS
- Marzo 2020 — Strategic Cyber

mercado, como gestión del cloud, o de gestión de los documentos, cumplimiento, business intelligence, etc. ¿Qué aporta toda esta experiencia a la propuesta de ciberseguridad de la compañía? Explica Paolo Cappello que “cuanto más nos metemos en el mundo de la seguridad, tanto más vemos que hay una falta de automatización, por ejemplo, en todo lo que es la Security Automation, y nosotros tenemos herramientas de automatización que son un valor añadido adicional”. Al respecto la compañía ofrece una analítica centralizada basada en la integración de todas las capacidades de toda esa oferta de seguridad adquirida; “hay una oportunidad de explotar toda esta información para no tener que esperar para poder reaccionar y añadir automatización a nivel de seguridad”, dice el directivo.

No se olvida el Managing Director of International de HelpSystems del Threat Research, “que no siempre tiene suficiente visibilidad” pero enriquece al resto de herramientas de seguridad y permiten predecir un ataque.

Sobre el cliente tipo para esta oferta de ciberseguridad, “es bastante heterogéneo”. Menciona el directivo organizaciones de defensa “por la naturaleza de los productos de seguridad”, pero apuntan a toda empresa que tienen activos que proteger. Respecto al tamaño, se hace foco en la gran cuenta, “pero no nos olvidamos de las que tienen un tamaño medio y no llegamos a la pequeña”.

La compañía busca balancear el origen de sus ingresos: 50% Norteamérica y 50% el resto

del mundo, que coincide con la distribución del gasto en seguridad IT “para así aprovechar al máximo las oportunidades que nos ofrece el mercado”. Actualmente el peso de Norteamérica es mayor, explica, añadiendo que en España hay un equipo de 35 personas, la mayoría dedicada a seguridad, y que la aproximación está muy orientada al canal de distribución, aunque también se trabajan algunas cuentas de manera directa. En España los principales distribuidores son: IREO, Nextret, Westcon, Danysoft, Exevi, Bartech, Innovery, PFS Tech y Software Greenhouse.

“Queremos ser líderes” responde con seguridad Paolo cuando le preguntamos hacia dónde quiere ir la empresa. “Sabemos que si somos capaces de encontrar los mejores productos en el mercado, y somos capaces de juntarlos, no hay posibilidad de que no tengamos éxito. Esto es lo que estamos intentando hacer”. it

Enlaces de interés...

- HelpSystems Ciberseguridad
- W Seguridad y Gobierno de datos

HelpSystems entra en el mundo de la seguridad con un amplio recorrido en otras áreas de mercado, como gestión del cloud, o de gestión de los documentos, cumplimiento, business intelligence...

Compartir en RRSS

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

‘Galaxy es la gran apuesta de CyberRes para devolverle el brillo a Arcsight’

(Ramsés Gallego, CyberRes)

Con muchos años de experiencia en el mercado de seguridad, Ramsés Gallego es el responsable de CyberRes, una unidad de negocio independiente de Micro Focus, que busca triunfar en el mercado de ciberseguridad con cuatro líneas de negocio sostenidas por nombres tan conocidos como Voltage, NetIQ, Fortify y Arcsight.

Rosalía Arroyo

“Si algo nos identifica es que no somos monolíticos”, así lo asegura Ramsés Gallego, responsable de CyberRes, la unidad de negocio de ciberseguridad de Micro Focus, con foco en cuatro pilares: protección de datos, con Voltage; protección de identidad, con NetIQ; protección de aplicaciones, con Fortify, y Operaciones de seguridad, con Arcsight. Esa propuesta, que el directivo define como “holística, completa y coherente” es uno de los grandes diferenciales de la compañía.

De los cuatro pilares el que más crece, y no solo en CyberRes sino en el mercado en general, es Fortify, que permite “robustecer las aplicaciones”.

CYBERRES, TU VIAJE HACIA LA CIBERRESILIENCIA

CLICAR PARA VER EL VÍDEO

Asegura Ramsés Gallego que se ha hecho mucho en seguridad, pero hay muchas aplicaciones legacy que, como ha demostrado la brecha de Log4j, pueden generar importantes problemas; “robustecer las aplicaciones es una de las áreas de gran crecimiento en CyberRes y donde el mercado crece especialmente”.

En crecimiento dentro de la unidad de negocio de Micro Focus le sigue NetIQ, el área de gestión de identidades, en la que no se habla solo de IAM, sino PAM, MFA, SSO o federación de identidades. La tercera sería Voltage, centrada en la gestión de

"Cada vez se ven más ataques desatendidos, en los que el que te está atacando básicamente es el algoritmo"

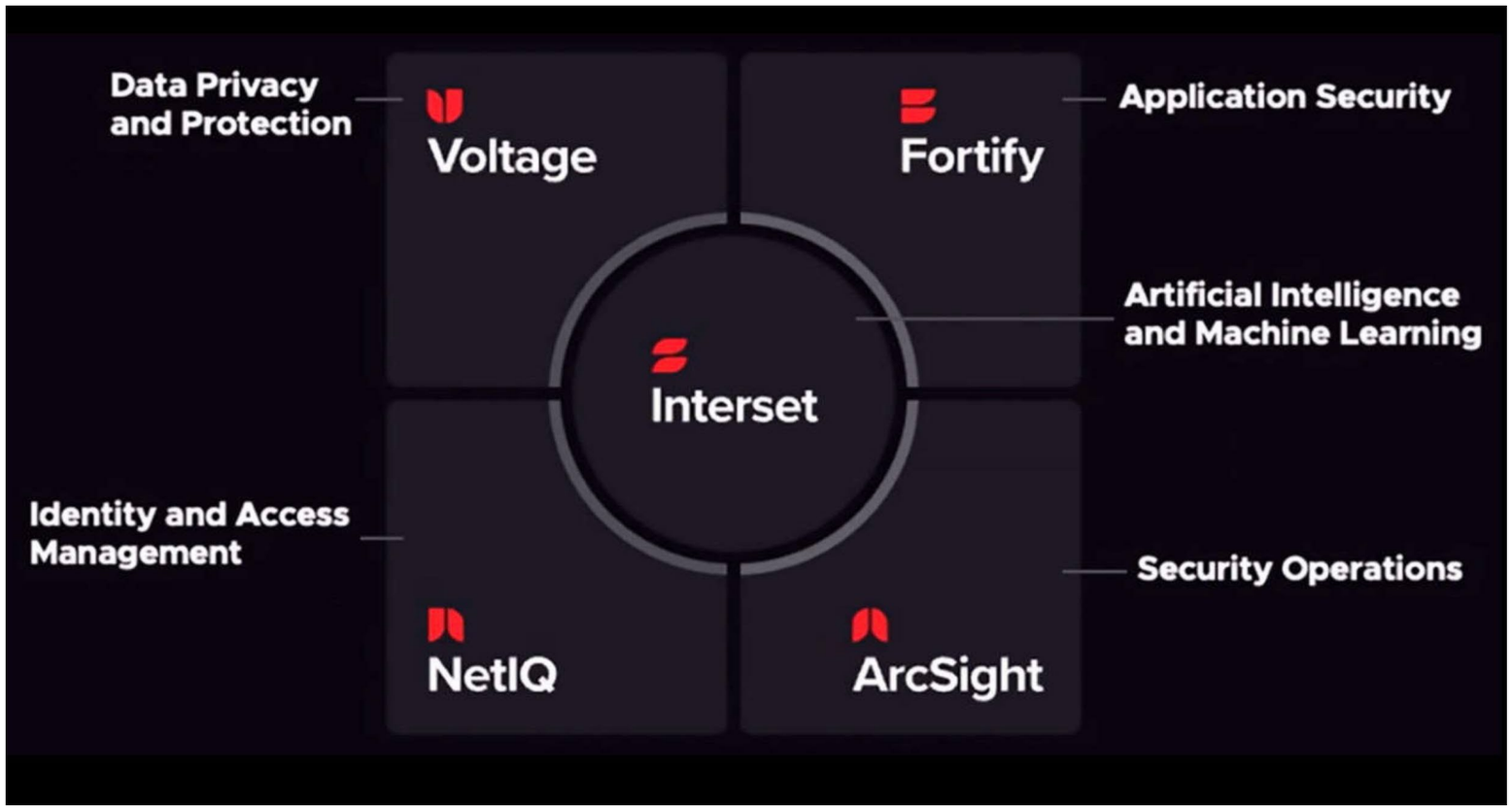
"Nosotros jugamos en muchos espacios de seguridad. En el que no jugamos, porque no queremos, es en el del endpoint"

datos y protección de la información, y finalmente Arcsight, una propuesta que acumula 21 años de historia, debe competir con grandes jugadores, y donde "hay que esforzarse un poquito más"; un esfuerzo que llega con Galaxy.

Galaxy

"En operaciones de seguridad hemos perdido el liderazgo que tuvimos y que creo que merecemos, y uno de los planes que tenemos en marcha para devolverle el alma a Arcsight es Galaxy", explica Ramsés Gallego.

Por lo tanto Galaxy es la gran apuesta de CyberRes para devolverle el brillo a Arcsight. Dice el directivo que se trata de un programa de inteligencia de amenazas que el 18 de enero tendrá una versión sin coste: Galaxy Community Edition, "un programa de investigación y de inteligencia de



"Robustecer las aplicaciones es una de las áreas de gran crecimiento en CyberRes y donde el mercado crece especialmente"

amenazas que ponemos a disposición de cualquier cliente, de cualquier tamaño, de cualquier industria y que contará con Boletines de Amenazas, y un portal al que cualquiera se suscribe identificando sus preferencias".

Una vez suscrito y definido el tipo de empresa, región y otros detalles Galaxy entregará, sin coste en la versión Community, información de lo que ocurre tanto en el internet público como en la Dark y Deep web. Algo que, en opinión de Ramsés Gallego "es muy interesante para el CISO o los equipos de investigación"; y si el cliente tiene Arcsight, "la bidireccionalidad es donde todo realmente gana".

Canal

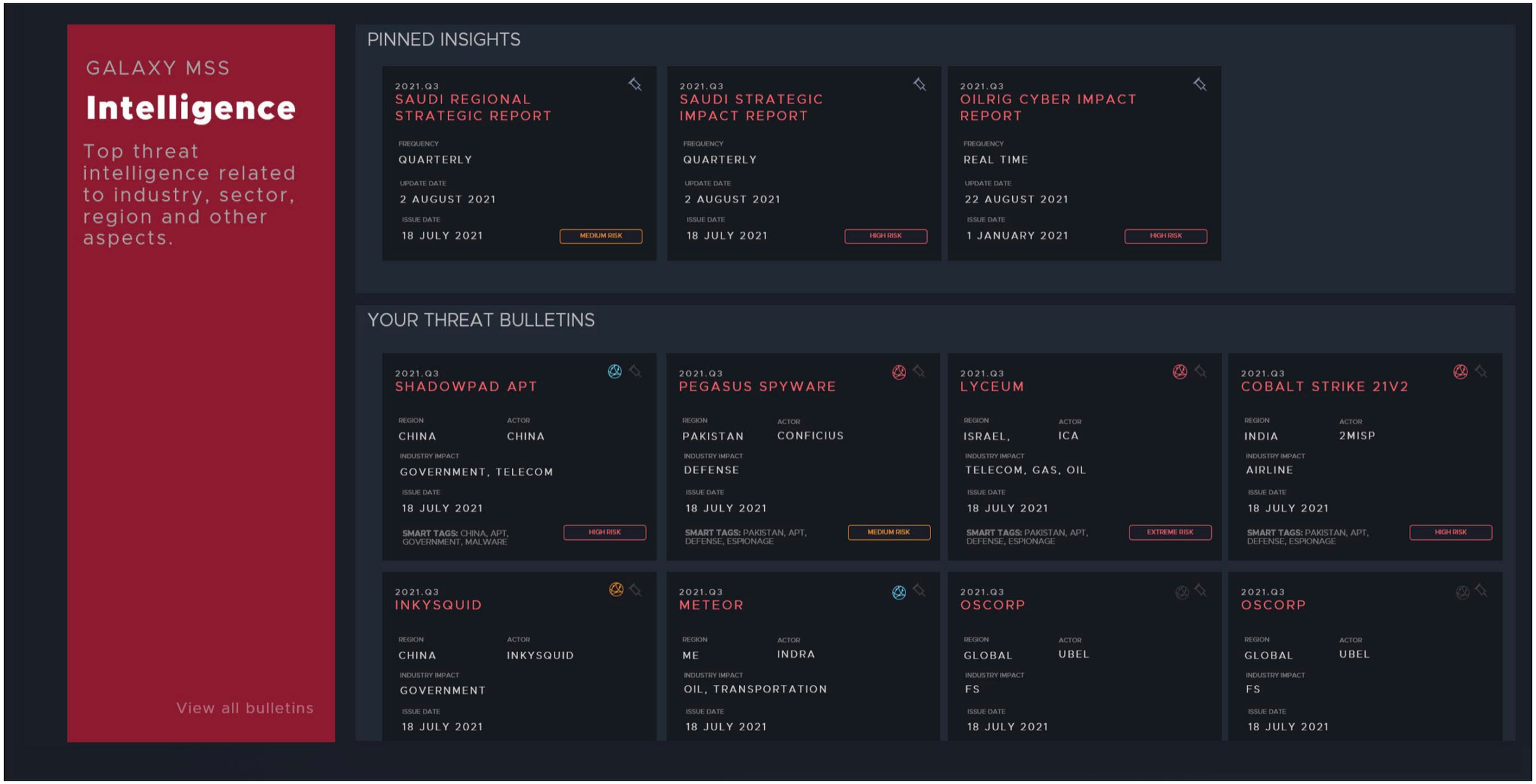
Ser una unidad de negocio de MicroFocus hace que muchos de los partners con los que trabaja CyberRes sean comunes. Pero también "tenemos algunos partners que son de seguridad específicos y que no están interesados en el resto de las magníficas cosas que hace Micro Focus", dice Gallego.

Javier Barandiarán es quien se encarga del programa de canal de CyberRes, que tiene opciones específicas de niveles, formación, etc.

Como curiosidad nos cuenta Ramsés Gallego que parece mentira cómo un logo, una marca, una nueva identidad en definitiva, está haciendo que muchos partners se estén interesando en una unidad de negocio, CyberRes, que hasta hace unos meses era una división de Micro Focus llamada Security Risk and Governance.

Tendencias. Hablando de SASE

Ramsés Gallego se considera un convencido de SASE (Secure Access Service Edge) y de Zero Trust porque "dan respuesta a las necesidades del mercado" que no son otras que garantizar la seguridad de la identidad, de los datos o que las aplicaciones sean robustas. Añade también el directivo que tendencias como SASE y Zero Trust



están presentes en las cuatro soluciones de CyberRes.

La esperada consolidación del mercado de seguridad está generando empresas cada vez más grandes que ofrecen un stack más completo con una plataforma de gestión que simplifique las operaciones de seguridad. Al mismo tiempo, el as-a-service está dando más capacidades al canal y a los proveedores de servicios imponiendo una consolidación a nivel de la cantidad de marcas que pueden llevar al mercado… ¿Cómo ves el mercado de seguridad? ¿Hacia dónde vamos? “Hay una inequívoca tendencia a la consolidación”, dice Ramsés Gallego mencionando las decenas de soluciones de seguridad que deben gestionar las empresas. Son decenas de soluciones que deben hablarse entre sí, decenas puntos de contacto que generan un riesgo, decenas de contratos que hay

"CyberRes tiene una oferta holística, completa y coherente"

Enlaces de interés...

- CyberRes, Viaja hacia la ciberresiliencia
- Fortalezca su ciberresiliencia

que ir renovando, en la mayoría de las ocasiones de manera escalonada.

Hay fabricantes que son monolíticos y otros, como CyberRes, que son multiproducto, "y la conversación con el cliente puede ser tan extensa como quiera".

Endpoint

Hace tiempo que el perímetro de seguridad, tan cuidadosamente delimitado por los primeros firewalls, se ha ido desdibujando gracias a la movilidad y al cloud. El perímetro se busca ahora en la identidad, el dato y el endpoint. Los dos primeros quedan cubiertos de manera concreta por NetIQ y Voltaje, ¿y el tercero?

"Nosotros jugamos en muchos espacios de seguridad. En el que no jugamos, porque no queremos, es en el endpoint. No competimos en el mercado de protección de puesto de trabajo, pero nos integramos muy bien con cualquiera de los fabricantes de esa área, especialmente con CrowdStrike", dice Ramsés Gallego.

Añade el directivo que el endpoint va a seguir siendo importante, especialmente ahora que el trabajo es verdaderamente híbrido, pero que cualquier cosa que se ofrezca desde la nube, en la nube y con la nube es fundamental y los avances tecnológicos están promoviendo que "los puestos de trabajo se conviertan en un activo más de la red y de la nube; el puesto de trabajo es infraestructura".

Mirando hacia 2022

"El año de la consolidación y de la estabilidad", así define Ramsés Gallego el segundo año de vida independiente de CyberRes, que se encuentra ahora cursando su primer trimestre fiscal. Prevén que Galaxy potencie la visibilidad CyberRes y que el crecimiento sea de doble dígito; "se han hecho cosas muy buenas y los clientes se han dado cuenta de que hay que hacer más en seguridad".

Habla el directivo de CyberRes de dos ciberamenazas que destacarán en 2022. Utilizando el Machine Learning no supervisado de la compañía para detectar ataques, explica el directivo que cada vez se ven más "ataques desatendidos, en los que no hay acción humana; en los que el que te está atacando básicamente es el algoritmo, capaz, con técnicas de machine learning, de buscar por múltiples vías dónde está el agujero de seguridad y encontrar el mejor camino para explotarlo. Es el ataque de las máquinas".

También se detecta como tendencia la "democratización" de los ataques, en los que grupos grandes venden a otros más pequeños ataques para que en una región, país o comunidad autónoma se ejecute, compartiendo los beneficios. En ambos casos la visibilidad que aporta Galaxy será fundamental para detectar esos ciberataques.

En tercer lugar, cualquier ataque a la nube también será tendencia, por lo que también debe serlo el proteger los datos en la cloud.

Compartir en RRSS

aruba
a Hewlett Packard Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

‘Lo importante, y más en el ámbito de la seguridad, no es tanto la solución o producto que vayas a seleccionar, sino el proveedor’

(Roberto González, Grupo Primavera)

Rosalía Arroyo

Tiene claro Roberto González Merino, CISO y CIO de Grupo Primavera, que en ciberseguridad hay que prestar atención a la prevención, y por eso la formación del usuario es fundamental; que los servicios gestionados son indispensables; que nadie quiere verse en una situación comprometida, pero que cuando te ves en ella lo que quieres es un buen soporte; que lo que todo el mundo tiene que tener es un EDR y que la virtualización, junto con sistemas de seguridad basados en IA, van a ser puntos clave para el próximo año.

Roberto González Merino es el CISO, y CIO, del Grupo Primavera, una empresa especializada en software empresarial para pymes con más de 55.000 clientes que suma la experiencia y el talento de Primavera BSS, Ekon, Triari Labs, Contasimple, Billage, Diez Software y Professional Software.

En su doble rol de hacerse cargo tanto de la ciberseguridad como de la gestión de TI del Grupo, dice Roberto González que en los últimos años tanto la figura del CISO como la del CIO “han evolucionado a ritmos forzados”. Un cambio que asegura que se lleva gestando desde antes de la pandemia y que, en el caso del CIO, ha pasado de encargarse de las operativas internas a tener un papel fundamental en un proceso de transformación digital que afecta a todas las unidades de negocio.

Sobre el CISO dice que la seguridad ha pasado de estar circunscrita a un firewall y un antivirus a tener que adaptarse a un importante cambio tecnológico que ha aumentado los factores de riesgo. Además de apuntar a que la mayor visibilidad del CISO, más involucrado en las diferentes unidades de negocio, les ha llevado a los consejos de dirección, asegura también el directivo del Grupo Primavera que “la pandemia ha llevado a una mayor colaboración entre el CISO y el CIO porque hemos pasado de pensar en el trabajo como un lugar físico a contemplar la movilidad”, que ha supuesto un cambio disruptivo que en ocasiones ha llevado a cambiar toda la arquitectura e infraestructura que las empresas tenían.

"Tenemos que acabar de evolucionar el tema de la virtualización"

Preguntado por los retos a los que se enfrenta el CISO y CIO de Grupo Primavera, menciona

"Los sistemas con inteligencia artificial es lo que más va a evolucionar en los próximos años"

Roberto González “el poder garantizar la misma seguridad, o incluso más, en un modelo de movilidad vs modelo físico. Garantizar de que puedas desarrollar las mismas funciones en una oficina que en el ámbito de tu casa”.

Habla también el directivo de la importancia de la educación que se le da al usuario porque “por mucho que modifiques los sistemas para que se adapten a la nueva situación, el usuario final, tanto interno de la empresa como tu cliente, también tiene que entender que su rol de usuario ha cambiado, que tenemos que evolucionar todos juntos y que se tiene que prestar también mucho énfasis en la prevención”. Añade que la mayor visibilización de incidentes de seguridad que afectan a empresas grandes está ayudando a que haya una mayor concienciación sobre la ciberseguridad.

Asegurando que le ha proporcionado más ventajas que inconvenientes, dice Roberto González que trabajar en una empresa que provee soluciones de TI “es un arma de doble filo”. Explica que trabajar en una empresa tecnológica puede hacer más fácil que se entienda y se empatice con las medidas que se tienen que implantar a nivel de seguridad en una empresa, pero también puede haber más riesgo del llamado Shadow IT por el mayor conocimiento tecnológico de los empleados, “lo que puede provocar alguna situación compleja”.

MSSP

“Para mí los servicios gestionados son indispensables y creo que, en mayor o menor medida, para todos deberían ser igual”, dice el directivo. Explica que “la principal premisa para entender no ya si es necesario, sino en qué medida se externalizan servicios, es el volumen de la empresa”, porque las muy grandes tienen recursos para tener la seguridad en casa.

La aceleración que se ha tenido que vivir con la pandemia demostró que había empresas que no estaban preparadas para todo lo que se nos ha venido encima, “y disponer de un socio, de un compañero de viaje, que te pueda ayudar a comprender la

situación es muy importante, sobre todo en el ámbito de la seguridad", dice Roberto González.

Hablamos también de la adopción del cloud y preguntamos si el ser CISO y CIO ha supuesto que dicha adopción se ha realizado de manera un poco diferente, teniendo en cuenta la seguridad desde el principio. Dice Roberto González que parte con una ventaja, que es el trabajar en Grupo Primavera, un grupo empresarial de joven creación en el que alguna de las empresas que lo conforman han sido pioneras "en promover una solución ERP cloud" lo que hace que la nube "ya esté muy interiorizado en nuestro ADN".

Asegurando que la evolución hacia el cloud es algo necesario, y que la seguridad es un punto a favor para su adopción, asegura Roberto González que el mercado en general se ha podido beneficiar "de la estandarización de los marcos regulatorios que todos los clouds públicos o los grandes proveedores han establecido".

Mantiene la apuesta por el cloud también desde su rol de CIO asegurando que es muy beneficioso y que "hemos ahorrado una cantidad de tiempo enorme en aprovisionamiento de infraestructuras, con despliegues prácticamente automáticos. Además, la parte del auto escalado que te aporta el cloud es fundamental. Y si entramos en las áreas de soporte de negocio, el que todas las herramientas de soporte, o la mayoría, estén en un en un ámbito cloud también ha sido fundamental para para agilizar muchos de los de los procesos y garantizar esa disponibilidad del servicio".

Tecnologías

En un mercado saturado de fabricantes, soluciones y propuestas como es el de seguridad, ¿cómo escoger la mejor solución? La respuesta es clara: "lo que mejor se adapte a ti". Asegura el CISO de Grupo Primavera que no existe una fórmula mágica sino una serie de necesidades. Añade además que "lo importante, y más en el ámbito de la seguridad, no es tanto la solución o producto que vayas a seleccionar, sino el proveedor". Explica que nadie quiere verse en una situación comprometida, pero que cuando te ves en ella "lo que quieres es un buen soporte, saber que la empresa que está detrás es un socio de confianza y que si en algún momento llegas a encontrarte en un punto delicado, vas a tener una respuesta rápida, eficiente y de confianza" y añade que "sobre todo en los últimos tiempos, lo que ha cobrado mucho peso es la respuesta o confianza que me transmite el proveedor".

"Para mí los servicios gestionados son indispensables"

"En los últimos años tanto la figura del CISO como la del CIO han evolucionado a ritmos forzados"

Tiene claro el CISO y CIO de Grupo Primavera que lo que todo el mundo tiene que tener es un EDR. "Cada empresa es un mundo, y sobre todo con el tema del presupuesto, pero si me preguntas qué herramienta de seguridad debería ser imprescindible en cualquier empresa la respuesta es un EDR", asegura. A partir de ese Endpoint Detection and Response, y teniendo en cuenta el negocio, tamaño de la empresa, etc., añade herramientas de inteligencia artificial, un SOC, un CASB… En todo caso tiene también claro que se puede invertir mucho en tecnologías de seguridad, "pero creo que se debería invertir más en la formación del usuario. Creo que en la actual situación la concienciación del usuario es esencial".

Hablando del usuario… "Lo que más está evolucionando en los últimos años, con todo el sentido, son los sistemas basados en el comportamiento del usuario y de inteligencia artificial", dice Roberto González antes de que le preguntemos por las tecnologías que serán imprescindibles en el futuro. Al respecto asegura que "los sistemas con inteligencia artificial es lo que más va a evolucionar en los próximos años".

De cara a 2022 dice Roberto González que "tenemos que acabar de evolucionar el tema de la virtualización". Explica que el foco es poder aportar al usuario un entorno deslocalizado, descentralizado y seguro para su trabajo y que la virtualización facilita además la agilidad y movilidad del usuario. Añade que tradicionalmente la virtualización ha estado asociada a grandes empresas y que poco a poco está llegando a las pymes; "el aportar una solución de movilidad segura para pequeña y mediana empresa, junto con los sistemas de seguridad basados en IA, van a ser puntos clave para el próximo año".

Enlaces de interés…

- 'En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento' (Mario Andrés, Mercadona)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)
- 'Las tecnologías ayudan, pero no son la clave' (Luis Ballesteros, WiZink)
- 'Si los clientes no son exigentes, las empresas no van a invertir en seguridad' (José Luis Paramio, Userlytics Corporation)
- '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)

Compartir en RRSS

La documentación TIC, a un solo clic

Nuevas reglas de seguridad para aplicaciones web y API

Es hora de poner al día las reglas de la seguridad para API y aplicaciones web para que correspondan a la manera en que se crean y gestionan las aplicaciones hoy en día. Al usar herramientas y procesos tradicionales, estarás siempre a la zaga de los adversarios y sus ataques. Con estas nuevas reglas, puedes tomar la delantera y conocer de primera mano el estado de la seguridad de tu empresa.

MTWO 6D BIM Construction Cloud Platform

MTWO es un software cloud de nivel empresarial para el sector de la construcción preparado para el futuro y que ayuda a gestionar todos los proyectos extremo a extremo con 6D BIM. Es capaz de conectar a todos los equipos en cualquier momento y en cualquier lugar a través de todos los dispositivos.

Los tres pilares de una Transformación Digital B2B exitosa

MTWO Complete Construction Cloud es una plataforma empresarial integrada de modelado de información de construcción en cinco dimensiones (BIM 5D) en la nube que permite a contratistas, propietarios de activos y desarrolladores acelerar su proceso de transformación digital.

Informe: Cloud, en busca de la agilidad

La nube se ha asentado en las organizaciones como un modelo de TI que permite ganar agilidad en las operaciones y en el despliegue de nuevos servicios. Este informe IT Trends apunta las principales tendencias en torno a la cloud en nuestro país.

itTRENDS

ENERO 2022

METAVERSO:

el espacio virtual que liderará la nueva revolución digital

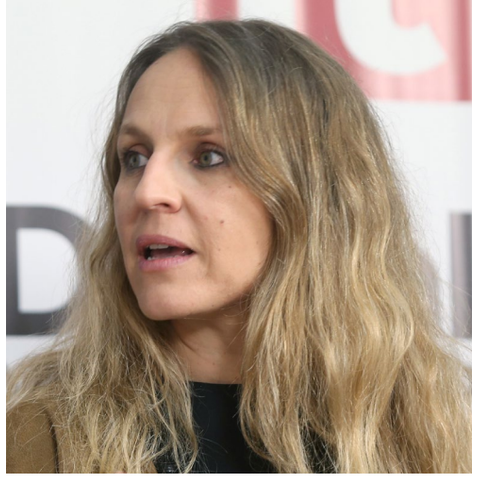
UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

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

Metaverso:
el espacio virtual que liderará la nueva revolución digital



En el horizonte de la evolución digital empezó a coger impulso a finales del pasado año un "nuevo" concepto, el de metaverso. Lo trajo a colación Facebook, con su propia reinvención, pero es una idea que viene de lejos y ya nos ha dejado algunas muestras a lo largo del tiempo: en 1992, el término aparece en la novela de ciencia ficción Snow Crash, de Neal Stephenson; en 2003 surge Second Life -que permite crearse un avatar y vivir una vida paralela dentro del juego, un mundo que aún visita un millón de personas-, y en 2020, Sony y el propio videojuego Fornite celebraron conciertos en sus plataformas virtuales.

Con la nueva estrategia de Facebook, esta idea de un metauniverso está adquiriendo un nuevo protagonismo, acelerado por la pandemia y la necesidad de comunicarse y colaborar cuando no puede hacerse de forma física; sin duda, se convertirá en megatendencia. Desde Bloomberg Intelligence señalan que ya el valor del metaverso es de 500.000 millones de dólares; en 2025 llegará a 800.000.

El desarrollo de este metaverso necesitará el soporte de la industria del software, el hardware, las comunicaciones, la nube... Habrá oportunidades de negocio para el sector tecnológico, pero también para el resto del mercado si las empresas quieren estar presentes en este espacio virtual y vender allí sus productos. Es, sin duda, una gran revolución la que se presenta, y a ella dedicamos algunas páginas de este número de IT Trends que estrena 2022.

También abordamos otras tendencias tecnológicas que veremos evolucionar en estos próximos doce meses, con especial atención a la ciberseguridad. Para analizarlo, reunimos a portavoces de **Entrust, Secure&IT, Stormshield, Sophos, Netwrix, WatchGuard, Citrix, Ikusi, SonicWall, Bitdefender, Qualys, Fastly, CyberRes (Micro Focus), y la Universidad Internacional de Valencia** en nuestro #EncuentroITTrends, cuyas conclusiones puedes leer a continuación.

Se presenta un año apasionante de tendencias tecnológicas aplicadas a la empresa. Cuento contigo para descubrirlas. ■

Arancha Asenjo
Directora IT Trends

www.ittrends.es

fastly

Signal Sciences
Now part of fastly

Protege las experiencias que impulsan tu negocio.

No importa dónde despliegues tus aplicaciones: Fastly puede protegerlas a escala. Ofrecemos a los equipos de desarrollo y seguridad soluciones que aportan visibilidad, control y acceso a información útil.

Una protección que no afecta al rendimiento.

Despliegue flexible y gestión sencilla.

La seguridad para aplicaciones que sí querrán tus desarrolladores.

Más información en:
fastly.com/es/products/cloud-security

En los últimos dos años, la industria tecnológica se ha visto afectada por muchas turbulencias a causa de los problemas en la cadena de suministro, la escasez de chips en muchas categorías y una recuperación económica que se desarrolla de forma lenta y desigual. Pero el progreso no se ha detenido, y el año que viene diferentes segmentos de la industria tecnológica se nutrirán de las últimas innovaciones para lanzar al mercado nuevos productos y soluciones que traerán cambios importantes.

Tendencias tecnológicas para 2022

La tecnología es uno de los pilares fundamentales de la economía moderna y en los dos últimos años esta industria en general se ha visto muy afectada por los problemas que ha causado la pandemia. La crisis sanitaria llegó en medio de una etapa de transición a nuevas tecnologías en campos como las telecomunicaciones o la computación, entre otros, y a su vez las organizaciones han tenido que pisar el acelerador de la transformación digital para adaptarse a un nuevo contexto.

Después de una etapa de cambios repentinos casi obligatorios en el ecosistema empresarial y de consumo, la industria tecnológica está retomando el camino que tenía marcado antes de la crisis, preparando el lanzamiento de innovaciones que serán la norma en los próximos años. Los investigadores de TrendForce han identificado 10 tendencias principales que impulsarán importantes cambios en la informática empresarial, las telecomunicaciones y la electrónica de consumo en general.

5 TENDENCIAS TECNOLÓGICAS ESTRATÉGICAS PARA 2022

COMUNICACIONES MÓVILES DE BAJA LATENCIA Y SEGMENTACIÓN 5G SA

Los operadores de telecomunicaciones están cambiando paulatinamente el núcleo de sus redes para implementar tecnologías 5G SA, que permiten sacar todo el potencial de la siguiente generación de redes celulares. La construcción de nuevas estaciones base en las principales ciudades está habilitando la diversificación de los servicios de red, gracias a la segmentación del espectro 5G, la computación en el borde y la capacidad de entrega de servicios de un extremo a otro con más garantías de calidad.

En 2022, los expertos anticipan que aumentará la sinergia entre 5G, IoT masivo e IoT para aplicaciones críticas, y la demanda empresarial dará lugar a nuevos servicios. Destacan los interruptores eléctricos, sensores y termostatos para fábricas inteligentes, que implican una combinación de puntos finales de red y transmisión de datos. En el ámbito de las aplicaciones críticas de IoT despuntará la automatización de redes inteligentes, la telemedicina, la seguridad y control del tráfico, y la automatización industrial, tendencias que están cogiendo mucha fuerza. Y dentro del contexto de la Industria 4.0 los usos críticos de IoT más importantes serán el seguimiento de activos, el mantenimiento predictivo, la gestión de servicios de campo (FSM) y la optimización logística.

Bitdefender

BUILT FOR RESILIENCE

Bitdefender está diseñado para la resiliencia.
Elija nuestra plataforma de seguridad o servicio administrado para convertirse en el negocio más resistente a los riesgos más impredecibles.

- eXtended Endpoint Detection and Response (XEDR)
- Managed Detection and Response (MDR)
- Cloud Workload Security (CWS)

Diseñado para prevenir.
Diseñado para detectar.
Diseñado para responder.

www.bitdefender.es/business/

Al mismo tiempo, se anticipa una importante expansión de las redes privadas 5G y del estándar OpenRAN, cada vez más aceptado por importantes operadores de telecomunicaciones. También de los espectros de frecuencia no sujetos a licencias y del desarrollo de tecnologías mmWave. Estas innovaciones están propagándose entre los operadores de redes móviles y los proveedores de servicios emergentes, como OTT, CSP, redes sociales y negocios online. TrendForce prevé que, en el futuro, los operadores de redes móviles expandirán activamente sus aplicaciones empresariales 5G para cubrir las necesidades de nuevas industrias.

MAYOR COMPETENCIA EN LAS REDES SATELITALES MODERNAS

El despliegue de constelaciones de satélites de orbita baja (LEO) para construir redes globales se está acelerando, destacando el avance de empresas como SpaceX, Amazon, OneWeb, Telesat y otras. Al mismo tiempo, 3GPP ha anunciado recientemente que en 2022 se llegará la versión final del protocolo de la versión 17, en la que por primera vez se incluyen las comunicaciones NTT (Redes No Terrestres), lo que constituye un hito en la industria de telecomunicaciones móviles y por satélite. Este avance implica una sinergia entre estos dos ecosistemas tradicionalmente separados, que dará como resultado nuevas colaboraciones entre ambas industrias y supondrá un impulso para la innovación.

Por ahora, en el ámbito de las redes satelitales Estados Unidos lleva la ventaja, acaparando el 50% de todos los satélites lanzados entre sus diferentes operadores, pero se espera un crecimiento de operadores de otras regiones. Las ventajas que ofrecen las comunicaciones vía satélite, que no se ven afectadas por barreras geográficas, impulsarán su expansión en 2022. Y se espera que los operadores de satélites LEO colaboren con los de redes 5G para brindar servicios móviles en ubicaciones de difícil acceso para las redes convencionales. Esto se traducirá en un aumento considerable de los ingresos de las redes satelitales, que seguirá impulsando su expansión.

IOT COMO PILAR DEL METAVERSO EN LA INDUSTRIA

A consecuencia de la transformación digital, las empresas industriales están interesadas en adoptar tecnologías centradas en construir sistemas ciber-físicos (CPS), que permiten tener una visión digital detallada y en tiempo real del mundo físico. Por ejemplo, en la industria manufacturera, la logística y otros ámbitos en los que el seguimiento de activos y procesos es fundamental para mejorar la eficiencia en la fabricación y la entrega de productos.

La máxima expresión de los sistemas ciber-físicos está en los gemelos digitales, pero el año que viene muchas empresas industriales se centrarán en consolidar el primer paso necesario para desarrollar sistemas CPS. Se espera que aceleren la implementación de soluciones IoT para la recopilación de datos y el control automatizado, combinando tecnologías como 5G, computación perimetral e inteligencia artificial. Esto permitirá extraer y analizar información valiosa de los flujos de datos crecientes para mejorar la automatización y la predicción inteligente.

El siguiente paso está en construir y alimentar los gemelos digitales, que proporcionan una representación virtual del mundo real en base a todos los datos recopilados mediante IoT y otros sistemas. Actualmente están cada vez más aceptados en sectores como la industria manufacturera o las ciudades inteligentes, pero en los próximos años se expandirá su uso a nuevos sectores. Y los expertos anticipan que se producirá una mayor integración de otras innovaciones como la detección 3D, la realidad virtual y aumentada, que expandirán el metaverso IoT inteligente que se está construyendo a un nuevo nivel.

Posteriormente llegarán otras innovaciones tecnológicas que permitirán recopilar e integrar nuevas categorías de datos en estos sistemas ciber-físicos, como la información visual, auditiva y ambiental capturada a través de nuevos sensores. O el análisis de datos mediante plataformas de IA integradas y la securización de los flujos de información a través de tecnología blockchain.

NUEVAS TECNOLOGÍAS PARA MEJORAR LAS EXPERIENCIAS AR/VR

Además de acelerar la digitalización, la pandemia ha cambiado la forma de vivir y trabajar de las personas, y ha estimulado la exploración de tecnologías emergentes en las empresas. Entre ellas, la realidad virtual y aumentada han comenzado a hacerse más presentes para reuniones virtuales, soporte remoto basado en AR y diseño virtual. Los expertos de TrendForce señalan que dos de los segmentos más importantes para estas tecnologías son la interacción remota en comunidades virtuales y los juegos en línea, gracias a que los fabricantes están bajando los precios de sus sistemas de visualización enfocados a estos segmentos.

Pero, además de democratizar la tecnología, los fabricantes están buscando formas de mejorar las experiencias inmersivas con imágenes más realistas, construidas con herramientas de software más avanzadas. Entre ellas destacan las que son capaces de generar respuestas virtuales a partir de los datos del mundo real con asistencia de inteligencia artificial y datos provenientes de sensores avanzados. Un ejemplo es la capacidad de seguimiento ocular, que se ha convertido en una característica opcional en los modelos de consumo de varias marcas importantes. Pero los expertos creen que se va a avanzar hacia la integración de otros dispositivos externos capaces de mejorar la experiencia inmersiva para el usuario, por ejemplo, proporcionando retroalimentación háptica parcial a través de complementos para las gafas.

CAMBIOS EN LA INDUSTRIA DE SEMICONDUCTORES DE TERCERA GENERACIÓN

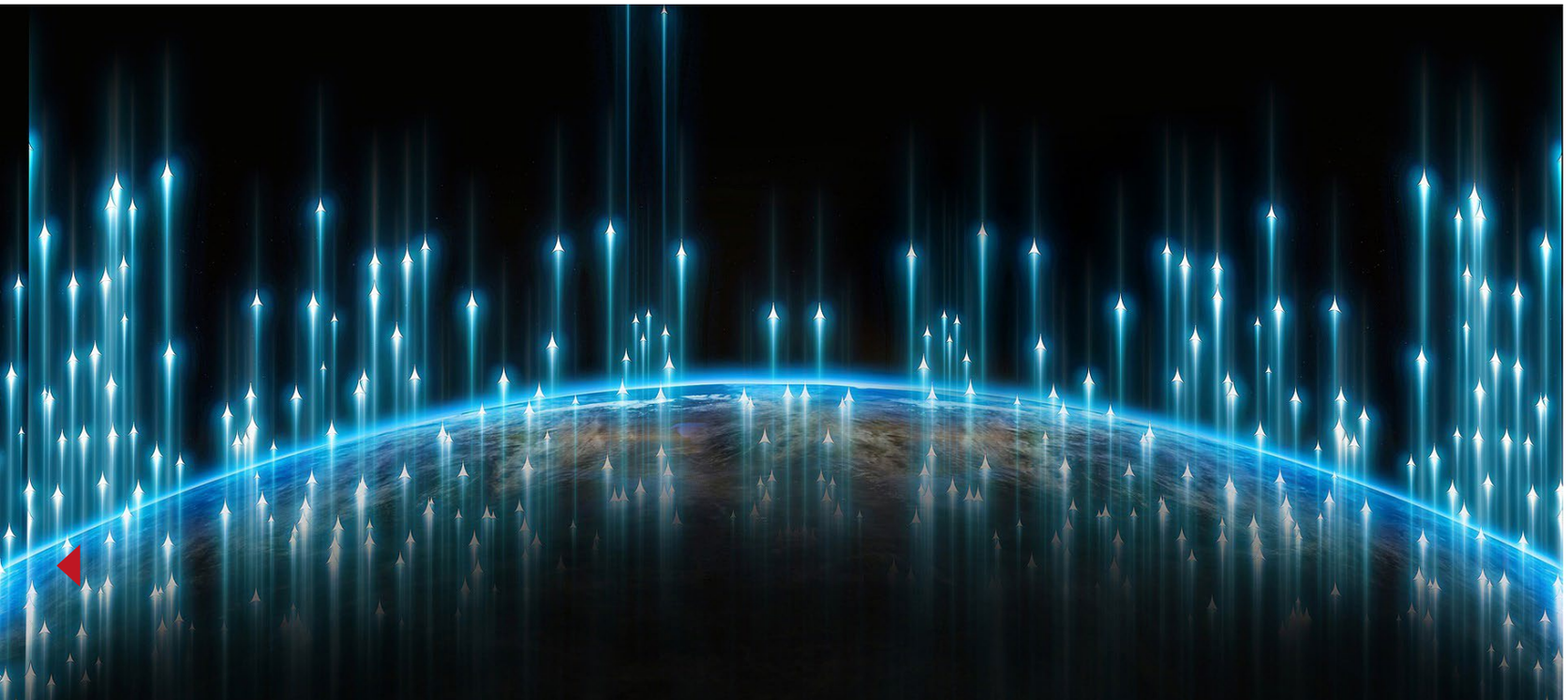
Los fabricantes de chips de tercera generación están adoptando nuevas tecnologías de empaquetado y obleas de 200 mm para la fabricación de sus productos más avanzados. Esto responde a la demanda de industrias como la de vehículos eléctricos y a la creciente tasa de penetración de dispositivos y módulos SiC y GaN en industrias como la de telecomunicaciones. Hasta ahora, los fabricantes han recurrido a las obleas de 150 mm (6 pulgadas) para garantizar el rendimiento de sus fábricas ante la escasez de suministros de SiC y GaN, pero esto ha exacerbado la escasez global de semiconductores a largo plazo en las fundiciones y los IDM.

Para solucionar este problema, los proveedores de sustratos más importantes del mundo planean aumentar su producción en 2022 y migrar a obleas de 200 mm (8 pulgadas) para los soportes de SiC y GaN. Con ello esperan aliviar la escasez actual de materiales para la fabricación de semiconductores de tercera generación. Al mismo tiempo, los fabricantes de semiconductores están adoptando nuevas técnicas de fabricación y empaquetado para incrementar la eficiencia energética de sus chips.

NUEVAS TECNOLOGÍAS DE PROCESO EN LA FUNDICIÓN DE SEMICONDUCTORES

Otro de los cambios importantes que se acelerarán este año en la industria de semiconductores se dará en el ámbito de la fundición. TrendForce explica que a medida que los procesos de fabricación se acercan a los límites físicos, la industria está realizando cambios en la arquitectura de transistores; y a nuevos avances en las tecnologías y materiales de empaquetado back-end, lo que permitirá aumentar el rendimiento, reducir el consumo energético y el tamaño de los componentes. Tras la incorporación de la litografía EUV en los nodos de 7 nanómetros, en 2022 llegarán los nuevos nodos de 3 nanómetros, inicialmente de la mano de TSMC y Samsung, que los implementarán en el segundo semestre de 2022.

La fundición taiwanesa seguirá utilizando la arquitectura FinFET que lleva empleando desde el nodo de 1Xnm, mientras que Samsung comenzará a usar su propia implementación de GAA-FET, que denomina MBCFET en sus tecnologías de 3 nanómetros. Esta consiste en una puerta que rodea el canal de nanocables o nanoplacas por cuatro lados, lo que incrementa el área de superficie de contacto y reduce las corrientes de fuga al tener una puerta con un mayor grado de control sobre el canal. Esta tecnología se utilizará inicialmente en la fabricación de chips para supercomputación y dispositivos móviles, pero posteriormente se expandirá a otros campos.



NUEVA GENERACIÓN DRAM Y MÁS CAPAS PARA ALMACENAMIENTO NAND FLASH

A lo largo del año que viene los tres principales fabricantes de memoria DRAM (Samsung, SK Hy-

CyberRes

Strengthen Your Cyber Resilience.

Adapte su ciberseguridad de forme inteligente.

Proteja todos los ámbitos de su empresa, adáptese de manera inteligente a las circunstancias cambiantes y conviértase en ciberresiliente para tener éxito en un mundo en constante cambio.

Proteger. Detectar. Evolucionar.

CyberRes.com

nix y Micron) comenzarán la producción en masa de los nuevos módulos DDR5. Y fomentarán la penetración de LPDDR5 en la industria de teléfonos móviles, aprovechando que 5G habilita nuevas aplicaciones y servicios de alto rendimiento y baja latencia. En el ámbito de las plataformas de computación, la llegada de los nuevos procesadores habilitados para DDR5 en ordenadores y servidores, se espera que DDR5 represente entre un 10% y un 15% de la producción global de bits DRAM a finales de 2022.

En el ámbito del almacenamiento NAND Flash, tras la introducción de chips con 176 capas este año, en el próximo verá la luz la nueva generación de memoria de 200 capas o más. Aunque los expertos dicen que la densidad de los nuevos chips se mantendrá entre 512 Gb y 1 Tb en los primeros productos. Otro cambio importante en la industria es la expansión de los nuevos SSD PCIe Gen 4 entre el segmento de ordenadores de consumo. Mientras tanto, en la industria de servidores se iniciará la producción en masa de SSD empresariales compatibles con PCIe Gen 5, con capacidades de entre 4 y 8 Tb, enfocados a las plataformas HPC de servidores y centros de datos.

Por otro lado, los expertos anticipan que en el mercado mundial de servidores seguirá aumentando la demanda de equipos por parte de los proveedores de servicios en la nube, impulsando más aún el mercado de los proveedores ODM Direct. Esperan que este gran segmento del mercado de servidores represente alrededor del 50% de las ventas globales, con un crecimiento anual del 10% o más en los envíos de los proveedores ODM Direct. Esto llevará a las marcas tradicionales de servidores a realizar cambios estructurales en su modelo de negocio, por ejemplo, ofreciendo servidores de colocación o servicios completos de soporte para la migración a la nube.

PANTALLAS LED DE MATRIZ ACTIVA

A lo largo de 2022 se espera que persista el cuello de botella que afecta al desarrollo de Micro LED, y a causa de ello los costes de fabricación de estos productos seguirán siendo muy elevados. Pero los principales fabricantes quieren participar en todos los segmentos de la cadena de suministro de esta tecnología, y están ampliando sus líneas de producción. Uno de los principales segmentos de pantallas Micro LED autoemisoras son los televisores, que son más fáciles de fabricar que otras categorías de productos TI. Y se prevé un aumento de producción de pantallas Micro LED de matriz activa de gran tamaño, llegando al estándar de 88 pulgadas de diagonal.

Mientras tanto, el año que viene los fabricantes seguirán aumentando los recursos destinados a la producción de chips para pantallas con retroiluminación Mini LED, para mejorar las especificaciones de sus pantallas, haciéndolas comparables a las OLED. Y se espera que los fabricantes migren desde las matrices pasivas a nuevas ma-

AVANCES PARALELOS A LA CONDUCCIÓN AUTÓNOMA

El avance de los vehículos autónomos está siendo moderado, y mientras se implementan las numerosas tecnologías necesarias para hacerlos realidad irán viendo la luz ciertas capacidades automatizadas para mejorar los servicios al conductor. En 2022, los vehículos de gama alta incorporarán de forma opcional sistemas AVP (Automated Valet Parking), un servicio de estacionamiento automatizado de nivel SAE 4. Las regulaciones internacionales necesarias para hacer esto posible todavía están en preparación, pero comenzarán a verse en este año.

Los expertos señalan que la viabilidad y la popularización de esta tecnología está condicionada por numerosos factores, como las restricciones relacionadas con las condiciones de conducción y de estacionamiento de cada vehículo y entorno, la presencia de señalizaciones adecuadas y una conectividad de red de calidad. Las leyes nacionales ya contemplan la distancia adecuada entre el vehículo y las personas circundantes en cada país, lo que complicará el proceso de establecer una estandarización internacional. Por otro lado, existen dos formas de crear las rutas de estacionamiento empleadas en las funciones de AVP, que se pueden generar a través de computación local en el propio vehículo, o de computación basada en la nube. Esto resalta la importancia de la calidad de la conexión del vehículo. Para suplir posibles carencias algunos modelos de vehículos contarán con ambas soluciones, y la industria seguirá trabajando en los avances de V2X y de los mapas modernos para vehículos con el fin de habilitar diferentes vías para establecer las rutas de parking automatizado.

trices activas para sus productos con retroiluminación Mini LED, incrementando por ello la compra de chips Mini LED.

NUEVAS PANTALLAS AMOLED Y CÁMARAS PARA SMARTPHONES

La tecnología de pantallas AMOLED ha ido madurando y los fabricantes han añadido nuevas funciones y mejorado las especificaciones para incrementar el valor añadido y lograr ventajas competitivas. Este año 2022, la principal línea de acción será continuar mejorando los paneles AMOLED flexibles, reduciendo su peso y mejorando su eficiencia energética. Y los expertos creen que los fabricantes se enfocarán a lanzar nuevos paneles flexibles capaces de alcanzar el tamaño de una tableta, con diseños tipo concha y cuerpos abatibles en dos direcciones, que permitirá albergar paneles de estas dimensiones.

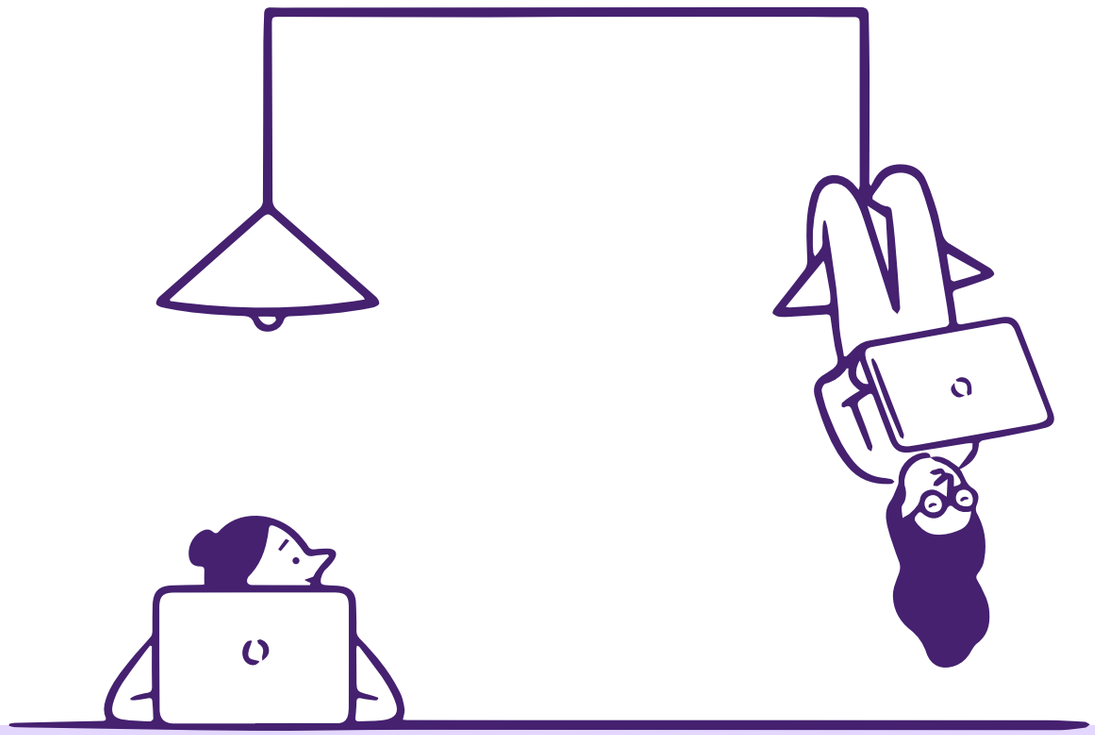
También se espera una bajada de precios de estos formatos flexibles en los modelos insignia de las marcas, con el fin de impulsar las ventas. Y los fabricantes seguirán trabajando en el desarrollo de modelos con pantallas de más pliegues y pantallas enrollables, que en los próximos años tratarán de establecerse en el mercado. En general, TrendForce pronostica que este 2022 los teléfonos plegables alcanzarán una penetración del 1%, que podría ascender hasta el 4% para el año 2024.

En otro orden de cosas, se espera que los paneles LTPO se consoliden como la principal opción para los modelos de smartphone 5G más importantes, gracias a que generan un menor consumo y proporcionan una alta frecuencia de actualización. Y otra característica que comenzará a expandirse será la cámara bajo la pantalla, que se verá en los modelos de gama más alta de los principales fabricantes. ■

MÁS INFORMACIÓN

- Redes privadas y empresariales
- Tendencias IT 2022: ¿qué impactará en la TI corporativa?
- Tendencias de ciberseguridad 2022. La ciberinteligencia entra en escena
- Gartner: Tendencias estratégicas para 2022
- Las empresas seguirán incrementando el gasto en Transformación Digital
- Tendencias tecnológicas para la industria en 2022 (TrendForce)
- Se acelera el lanzamiento de redes 5G Stand Alone
- Los problemas de conectividad frenan los despliegues de IoT
- El mercado OpenRAN crece con fuerza
- Telecomunicaciones por satélite para un mundo mejor conectado
- Aumenta la adopción de gemelos digitales
- El Metaverso aumentará la venta de tecnología de AV y RV
- La UE quiere impulsar la industria de chips en Europa
- Lectura optimizada de SSD antiguos
- La escasez de chips aumenta el precio de pantallas y dispositivos
- Gestión inteligente del tráfico para un transporte más eficaz

Tus empleados
se merecen una
tecnología tan
única como ellos.



citrix™

METAVERSO:
el mundo virtual se convierte en realidad

Finalizado el año 2021, podemos decir que ha habido un término que ha copado todo el interés del mundo TI, sobre todo en los últimos meses: Metaverso. Esta idea comenzó a hacerse popular a finales de octubre, cuando Mark Zuckerberg, hasta entonces CEO de Facebook, anunció el cambio de denominación de su compañía, desde ese momento Meta, y la creación del Metaverso, un entorno virtual de convivencia con el que la firma quiere seguir ampliando sus fuentes de ingresos más allá de la publicidad.

El Metaverso o metauniverso se define como una experiencia inmersiva y multisensorial por el uso aplicado de diversos dispositivos y desarrollos tecnológicos en Internet. Generalmente, está compuesto por múltiples espacios virtuales tridimensionales, compartidos y persistentes, vinculados a un universo virtual. En un sentido más amplio, el Metaverso puede no solo referirse a los mundos virtuales, sino a las experiencias multidimensionales de uso y aplicación de Internet en su conjunto, especialmente el espectro combinado de la web 2.0, la realidad aumentada, la tecnología 3D y la realidad virtual.

Los metaversos son entornos donde los humanos interactúan social y económicamente como avatares, a través de un soporte lógico en

el ciberespacio, que actúa como una metáfora del mundo real, pero sin limitaciones físicas o económicas. Hasta ahora se han identificado usos aplicados de los metaversos en el terreno del entretenimiento, la teleeducación, la telemedicina y la economía digital, donde comienzan a emerger nuevas formas de valor como los token no fungibles (NFT, por sus siglas en inglés).

ORIGEN DEL METAVERSO

Como ocurre con algunos otros términos y conceptos en el mundo de las TI, el origen del Metaverso no está del todo claro, si bien parece que existe cierto consenso alrededor del primer momento en que se empezó a hablar de ello. Nos referimos a la publicación en 1992 de la novela Snow Crash de Neal Stephenson. En ella, se cuenta la historia de Hiroaki Hiro, un personaje que es repartidor de pizza en el mundo real y samurái en el mundo virtual. Pero más allá de la historia, la importancia de esta novela radica en el hecho de que establece la primera referencia escrita de un mundo completamente virtual mucho antes de que se empezara a hablar del ciberespacio. Además, en su libro, Stephenson introduce la idea de los avatares, personajes virtuales de las personas del mundo real.

Hasta ahora se han identificado usos aplicados de los metaversos en el terreno del entretenimiento, la teleeducación, la telemedicina y la economía digital

FACEBOOK, META Y EL METAVERSO

En cualquier caso, el concepto de Metaverso saltó a las primeras páginas de la prensa mundial el pasado 28 de octubre cuando Mark Zuckerberg anunciaba su apuesta por esta realidad virtual que incluía el cambio de nombre de la compañía que él fundaba y dirige, que pasaba de llamarse Facebook a denominarse Meta.

Así, en una presentación en la conferencia Connect 2021, Zuckerberg anunció que la empresa se renovaba como Meta, algo que se produce después de que la corporación se haya visto envuelta en diferentes escándalos que

¿QUÉ ES EL METAVERSO CON EL QUE MARK ZUCKERBERG PRETENDE REVOLUCIONAR FACEBOOK?

han afectado a su reputación e imagen pública, y detalló cómo su compañía pretende construir una nueva versión de Internet. Tal y como él mismo explicó, "creemos que el Metaverso será el sucesor de la Internet móvil, podremos sentirnos presentes, como si estuviéramos allí mismo con la gente, sin importar lo lejos que estemos en realidad".

Si el Metaverso se convierte en el sucesor de Internet, podría ser muy importante para el futuro de la economía y la sociedad en su conjunto. Por este motivo, Facebook tiene como objetivo desempeñar un papel de liderazgo en la configuración del Metaverso, en parte mediante una fuerte inversión en la realidad virtual. El propio Zuckerberg explicó en una entrevista en The Verge su visión de que el Metaverso abarca plataformas no inmersivas, como las redes sociales actuales, junto con tecnologías de medios 3D inmersivas, como la realidad virtual, y que será tanto para el trabajo como para el juego.

Según Zuckerberg, "el Metaverso brindará enormes oportunidades a los creadores y artistas individuales; a las personas que quieran trabajar y tener casas lejos de los centros urbanos actuales; y a las personas que viven en lugares donde las oportunidades de educación u ocio son más limitadas. Un Metaverso realizado podría ser lo más parecido a un dispositivo de teletransporte que funcione". Por esta razón, con la división Oculus, que produce el auricular Quest, su compañía está intentando desarrollar uno.

En su entrevista en The Verge, el creador de Facebook comentaba que "creo que mucha gente, cuando piensa en el Metaverso, piensa sólo en la Realidad Virtual, que creo que va a ser una parte importante de ella. Y es claramente una parte en la que estamos muy involucrados, porque es la tecnología que ofrece la forma más clara de presencia. Pero el Metaverso no es solo realidad virtual. Va a ser accesible a través de todas nuestras plataformas informáticas, Realidad Virtual y Realidad Aumentada, pero también PC, dispositivos móviles y consolas de juegos. Hablando de eso, mucha gente también piensa en el Metaverso como algo principalmente relacionado con los juegos. Y puede que el entretenimiento vaya a ser claramente una gran parte de él, pero no creo que esto sea solo juego. Se trata de un entorno persistente y sincrónico en el que podremos estar juntos, que probablemente se parecerá a una especie de híbrido entre las plataformas sociales que vemos hoy en día, pero en un entorno en el que estás presente".

¿QUIÉN SE BENEFICIA DE LA EXPANSIÓN DEL METAVERSO?

Evidentemente, el objetivo de Mark Zuckerberg con su anuncio es que su compañía tenga un papel protagonista en el desarrollo del Metaverso, lo que le colocaría en una posición de privilegio

Sus Nubes, **Sus** Datos, **Sus** Claves, **Nuestra** Protección de datos.

¿Está seguro de tener el control total de los datos de su empresa en la nube?

Pregúntese:

- ¿Cómo se crean mis claves?
- ¿Cómo se protegen mis claves?
- ¿Quién tiene acceso a esas claves?
- ¿Qué se puede hacer con esas claves?

Mantenga la seguridad de sus datos sensibles, sistemas y claves de cifrado en su plataforma de nube con nShield HSM y Entrust KeyControl.

Para saber más:
ENTRUST.COM/ES/HSM

ENTRUST

SECURING A WORLD IN MOTION

para recoger los beneficios que se puedan generar. Pero ¿quién más se puede ver beneficiado?

A primera vista, dos compañías que durante años han sido rivales tecnológicos podrían adquirir un protagonismo muy destacado alrededor del Metaverso. Nos referimos a Samsung y Sony. Recientemente, Samsung anunció que la ciudad estadounidense de Taylor albergaría su planta de semiconductores más avanzada, una inversión que representa otra apuesta decisiva de la empresa por el hardware tecnológico y un producto con una demanda mundial que parece no tener fin. Justo antes de este anuncio, la compañía daba a conocer un plan de inversión de 206.000 millones de dólares en tres años, con el objetivo más probable, según indican diferentes analistas, de incrementar su apuesta por el hardware, no por las memorias. Por su parte Sony, que posee desde hace tiempo un estudio de Hollywood, un importante negocio musical y el enorme imperio de videojuegos, está apostando claramente por un liderazgo en el mundo de los contenidos.

PRESENTACIÓN MARK ZUCKERBERG, METAVERSO DE FACEBOOK EN CONNECT 2021

A pesar de toda la ambigüedad que rodea a las visiones de los mundos virtuales, los lugares de trabajo de realidad aumentada y todo lo demás que se ha comentado alrededor del Metaverso, hay dos elementos que parecen seguros: la incesante demanda de hardware, de más memoria, más chips, más sensores y más pantallas, y la convergencia cada vez mayor del entretenimiento, lo que coloca a ambas firmas asiáticas en una posición de privilegio en este terreno.

La firma UBS ha destacado recientemente algunas oportunidades de negocio que se vislumbran con la irrupción del Metaverso. Según estos expertos, son varios los sectores implicados en la construcción de esta realidad virtual, pero se pueden dividir en tres: proveedores de contenidos y plataformas, las interfaces de usuario y la infraestructura. Y, de hecho, UBS ha puesto el foco en el

> **"El Metaverso no es sólo Realidad Virtual. Va a ser accesible a través de todas nuestras plataformas informáticas, incluidas la Realidad Virtual y la Realidad Aumentada, pero también PC, dispositivos móviles y consolas de juegos"**
>
> MARK ZUCKERBERG, CEO DE META

segundo de ellos, ya que son numerosas las posibilidades por la cantidad de productos que se pueden desarrollar.Las interfaces de usuario son todas aquellas que consiguen que los usuarios y sus avatares puedan interaccionar. Un ejemplo de ello son las gafas de Realidad Virtual, que permiten a las personas tener una experiencia inmersiva, con unas sensaciones muy parecidas a la realidad.

En este grupo, los expertos de UBS se fijan en Meta Oculus, HTC Vive, Pico y Sony dentro de la Realidad Virtual (RV); Apple, MSFT HoloLens, DPVR y Magic Leap dentro de la Realidad Mixta (RM); y Meta Nazare, Apple Glasses, Google, Oppo, Xiaomi y Samsung en la Realidad Aumentada (RA).

La entidad, asimismo, cree que en este segmento Logitech tiene una oportunidad de crecimiento importante gracias a los auriculares que está desarrollando para la RV y la RA, con una previsión de crecimiento hasta 60 millones de unidades en 2025 desde las 10 millones de 2021.

Según UBS, son varios los sectores implicados en la construcción de esta realidad virtual, pero pueden dividir en tres: proveedores de contenidos y plataformas, las interfaces de usuario y la infraestructura

UBS indica en su informe que, dentro de la RV y RA, las soluciones de pantalla con óptica y cámara tienen una mayor presencia, un 25%. Se calcula que los envíos a nivel mundial puedan crecer hasta los 1.000 millones de dólares en 2025, quintuplicando la facturación actual. Dentro de este subsector, Meta Oculus tiene el 75% de la cuota de mercado, y se le pueden unir Sony y Apple en 2022. En cuanto a los sistemas de cámaras y lentes, los principales proveedores son LG Innotek, Primax, Cowell, Genius y Sunny Optical.

Pero esto es solo una parte del pastel, porque Cathie Wood, fundadora y directora ejecutiva de Ark Invest, empresa gestora de inversiones, aseguró en CNBC que el metaverso será una oportunidad multimillonaria que afectará a todas las partes de la economía. Según esta experta, "es una gran idea que probablemente se infiltrará, al igual que la tecnología, en todos los sectores, de formas que ni siquiera podemos imaginar en este momento".

Así, una de estas formas de negocio que no podíamos imaginar hace unos meses era la adquisición de bienes inmobiliarios digitales, que parece que ahora se va a convertir en un boom, dado que en pocas semanas ya se han llevado a cabo

24 HORAS EN EL METAVERSO

operaciones de compra y venta de inmuebles virtuales valorados en varios millones de dólares.

ALGUNAS VOCES EN CONTRA DEL METAVERSO

Sin embargo, desde su anuncio el Metaverso no ha sido bien recibido por todo el mundo en el mercado. Uno de los más críticos con la idea de Mark Zuckerberg es Intel, que, en boca de uno de sus vicepresidentes señalaba que la tecnología no está todavía preparada para su desarrollo.

En un reciente post, Raja Koduri, vicepresidente sénior y director general de Gráficos y Sistemas de Computación Acelerada de Intel, señalaba que lograr metaversos verdaderamente inmersivos podría ser un objetivo que no se alcanzará tan pronto, ya que sería necesario aumentar 1.000 veces la eficiencia computacional desde su estado actual.

Koduri considera que llevar a la realidad el concepto de Metaverso demandará una potencia informática exponencialmente mayor que la disponible en las mejores herramientas existentes. Según este ejecutivo, "los metaversos corresponden a una aspiración de habilitar entornos ricos de Realidad Virtual y Aumentada, en tiempo real e interconectados globalmente, que permitirán que miles de millones de personas trabajen, jueguen, colaboraren y socialicen virtualmente. No obstante, crear un universo digital convincente demandaría, no solo mejoras de hardware, sino también a nivel de software y conectividad de Internet. El proceso implicaría crear avatares detallados y renderizar en tiempo real datos de gestos, audio, objetos... para luego transferirlos al ciberespacio con latencias mínimas".

Para Koduri, "el sueño de alcanzar un petaflop de potencia informática y un petabyte de datos en un milisegundo es inalcanzable".

Los metaversos son entornos donde los humanos interactúan social y económicamente como avatares, a través de un soporte lógico en un ciberespacio, que actúa como una metáfora del mundo real, pero sin limitaciones físicas o económicas

ALGUNOS TEMAS PENDIENTES DE RESOLVER

Bien es cierto que hace poco más de dos meses que saltaba a la palestra la idea del Metaverso, pero en el mundo tecnológico eso es mucho tiempo, y todavía quedan por resolver algunas cuestiones importantes que esperemos queden aclaradas lo antes posible.

De hecho, no son pocas las voces que hablan de los retos que el Metaverso y, por extensión, la sociedad real, tienen que enfrentar.

El primero de ellos es que el viaje al mundo virtual dejará fuera a una gran cantidad de personas que no pueden alcanzar el nivel de co-

nectividad necesario. Además, algunos expertos consideran que "los problemas de las redes sociales se amplificarán en este mundo virtual futurista. La polarización, la división y la desinformación se multiplicarán por diez, y el Metaverso fracturará la realidad".

Pero también aparecen nubes negras en el horizonte en forma de problemas alrededor de la privacidad de los usuario. De hecho, al igual que con las redes sociales, un cambio disruptivo de ese calibre en Internet puede suponer un desafío regulatorio, según los expertos en derecho digital, que también precisan que en la Unión Europea se cuenta con las herramientas necesarias para prevenir sus riesgos.

PRIMEROS PASOS EN EL METAVERSO

Con todo, en estas semanas ya hemos asistido a los anuncios de diferentes compañías que llegan al Metaverso. Y una de ellas ha sido la española Zara, que ha presentado su primera colección de ropa para el mundo real y el mundo virtual. En el caso de Oppo, la compañía ha organizado un evento Inno Day 2021 en un entorno virtual. Por su parte, el Centro Blockchain de Cataluña ha anunciado Catvers, un Metaverso Blockchain en catalán con economía propia, que verá la luz oficialmente durante este mes de enero. ■

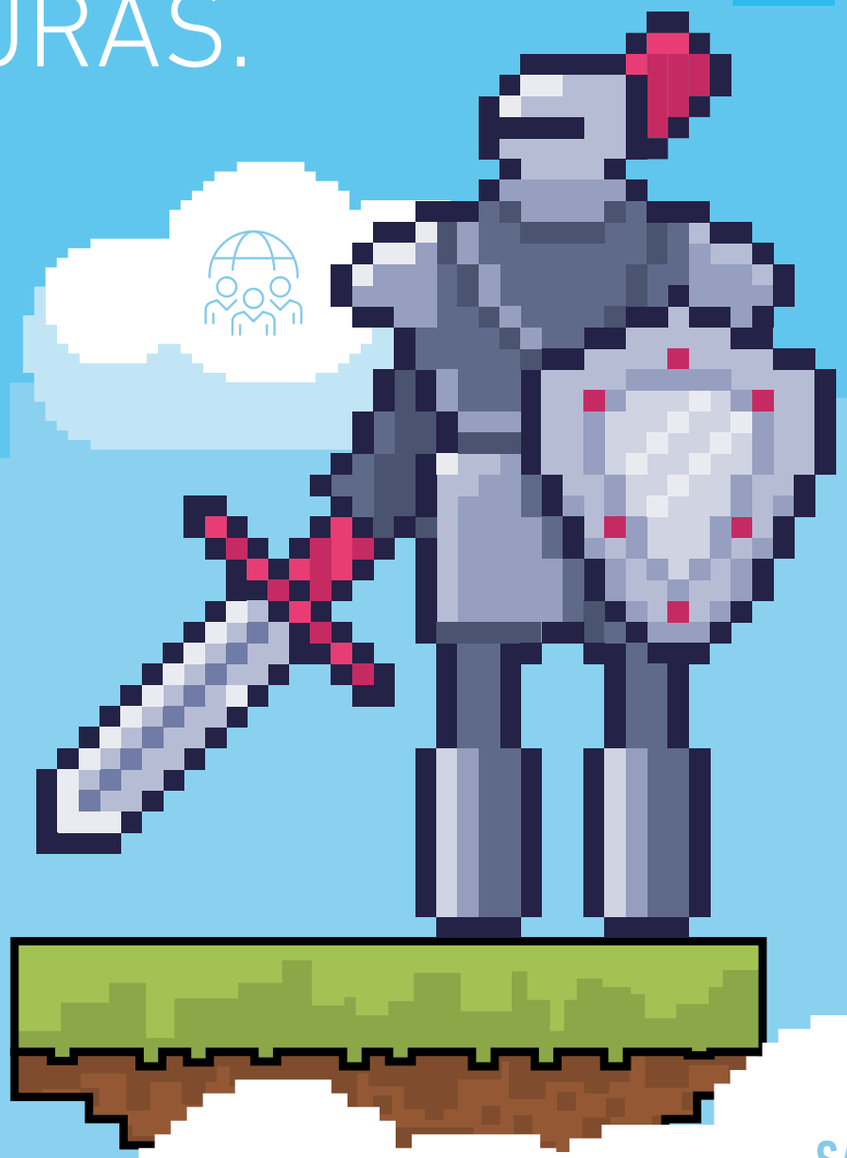
MÁS INFORMACIÓN

- Qué es el Metaverso
- El Metaverso, economía virtual de la Web 3.0
- El origen del Metaverso
- Metaverso, ¿futuro de la convivencia humana?
- The Verge: entrevista a Mark Zuckerberg
- Metaverso, el mundo virtual de Mark Zuckerberg
- Samsung y Sony, una rivalidad que puede reavivarse en el Metaverso
- Oportunidades de negocio en el Metaverso
- Metaverso, una oportunidad de inversión milmillonaria
- Revolución en la adquisición de bienes inmobiliarios digitales
- El Metaverso dejará fuera a los no conectados
- Metaverso, un desafío para la privacidad
- El mundo no está preparado para el Metaverso
- Zara presenta su primera colección de ropa para el mundo real y virtual
- Oppo organiza su Inno Day 2021 en el mundo virtual
- Catvers, un mundo virtual en catalán
- Las tecnologías del metaverso ayudarán al modelo de fabricación inteligente
- De la era Post-PC al Metaverso

SASE, LA ARQUITECTURA EMERGENTE QUE OFRECE UNA CONEXIÓN SEGURA Y SIN FISURAS.

IKUSI velatia

cisco Partner



CONTROLA EL ACCESO SEGURO DESDE TU CENTRO DE DATOS HASTA LA NUBE

GOOGLE CLOUD

AZURE

OFFICE 365

WORKDAY

SALESFORCE

En Ikusi te mostramos el camino... Contáctanos en **www.ikusi.com**

#ENCUENTROSITTRENDS

Tendencias de ciberseguridad 2022: la ciberinteligencia entra en escena

Los ciberataques llevan creciendo en cantidad y en sofisticación desde hace años, y nada hace pensar que el año próximo vaya a cambiar la tendencia. Los ciberdelincuentes se esmeran cada vez más, han creado un negocio extremadamente rentable y siguen estando lejos de las autoridades.

Como consecuencia, las pérdidas financieras de los ciberataques se han multiplicado, así como los daños reputacionales.

Todo apunta a que en 2022 veremos más ataques de ransomware, porque siguen funcionando y porque se ha dado una vuelta de tuerca con la doble extorsión, que provoca una situación insostenible. La cadena de suministro seguirá siendo uno de los vectores preferidos de ataque para los ciberdelincuentes, y las actualizaciones a Windows 11 una excusa perfecta para dejar puertas abiertas por las que entren los malos.

Llevamos tiempo hablando de la inseguridad móvil y mucho más del phishing, que sigue estando presente en un altísimo porcentaje de los ciberataques exitosos. ¿Será 2022 el año en que consigamos hacerles frente?

De todo ello, así como de algunas tecnologías que llegan para hacer frente a las amenazas más avanzadas, hemos hablado en la sesión on-line Tendencias de ciberseguridad 2022: la ciberinteligencia entra en escena, en la que se incluyen dos debates con expertos del mercado de ciberseguridad, y en una entrevista con Pere Blay Serrano, Director del Máster en Ciberseguridad de VIU - Universidad Internacional de Valencia. ■

netwrix

UN MUNDO PROTEGIDO CONTRA LAS CIBERAMENAZAS

En una era de ciberamenazas constantes, ¿cómo puede hacer que su organización sea más segura de lo que es actualmente?

Netwrix ayuda a más de 10.000 organizaciones en todo el mundo:

- Supere la seguridad en silos eliminando los puntos ciegos
- Siga las mejores recomendaciones para identificar, gestionar y reducir el riesgo de ciberseguridad

Potente seguridad de datos, identidades e infraestructura con sencillez

www.netwrix.es

PERE BLAY SERRANO, Director del Máster en Ciberseguridad de VIU - Universidad Internacional de Valencia

“La falta de profesionales con los conocimientos adecuados es uno de los problemas a los que se enfrenta el mercado”

“2021 ha sido un año complicado”, dice Pere Blay Serrano, Director del Máster en Ciberseguridad de la Universidad Internacional de Valencia (VIU), añadiendo que aún arrastramos los efectos de la pandemia, cuando se ha disparado el teletrabajo y el uso de internet, “un nicho perfecto para que se desarrollen todo tipo de ataques, ya conocidos y nuevos, por parte de los ciberdelincuentes”.

ENTREVISTA: “El de la ciberseguridad en España es un sector fuerte y muy dado a colaborar”, Pere Blay Serrano (VIU)

De cara a 2022, asegura Blay Serrano, los ataques crecerán porque "es un mercado en auge y es relativamente sencillo montar campañas de phishing, que se ofrecen como servicio".

A pesar de que sigue habiendo una tendencia al "esto a mí no me va a pasar", asegura el director del Máster en Ciberseguridad de VIU, que las empresas empiezan a darse cuenta de los problemas que ocasionan los ciberataques, y se ha notado un incremento en la concienciación a la hora de protegerse. En todo caso, "todavía no se reporta o se hace cuando han pasado meses del incidente, cuando el daño ya es muy superior". Añade también que, aunque las empresas grandes son las que pueden permitirse un equipo dedicado, organizaciones como INCIBE ofrecen mucha información "para que todo tipo de empresas sepan cómo protegerse y cómo reaccionar ante incidentes".

Tiene la esperanza Pere Blay Serrano de que, después del año de ataques que hemos visto, "las empresas empiecen a concienciarse de la necesidad de prevenir para minimizar el impacto, el tiempo de recuperación y las penas económicas", y añade que resulta interesante ver la mayor proliferación de empresas que empiezan a ofrecer ciberseguros para ayudar a las empresas a recuperarse de un incidente.

El de la ciberseguridad en España es un sector fuerte y muy dado a colaborar en formación, dice Blay Serrano, apuntando a la falta de profesionales con la formación adecuada como uno de los problemas a los que se enfrenta este mercado, un inconveniente que se afronta con un crecimiento de los servicios gestionados de seguridad. ■

"Los ataques crecerán porque es un mercado en auge y es relativamente sencillo montar campañas de phishing, que se ofrecen como servicio"

Una única plataforma.
Un único agente.
Una única vista.

Qualys Cloud Platform y su poderoso Agente Cloud proporcionan una solución completa que cubre TI, seguridad y cumplimiento, desde la prevención hasta la detección y la respuesta

¡Pruébalo gratis!

qualys.com/free-trial

Qualys®

#ENCUENTROSITTRENDS

Ciberseguridad en 2022:
de la seguridad OT a la cadena de suministro

La ciberseguridad es un elemento básico en cualquier actividad empresarial, independientemente del tamaño de las compañías o del sector económico en el que operen. Las amenazas son cada día más sofisticadas y, por ende, las herramientas y políticas para combatirlas deben serlo también, adaptando nuevas tendencias tecnológicas como Inteligencia Artificial o Machine Learning.

Pero, ¿cuáles serán las principales líneas que definirán el segmento de la ciberseguridad a lo largo de los próximos meses? Hemos debatido con algunos expertos para conocer, de primera mano, qué tendencias vislumbran en el horizonte y cómo las políticas y estrategias de seguridad de las entidades deben adaptarse para poder mantener protegidos los datos, las aplicaciones y los dispositivos.

Horatiu Bandoiu, Channel Marketing Manager de Bitdefender; Jacinto Grijalba González, Cyber Security Sales Manager de CyberRes; Javier Sánchez Fuertes, Territory Sales Manager de Entrust; Sergio Martínez, Country Manager Iberia de SonicWall; Javier Donoso, Sales Engineer de Sophos; Borja Pérez, Country Manager Iberia de Stormshield; y Guillermo Fernández, Manager Sales Engineering de WatchGuard, participaron en este debate moderado por Rosalía Arroyo, Directora de IT Digital Security. Clica en la imagen para ver el vídeo.

BITDEFENDER

“Vamos a sufrir más ataques avanzados dirigidos a las infraestructuras críticas”

HORATIU BANDOIU, CHANNEL MARKETING MANAGER DE BITDEFENDER

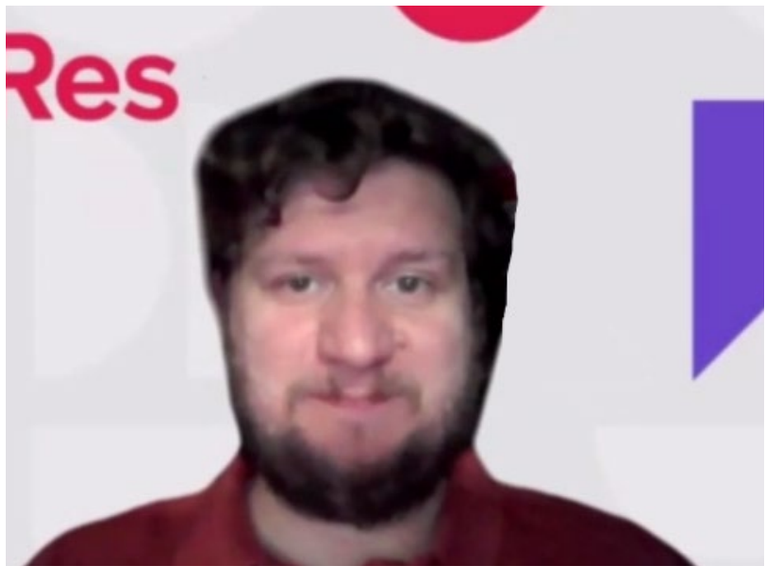
“El ransomware será, también en 2022, un grave problema de seguridad”

Para Horatiu Bandoiu, Channel Marketing Manager de Bitdefender, el ransomware va a seguir estando presente y será cada vez más avanzado. “Vemos un gran incremento de los ataques dirigidos, de los ataques avanzados. Yo destacaría que vamos a sufrir más ataques avanzados dirigidos a las infraestructuras críticas, sea de tipo ransomware o Asymmetric Cyberwarfare, donde ya entran otros países”.

Bandoiu señala dos tendencias claras a la hora de hablar de los EDR. Una gran parte de las soluciones del ámbito de la detección y respuesta se van a transformar en soluciones como XDR. Las soluciones EDR han probado su eficacia en la detección de los ataques avanzados a nivel de endpoint y es lógica su extensión a todos los activos. Las plataformas de analítica de seguridad van a ganar más inteligencia y van a emplear también más Machine Learning. Por otro lado, especialmente en la PYME, empiezan a darse cuenta de que se han enfocado demasiado en la detección y respuesta y se han olvidado de la prevención. “Sin una buena prevención, nos estamos enfocando a la detección, pero permitimos, por ejemplo, que el ransomware llegue hasta donde ha llegado. Probablemente, todo se va a canalizar hacia las soluciones XDR”.

Este portavoz espera que las PYMES dejen de ser las grandes olvidadas. “En teoría, van a tener recursos para modernizarse y para crecer de la mano de la Transformación Digital, para fomentar la innovación y las nuevas tecnologías y pasar a la nube”. En este contexto, la ciberresiliencia ya no es un sueño disponible solo para las empresas más grandes, será alcanzable para todos. Bandoiu indica que una seguridad fuerte solo se va a conseguir de 2 maneras: si tienen recursos internos, se van a orientar a plataformas integradas de ciberseguridad que puedan cubrir varias necesidades a nivel de endpoint, redes o la cloud, y también a reforzar el equipo humano. Si no tienen recursos, será una gran oportunidad para los proveedores de servicios gestionados.

CYBERRES



"Es muy probable que cada vez más se utilicen algoritmos de Inteligencia Artificial basados en Machine Learning para hacer ataques"

JACINTO GRIJALBA GONZÁLEZ, CYBER SECURITY SALES MANAGER DE CYBERRES

"Ofrecemos un catálogo único que, además de proteger, ayuda a recuperarse de un ataque"

Para Jacinto Grijalba González, Cyber Security Sales Manager de CyberRes, a Micro Focus line of business, los ciberatacantes están desarrollando nuevo malware que va a aprender nuevas técnicas por sí mismo: "la única manera de poder parar esta oleada que va a venir alrededor de estos nuevos tipos de ataque que van a utilizar Inteligencia Artificial, es utilizar la propia IA para pararlos: poner una serie de contramedidas que se basen también en algoritmos de Machine Learning".

Jacinto Grijalba cree que una de las tendencias para este 2022 será el Machine Learning no supervisado. Hay muchos tipos de ataques nuevos, cada vez más avanzados, ante los que no se pueden utilizar sistemas estáticos o relativamente dinámicos. "Tienen que ser sistemas que puedan aprender solos y que no tengan ni gente ni equipo detrás que pueda trabajar con ellos, porque también uno de los problemas que estamos viendo en España es la falta de recursos humanos, de personal formado en la ciberseguridad". Para este portavoz, "igual que el ransomware está evolucionando a métodos de propagación que utilizan algoritmos de Inteligencia Artificial, y va aprendiendo, la única manera de poder detectar esto es a nivel de anomalías, a nivel del uso de mecanismos de Inteligencia Artificial, de Machine Learning".

Para Jacinto Grijalba, la información es poder, pero hay que saber utilizarla. "Ese enfoque global a veces es muy difícil alcanzar, porque nos bombardean diariamente con información, mucha de ella no veraz, y en el mundo de la ciberseguridad pasa igual. Cuando una organización se ve atacada le viene información de muchísimos lados". Este responsable señala que para que esa información sea realmente útil hay que aplicar la inteligencia. "Inteligencia ante todo, con la información adecuada".

SECURE ACADEMY

TU CENTRO AVANZADO DE FORMACIÓN EN CIBERSEGURIDAD

www.secureacademy.es

Secure&IT by LKS

ENTRUST

“Sencillamente, quiero tener el control sobre esas claves de cifrado, porque son mis claves”

JAVIER SÁNCHEZ FUERTES, TERRITORY SALES MANAGER DE ENTRUST

“Los responsables de seguridad en la nube no saben cómo se protegen o generan las claves de cifrado”

El Blockchain va a ser la tendencia que va a liderar las iniciativas de Ciberseguridad en 2022. Al menos, así lo indica Javier Sánchez Fuertes, Territory Sales Manager de Entrust, al señalar que “con las finanzas descentralizadas, los NFT, los metaversos y la gestión de identidades asociadas al metaverso”, va a ser una tendencia importante en el mercado en 2022.

Centrándose en el cifrado, Sánchez Fuertes subraya el control de las claves en los proveedores públicos de nube. “Hace 2 o 3 años, cuando la gente empezaba a abrazar el mundo de la nube, lo hacía con absoluta confianza, pero pasado el tiempo la gente empieza a preguntarse cómo se gestionan las cosas, en concreto las claves”. Los responsables de seguridad con mayor sensibilidad empiezan a preguntarse quién crea las claves, cómo las crea, qué derechos hay asociados a las mismas, si se pueden compartir, si las pueden exportar, si hay alguna política de rotación de claves... “no es que no confíe en mi proveedor público de nube, es que, sencillamente, quiero tener el control sobre esas claves, porque son mis claves. Lo que no quiero perder en ningún caso es la soberanía sobre esas claves”.

Sánchez Fuertes cree que las empresas harán ese movimiento de adopción de servicios de HSM en la nube en la medida en la que el proveedor de ese servicio dé confianza a la empresa. Los proveedores de nube pública ya ofrecen ese servicio, pero hay muchas cosas que las empresas desconocen alrededor de cloud. “Nosotros tenemos una particularidad a la hora de proteger las claves y es que las protegemos fuera del HSM, pero las protegemos cifradas. Esto permite que, con independencia de que el HSM esté como servicio en cualquiera de nuestros CPD, el cliente, si quiere, puede tener las claves. Eso es un elemento diferencial que va a ayudar a la adopción del HSM como servicio”.

SONICWALL

“El ransomware está creciendo a un 150%”

SERGIO MARTÍNEZ, COUNTRY MANAGER IBERIA DE SONICWALL

“La mejor opción posible es una defensa coordinada por capas”

Para Sergio Martínez, Country Manager de SonicWall Iberia, el ransomware sigue siendo la tendencia más importante de Ciberseguridad. “El ransomware ha crecido un 150% en los tres primeros trimestres del año, con respecto a los del año pasado”. Se trata de un ransomware muy selectivo, que viene de un crimen organizado mucho más dirigido, con muchas herramientas de Inteligencia Artificial para realizar la extorsión a cualquier tipo de empresa.

La complejidad de los ecosistemas de seguridad, con multitud de herramientas, está provocando el llamado efecto Platform-over-platform, lo que también será tendencia en 2022. “Al final, el Esquema Nacional de Seguridad es un ejemplo que recomienda el uso de múltiples fabricantes. Esto genera la necesidad de desplegar múltiples plataformas”. Martínez indica que en esta nueva TI distribuida, se ha creado una superficie de exposición sin precedentes con el teletrabajo, las operaciones, el shadow IT… con un enorme incremento de los ataques de todo tipo, pero muy dirigidos, y con un presupuesto de ciberseguridad que este año podría aumentar gracias a los Fondos Next Generation.

“Verificar la identidad tiene 3 componentes para hacerlo: algo que sabes, algo que tienes y algo que eres. La Unión Europea y las entidades bancarias están exigiendo ya dos componentes y se están utilizando mucho los dos primeros elementos. La password al final es un secreto compartido, es algo que se debe almacenar en algún sitio y éste es el primer problema, porque eso se puede robar”. El segundo problema para el portavoz es la reutilización de esa password. Esto genera inquietud por su uso, pero en el fondo los factores biométricos tienen el mismo problema. “También estás compartiendo esa información que no deja de ser un hush que está almacenado en algún sitio y también se reutiliza, porque tu cara es la misma siempre. Realmente esto tiene que ir mucho más allá”. Por ello, es importante desplegar una defensa por capas y tener visibilidad central de lo que ocurre en la red, para poder aislar y detectar los ataques, y poder así responder en tiempo real.

SOPHOS

“Este año 2022 este modelo RaaS va a seguir dominando el panorama de las amenazas”

JAVIER DONOSO, SALES ENGINEER DE SOPHOS

“Seguimos apostando por nuestro modelo XDR”

Un ecosistema de seguridad adaptativo, en el que todas las soluciones involucradas sean capaces de sincronizarse entre sí para poder tomar acciones de manera autónoma, y la unión del mundo de la Inteligencia Artificial con el de los profesionales que están trabajando en la Ciberseguridad, serán las principales tendencias en 2022, según Javier Donoso, Sales Engineer de Sophos.

También señala la movilidad. “Esperamos que estas amenazas móviles y estas estafas e ingeniería social continúen ganando terreno y se diversifiquen aún más entre particulares y empresas. Hay claros ejemplos de que esto va a seguir siendo así. Hay mucho malware que está enfocado exclusivamente a este tipo de plataformas”. Javier Donoso, además, habla del smishing, que es una forma relativamente nueva de ciberataque que está dominando el mercado y que intenta suplantar identidades, ya sean de personas físicas o jurídicas. “Al final, lo que intentan es engañarte y que tú pinches en ese enlace para que el ciberatacante que está detrás consiga el control de tu teléfono y te expolie los datos, te los secuestre, te amenace, te extorsione… cualquier cosa”.

“El ransomware se ha convertido en un elemento importantísimo en el ecosistema cibercriminal”. Este tipo de malware es el más dañino, y sigue manteniendo en vilo a todos los administradores y a todas las empresas de ciberseguridad. “El cambio más importante que hemos visto, y se espera que continúe así, es que antes un atacante escribía su código y ejecutaba el ataque desde el principio hasta el final, y ahora hay cibermafias que escriben su código y lo que hacen es venderlo, intentan sacar rédito de este código alquilándoselo o vendiéndoselo como servicio a otras cibermafias, como si fuera un programa legítimo, el famoso RaaS (Ransomware as a Service). Pensamos que en este año 2022 este modelo RaaS va a seguir dominando todo este panorama de las amenazas”.

2021

SONICWALL® INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

A medida que las situaciones de trabajo evolucionaron en 2021, también lo hicieron los **métodos de los actores de las amenazas y los perpetradores motivados**.

En la **actualización semestral del Informe de Ciberamenazas 2021 de SonicWall**, se analiza cómo los actores de las amenazas utilizan cualquier medio necesario (**controles de seguridad laxos, vulnerabilidades sin parches, ataques de día cero y debilidades en la cadena de suministro**) para obtener beneficios maliciosos y provocar disturbios a nivel mundial.

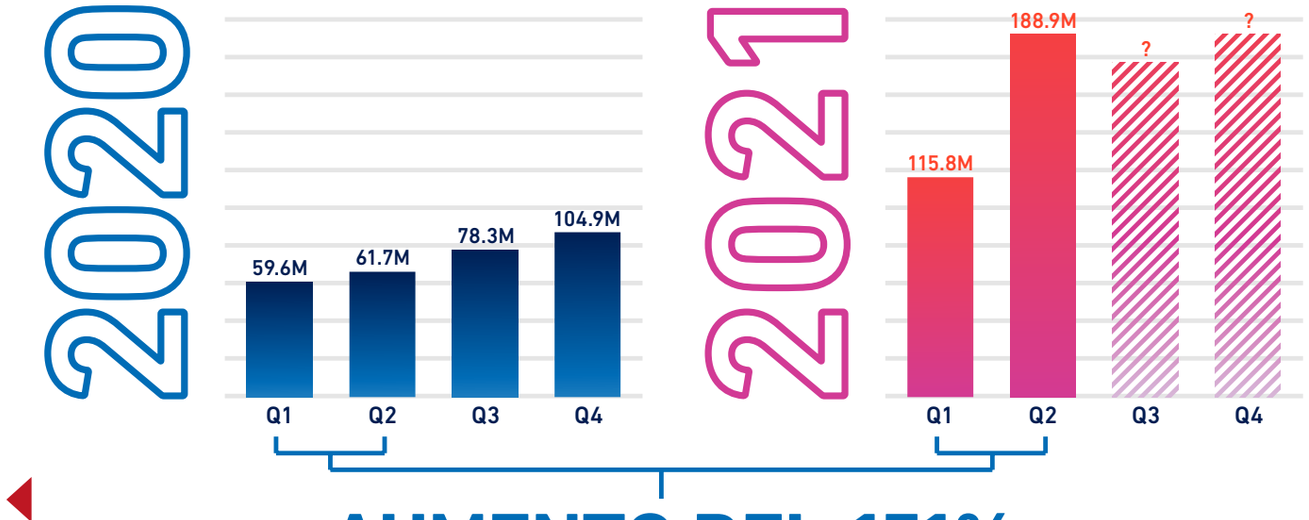
OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

EL RANSOMWARE ALCANZA SU MÁXIMO HISTÓRICO

Los ataques de ransomware en el primer semestre de 2021 ya han eclipsado todo el volumen total de 2020: **un aumento del 151% en lo que va de año.**

En los primeros seis meses de 2021, el volumen mundial de ransomware alcanzó la cifra sin precedentes de **304,7 millones** de intentos de ataque.



AUMENTO DEL 151%

TENDENCIAS MUNDIALES DE LOS CIBERATAQUES

-22%
2.5 billones
ATAQUES DE MALWARE

+151%
304.7 millones
ATAQUES DE RANSOMWARE

+59%
32.2 millones
ATAQUES DE IoT

+26%
2.1 millones
AMENAZAS CIFRADAS

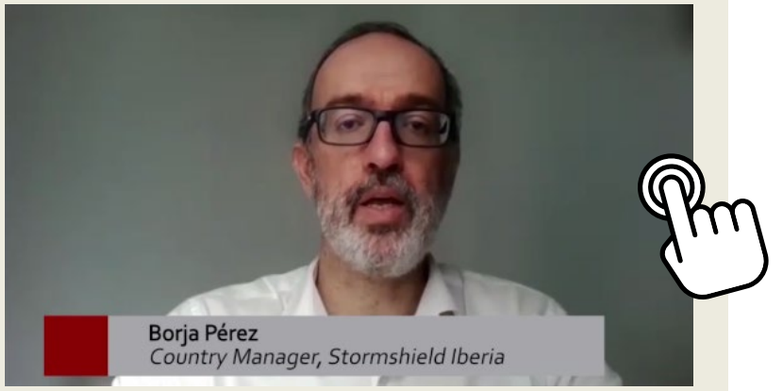
+23%
51.1 millones
ATAQUES DE CRYPTOJACKING

+9%
2.5 trillones
INTENTOS DE INTRUSIÓN

STORMSHIELD

“Creo que a veces somos injustos poniendo la responsabilidad sobre el usuario”

BORJA PÉREZ, COUNTRY MANAGER IBERIA DE STORMSHIELD



“Hemos de tener los datos debidamente cifrados y guardados”

Para Borja Pérez, Country Manager de Stormshield Iberia, el ransomware y los ataques de denegación de servicio van a seguir estando en el centro del huracán en este 2022. “También destaca la importancia que va a adquirir el Esquema Nacional de Seguridad, porque muchos de los fondos europeos que recibiremos para digitalización de empresas van a ir asociados a proyectos de ciberseguridad”.

A la hora de hablar de la seguridad del mundo OT, Borja Pérez señala que “todos tenemos en mente ataques a todo tipo de industrias. Cada semana tenemos un incidente en entorno industrial que aparece en los medios de comunicación. Esta tendencia va a seguir”. El entorno industrial es un sector muy heterogéneo, que tradicionalmente ha estado aislado, no ha estado expuesto al mundo TI, y que se está digitalizando muy rápido. “Muchas veces también es un problema más que de tecnología, de organización, con departamentos de TI aislados de OT”.

A la hora de hablar de concienciación, este portavoz señala que “soy muy partidario de tener a nuestro personal lo más concienciado posible, pero también de actuar como si no estuviesen concienciados. Creo que a veces somos injustos poniendo la responsabilidad sobre el usuario”. Los ataques son cada vez más dirigidos, personalizados y sofisticados. Alguien que no se dedica a ciberseguridad puede cometer errores y puede abrir puertas a ataques; por ello, toda concienciación es buena. “Concienciación sí, toda la que se pueda, e incluir la formación de los empleados en ciberseguridad dentro de las formaciones de Recursos Humanos, igual que la de riesgos laborales, pero los responsables de TI, de ciberseguridad, los CISO, deben de poner medidas considerando que los usuarios no tienen ningún conocimiento”.

WATCHGUARD

“La complejidad es el enemigo de la seguridad”

GUILLERMO FERNÁNDEZ, MANAGER SALES ENGINEERING DE WATCHGUARD

“Automatizar la actualización de aplicaciones es clave”

El ransomware va a seguir siendo una tendencia muy clara en 2022. Además, Guillermo Fernández, Manager Sales Engineering de WatchGuard, señala el robo de identidad y el smishing, que se va a dirigir hacia las aplicaciones de mensajería instantánea. “Vamos a ver cómo los atacantes abordan esas otras líneas que hasta ahora no se estaban viendo”.

“Todo lo que son los ataques a la cadena de suministro no es algo nuevo, existen desde hace muchísimos años, ha habido ejemplos muy sonados”. Para Guillermo Fernández, la filosofía vuelve a ser la misma: es la búsqueda de cuál es el eslabón más débil. “Al final el nivel de seguridad que vamos a tener va a ser aquél que esté determinado por el más débil de todos”. Es posible que un proveedor pueda ser el vector de entrada para poder llegar a una empresa mayor. “Hemos visto algunos casos de empresas que daban servicios gestionados y, lógicamente, con toda esa gestión han hecho una distribución de malware en muchísimos clientes finales”.

Según Guillermo Fernández, cada vez se va a escuchar hablar más del Cybersecurity Mesh. “Los clientes optan por tener diferentes productos dentro del mercado de la ciberseguridad de diferentes fabricantes. Al final es el lema de siempre, la complejidad es el enemigo de la seguridad. Si tengo diferentes productos que actúan de forma autónoma y de forma aislada, representan siempre un riesgo, por errores de configuración, por los motivos que sean. Muchas veces, cuando se hace un estudio de cómo una empresa ha sido atacada, no es porque no contaran con tecnología, todo lo contrario, pero normalmente siempre ha habido algún tipo de error”. Para este portavoz, la propuesta que se hace cuando se habla de Cybersecurity Mesh es apostar porque haya un orquestador, para que resulte más sencillo que todos estos productos se combinen a la hora de hacer un despliegue. ■

Si te ha gustado este artículo, compártelo

La educación, uno de los sectores más afectados por el ransomware.

Sophos Endpoint

Intercept X

Bloquee los ataques de ransomware antes de que causen estragos en su entorno con tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

sophos.com/es-es/endpoint

SOPHOS
Cybersecurity evolved.

21-09-20 ES(DD)

#ENCUENTROSITTRENDS

Ciberseguridad en 2022: avanzando hacia la Cybersecurity Mesh

Los entornos corporativos son cada vez más complejos. El perímetro tal y como se planteaba hace algunos años, ha desaparecido, y cada día son más los usuarios, servicios y dispositivos que trabajan fuera de la infraestructura corporativa, lo que es una pesadilla para los responsables de la seguridad de la empresa.

Por este motivo, las soluciones de ciberseguridad deben proporcionar, en primer lugar, la mayor visibilidad posible de los recursos conectados a la red corporativa, con el fin de saber, en todo momento, lo que está pasando. Pero, además, tienen que ofrecer capacidades analíticas para permitir a los responsables anticiparse a los posibles problemas o ataques que puedan acontecer, dado que es mejor una seguridad proactiva que no una reactiva.

Asimismo, y dado que cada vez son más las herramientas de diferentes proveedores y con distintas funciones que conviven en una plataforma de seguridad, es imprescindible la adecuada coordinación entre todas ellas, con el fin de poder ofrecer la mejor respuesta posible en cada momento y ante cualquier situación que se pueda producir.

Luigi Semente, Sales Specialist de Citrix; Daniel Howe, Senior Sales Engineer de Fastly; Héctor Manubens, Account Manager de Ikusi; Jesús Sáez, Country Manager Spain & Portugal de Netwrix; Sergio Fernández, Technical Account Manager de Qualys; y Francisco Valencia, Director General de Secure&IT, participaron en este debate, moderado por Rosalía Arroyo, Directora de IT Digital Security. Clica en la imagen para ver el vídeo.

CITRIX

“Hay que garantizar la seguridad de los activos sin impactar negativamente en la experiencia del usuario”

LUIGI SEMENTE, SALES SPECIALIST DE CITRIX

“Nuestra propuesta de valor es una seguridad consistente y coherente”

Para Luigi Semente, Sales Specialist de Citrix, el perímetro de seguridad cada vez va a estar más dilatado el próximo año. En 2022, la pandemia seguirá afectando las decisiones de muchas empresas y se irá hacia un modelo híbrido, que implica tener distintos tipos de usuarios que se conectarán desde cualquier red a los activos corporativos. La clave será “garantizar la seguridad de esos activos pero sin impactar negativamente en la experiencia del usuario”.

“Creemos que hay que adoptar tecnologías que, de forma transparente para el usuario, puedan controlar en cada momento cuál es el contexto de acceso, chequear si un usuario está trabajando según su perfil, y aplicar de forma proactiva medidas de seguridad”.

Luigi Semente incide en que “este año vamos hacia un modelo de trabajo híbrido totalmente, y a nivel de seguridad supone un reto muy importante”. Este portavoz cree que en 2022 las empresas sí se van a mostrar dispuestas a añadir algunos controles o elementos adicionales de seguridad, por ejemplo, en la parte de la post-autenticación del usuario. Controles que sean capaces de definir desde dónde y cómo se está conectando ese usuario para asegurar que es quien dice que es.

Para este responsable, la clave va a ser utilizar soluciones que sean flexibles. “Es fundamental disponer de soluciones que se puedan desplegar en los diferentes repositorios donde a día de hoy pueda estar una arquitectura”. Es importante tener una solución que pueda hablar con el ecosistema, que pueda incluir también una visibilidad total de aquellos elementos que se definen como activos corporativos. “No es lo mismo tener una arquitectura, una situación donde tengo a mis usuarios con mi CPD dentro de mi perímetro, que empezar a dar servicio a toda una serie de usuarios y de casos de uso que empiezan a necesitar, a lo mejor, servicios que van a estar fuera de nuestra casa. La flexibilidad y la interoperabilidad con el ecosistema es el elemento más importante que tenemos que perseguir”.

FASTLY

“Estamos viendo una explosión de elementos conectados a todos los niveles corporativos”

DANIEL HOWE, SENIOR SALES ENGINEER DE FASTLY

“Los WAF tradicionales se han quedado obsoletos”

Daniel Howe, Senior Sales Engineer de Fastly, señala la gran cantidad de dispositivos y puntos de acceso a la red con los que cuentan las empresas de hoy y subraya que “estamos viendo una explosión de elementos conectados a todos los niveles corporativos. El crecimiento de los microservicios y toda la ampliación de elementos en la nube, hacen que haya una variedad brutal de puntos de posible acceso a las corporaciones”.

La seguridad es algo fundamental. “Si tu negocio se basa en estar conectado hoy en día y pierdes la credibilidad o tienes un data breach, sabemos que hasta el 50% de las empresas no salen adelante. Esto es algo muy serio, los CISO tienen que estar en los comités de dirección de las empresas”. Para este portavoz, hay que dar seguridad y garantizar la visibilidad de la plataforma, que todos los elementos críticos puedan ser vigilados y securizados.

Daniel Howe cree que el hecho de que las herramientas de un stack de seguridad sean capaces de detectar intenciones, y no únicamente amenazas específicas, es algo importante. “Vamos a ir viendo cómo se va a ir aplicando más lógica y un poquito más de inteligencia”. Este año, la evolución del sector se va a dirigir hacia el análisis para garantizar que los falsos positivos se reduzcan drásticamente y poder estar a la vez más securizados y controlados ante nuevas vulnerabilidades.

Este responsable también resalta la importancia de la observabilidad en el ámbito de la seguridad y de las integraciones de distintos proveedores en una única interfaz. “Lo que no tiene ningún sentido es que cada uno de los fabricantes vayamos viniendo con nuestro libro”, declara a la hora de abordar este tema. Integración, adaptabilidad y visibilidad, son los conceptos más importantes bajo su punto de vista.

IKUSI

“Si la ciberdelincuencia fuera un país, sería el tercero del mundo”

HÉCTOR MANUBENS, ACCOUNT MANAGER DE IKUSI

“Ofrecemos SASE como un servicio administrado”

“La principal amenaza, el principal worry point, es hacer frente a la ciberdelincuencia. Si la ciberdelincuencia fuera un país, sería la tercera economía del mundo”, comienza su discurso Héctor Manubens, Account Manager de Ikusi, que señala que la ciberdelincuencia como servicio se ha convertido en un auténtico negocio. “La principal preocupación y reto al que se enfrenta la industria es el aumento de la ciberdelincuencia, que se ha convertido al final en un negocio rentable. Los hackers no van a dañar reputación y a ser el más popular de su círculo de amigos, sino que lo ven como un modelo de negocio, tienen ingresos y gastos y lo ven como una forma de ganarse la vida”.

A la hora de hablar sobre el Cybersecurity Mesh, Héctor Manubens indica que “ya los usuarios acceden desde cualquier parte, es el work from everywhere, se trabaja desde cualquier punto, y, por lo tanto, hay que pasar a no solo proteger la red sino a temas de identidad, quién se conecta, desde qué lugar. Hay que considerar que todas las conexiones pueden no ser seguras, ya no te puedes fiar de ningún flujo de carga. Cybersecurity Mesh se apoya en la microsegmentación, es decir, a cada acceso o a cada dispositivo que se conecta, microsegmentarlo y poder darle esos barnices de ciberseguridad”. Cybersecurity Mesh sería una evolución de Zero Trust donde es posible hacer frente a las nuevas arquitecturas que van a surgir.

Al hablar sobre el efecto Platform-over-platform, este responsable señala que “la realidad es que los CISO están hartos de tanta plataforma. Según Gartner, el 78% de los CISO dicen tener 16 o más herramientas o plataformas de ciberseguridad”. Para este portavoz “hace falta llegar a un momento de normalización y, de alguna manera, no reinventar la rueda constantemente”, lo que se traduce en ciertos mecanismos para poder llegar a los mismos insights que permitan esa acción proactiva para prevenir los ataques antes de que se produzcan.

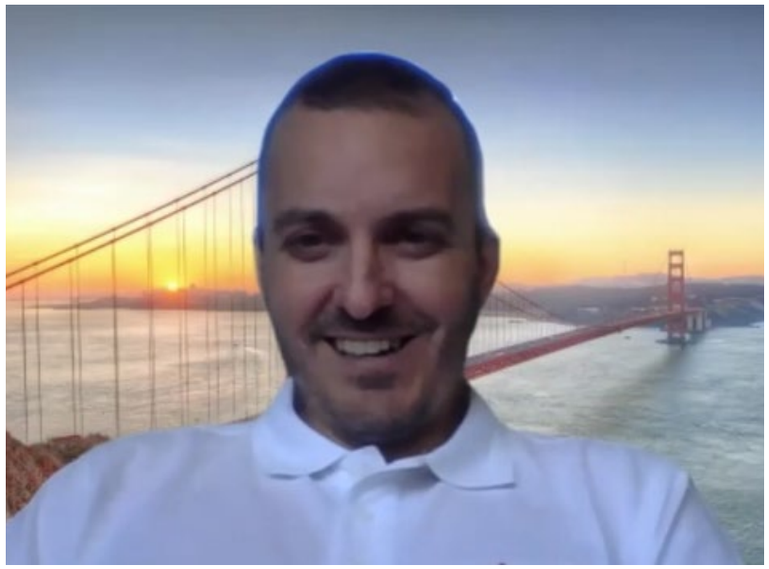
STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

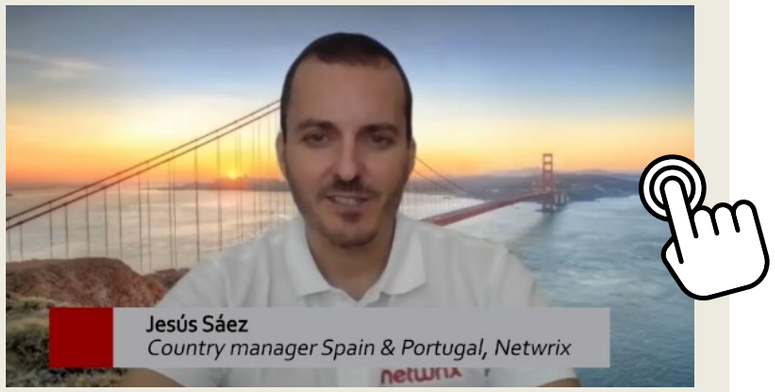
www.stormshield.com

NETWRIX



“No todo es ransomware”

JESÚS SÁEZ, COUNTRY MANAGER SPAIN & PORTUGAL DE NETWRIX



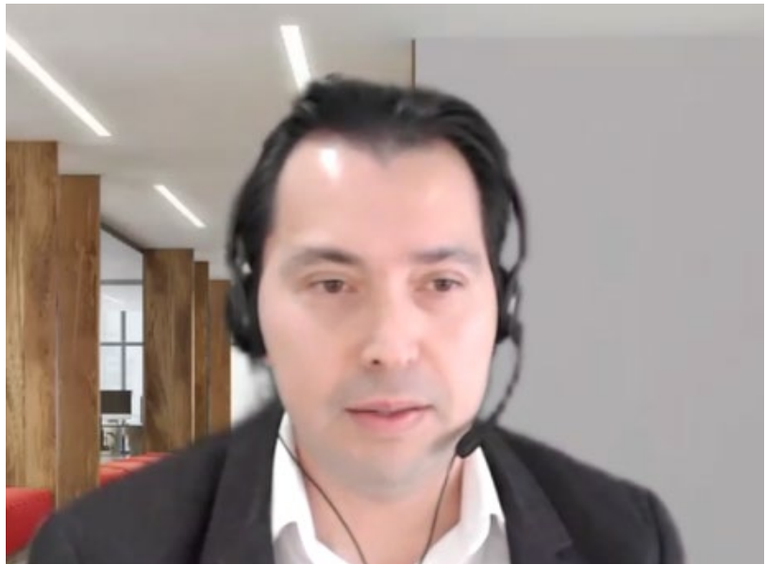
“Ransomware, exfiltraciones de datos y concienciación, serán los focos en 2022”

“El reto fundamental es la ciberdelincuencia. El tema del ransomware no lo vamos a poder contener, va a seguir creciendo. No hace falta ser un gurú para darse cuenta de que van a seguir por esa línea, que realmente está siendo muy difícil de parar y están sacando mucho dinero”. Jesús Sáez, country manager Spain & Portugal de Netwrix, señala que para hacer frente a estas amenazas hay herramientas, pero hacen falta presupuestos. “Si no te proteges, si no pones dinero encima de la mesa para tomar acciones, vas a ser atacado”.

Para Jesús Sáez, la seguridad gira cada vez más en torno a la identidad y los datos. “No todo es ransomware. Hay gente que se preocupa por robar información para venderla, para sacar provecho de ella”. Este portavoz indica que el control del acceso a los datos debería ser algo completamente estratégico para cualquier CIO dentro de la organización, y hace hincapié en la necesidad de tener visibilidad. “Muchas veces los ataques empiezan por los sitios más recónditos”.

Jesús Sáez indica que el cumplimiento normativo también es un reto importante. “La normativa es algo que lleva muchos años en la industria. Yo soy un defensor de las normativas, creo que son necesarias, que realmente aportan. Pienso también que cada compañía realmente debe extraer lo que es interesante de esas normativas para su negocio”. Para este responsable también es necesario que las empresas tengan herramientas que les ayuden a reducir tiempos en este sentido: “Bastante complicado es sacar la TI en el día a día, con todas las problemáticas existentes, y poder defenderte para que no te roben los datos, para que no tengas un ataque de ransomware y tengas toda la base de equipos cifrados; por lo menos reduce todo el tiempo que tienes que ocupar para los temas normativos, para el compliance, al máximo, y apóyate en herramientas que te ayuden en esa línea.

QUALYS



“La tendencia es tener más dispersión y variedad de activos”

SERGIO FERNÁNDEZ, TECHNICAL ACCOUNT MANAGER DE QUALYS

“Nuestra propuesta tecnológica es única y basada en la nube”

“Mucho se ha comentado sobre el teletrabajo, que ha venido para quedarse”, señala Sergio Fernández, Technical Account Manager de Qualys, “pero yo diría que son los entornos híbridos los que van a quedarse”.

Vamos a ver más plataformas, más aplicaciones, toda la gestión de OT va a seguir al alza, y eso va a requerir de las organizaciones una postura de ciberseguridad innovadora y de mejora continua, ya que en esos entornos híbridos lo que también van a ayudar es toda la cuestión de la resiliencia. “Uno de los desafíos para el año que viene es tener esa visibilidad holística de todos los activos, no solo los más tradicionales, sino también de esos nuevos activos, como contenedores, o los que estén en nubes públicas”.

“La tendencia es tener más dispersión y variedad de activos, entornos más complejos también, híbridos. Los equipos de ciberseguridad y de gestión de TI necesitan la información que proporciona la inteligencia para tomar mejores decisiones de una forma más rápida”.

Para Sergio Fernández lo importante es que esa información sea lo más precisa posible, hay que evitar que tenga muchos falsos positivos, ya que esos equipos de ciberseguridad y de gestión de TI están desbordados con tanta información que llega desde distintas fuentes. Tiene que ser una información que llegue muy rápida y de forma fluida.

Este responsable cree que la ciberinteligencia es necesaria para abordar la vulnerabilidad de los sistemas. “Para ello ya hay tecnología que permite el uso de la ciberinteligencia aplicada a la vulnerabilidad. Por ejemplo, los RTI son indicadores de amenazas en tiempo real, pero relacionados con vulnerabilidades. Es una información muy detallada, que se recopila de distintas fuentes”. Esta información tiene que estar contextualizada y ser accionable, para que las empresas puedan, de una forma muy fácil, priorizar y reducir esas alertas de seguridad.

SECURE&IT

“Estamos en una situación en la que necesitamos al usuario final”

FRANCISCO VALENCIA, DIRECTOR GENERAL DE SECURE&IT

“Nuestro trabajo consiste en que las compañías no estén en una falsa sensación de seguridad”

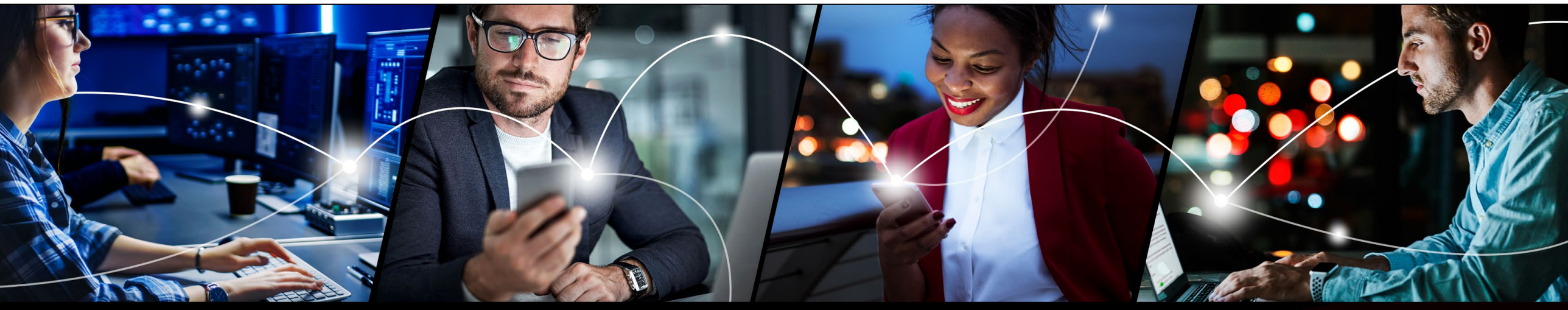
Francisco Valencia, Director General de Secure&IT, cree que el principal reto de cara a 2022 es la protección ante ataques que no solamente están afectando a la operativa de las compañías, sino que además están robando información. “Garantizar que los ataques de nueva generación, que lo que están haciendo es filtración de datos además del cifrado, y, por lo tanto, están exigiendo rescates y chantajes cada vez más duros, de forma más rentable para los ciberdelincuentes, puedan tener un freno”. Francisco Valencia cree que la formación será más importante que nunca. “El aislamiento que provoca el hecho de estar trabajando en casa hace que sea mucho más necesaria la formación y la concienciación en materia de ciberseguridad y protección de datos”.

Este portavoz señala que es bastante injusto echar la culpa al usuario final de la incompetencia del sector. “Estamos en una situación en la que necesitamos al usuario final y, por lo tanto, tenemos que ampliar la formación, no solamente a estos usuarios, sino también a las áreas de TI, a los expertos en tecnologías de la información, y, en general, a los que van a implantar procesos corporativos dentro de las organizaciones”.

La seguridad gestionada se ha convertido en un punto fundamental dentro de las organizaciones. “Realmente ya es algo que se ha hecho tremendamente amplio. La Administración Pública también lo está viendo así, se está creando la Red Nacional de Centros de Operaciones de Seguridad, con el objetivo de que la Administración pueda disponer de centros propios, públicos o privados, pero que les den ciberseguridad gestionada”. Para Francisco Valencia, casi es una necesidad más que un servicio. El problema es que no hay profesionales suficientes para poder realizar la labor de la gestión y la vigilancia de la seguridad. “2021 y 2022 van a ser puntos de inflexión en esta línea donde cada vez un porcentaje mayor de compañías van a reconocer la necesidad de tener un centro de seguridad que proteja su infraestructura e información”. ■

Si te ha gustado este artículo, compártelo

Seguridad unificada para un mundo RECONECTADO



SEGURIDAD DE RED

AUTENTICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD ENDPOINT

Unified Security Platform™

CLARIDAD Y CONTROL — **SEGURIDAD INTEGRAL** — **CONOCIMIENTO COMPARTIDO** — **ALINEACIÓN OPERATIVA** — **AUTOMATIZACIÓN**

Contacto: +34 917 932 531 Email: spain@watchguard.com www.watchguard.com

Tendencias de ciberseguridad para 2022:

hablemos de SASE

Llevamos tiempo hablando de SASE (Secure Access Service Edge)
¿Será 2022 el año de despegue de esta propuesta?

LUIGI SEMENTE, SALES SPECIALIST DE CITRIX

"En muchos casos SASE es ya una realidad. Hablamos de aquellas organizaciones con uso importante de servicios en la nube (SaaS) y con workforce distribuida. Con la llegada del trabajo híbrido, cualquier organización va a tener un perímetro de seguridad extendido, que sale del CPD y de las oficinas corporativas. Todo eso dará un empujón importante en la adopción del framework SASE, también en aquellas organizaciones que hasta ahora han decidido a apostar por una ciberseguridad más tradicional. El modelo SASE garantiza una seguridad coherente y consistente en cualquier ámbito".

JESÚS SÁEZ, COUNTRY MANAGER SPAIN & PORTUGAL DE NETWRIX

"SASE seguirá siendo una propuesta a considerar por muchas corporaciones tanto en 2022, como en los próximos años. La movilidad y el trabajo desde casa se ha convertido en la nueva norma y seguirá siéndolo en el futuro, por lo que el perímetro ha pasado a ser el usuario y no solo hay que protegerlo, sino monitorizar y auditar, ya que su actividad es clave para poder detectar y responder rápidamente ante posibles amenazas, con el fin de mantener a salvo los datos confidenciales y cumplir con las normativas existentes".

FRANCISCO VALENCIA, DIRECTOR GENERAL DE SECURE&IT

“Se han hecho patentes dos realidades paralelas. Por un lado, la adopción de tecnologías y servicios en nubes públicas y privadas, y, por otro, la necesidad de teletrabajo, movilidad y flexibilidad. Ambas realidades necesitan soluciones de ciberseguridad que cubran lo que ya veníamos haciendo con la tecnología tradicional (firewalls, IPS…). SASE viene a dar respuesta a la nueva situación en la que el perímetro deja de estar definido, los conceptos “oficina” o “Centro de Datos” están desvirtuados y ya casi nada está conectado a un cable. Las empresas que aún no han ido a un modelo SASE, es porque no han comprendido aún las ventajas que aporta”.

JAVIER DONOSO, SALES ENGINEER DE SOPHOS

“El “nuevo” perímetro de la red existe dondequiera que se encuentren los empleados cuando se conectan a la red corporativa, ya sea en casa, en una cafetería o donde sea, y SASE provee los mecanismos necesarios para proporcionar seguridad sea cual sea el punto de acceso a la red. Además, podemos decir que siguiendo la metodología o la arquitectura SASE, no importa dónde residen las aplicaciones, y esto encaja perfectamente con el cambio que se ha producido en los últimos tiempos en el que todas nuestras aplicaciones han pasado del centro de datos corporativo a los proveedores de nube en formato SaaS (Software como Servicio)”.

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL

“El acceso remoto seguro Zero-Trust es ya una necesidad imperiosa: la dilución del perímetro hacia un entorno multiperimetral, la hiperexposición a la que estamos expuestos, el entorno hostil en el que trabajan nuestros endpoints, la virulencia y directividad de los ataques, la hiperconectividad (2022 será el año de 5G), el malware inteligente, el cibercrimen real que busca cómo lucrarse de nuestros fallos... En este entorno, se necesita SASE para dar sentido otra vez al perímetro, securizar el acceso a las aplicaciones corporativas, independientemente de dónde estén, establecer roles y microsegmentar el acceso, gestionar los accesos de todo tipo, incluidos los privilegiados...”.

GUILLERMO FERNÁNDEZ, MANAGER SALES ENGINEERING IBERIA DE WATCHGUARD

“Desde WatchGuard vemos que 2022 será importante pero no definitivo. Es cierto que la pandemia ha ejercido como acelerante, llevando a todos en esa dirección, pero cada empresa, en función de sus presupuestos y prioridades, van dando los pasos en diferentes momentos. Al igual que ha ocurrido con otras tecnologías como Cloud, Virtualización, Zero-Trust… la adopción tiende a ser relativamente lenta, siendo necesarios varios años”.

Tendencias IT 2022:
¿qué impactará en la TI corporativa?

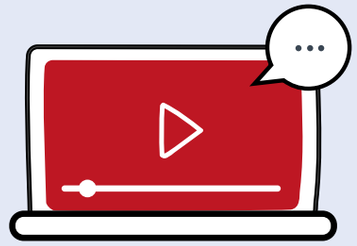
¿Cómo se ha comportado la TI corporativa en 2021? ¿Qué tecnologías han asumido el papel de transformadoras? ¿Cuál es el estado de la transformación digital de las empresas? ¿Cómo continuarán evolucionando en 2022? Todas estas serán cuestiones a abordar en esta sesión online junto a expertos del mercado y la empresa.

REGISTRO

REGISTRO

La transformación del trabajo:
el empleado conectado

La naturaleza del trabajo ha cambiado rápidamente. Hoy, la mayor parte de las compañías está adoptando un modelo híbrido o remoto, de manera definitiva. Esto requiere crear la mejor experiencia del empleado e invertir en plataformas e infraestructuras digitales que lo hagan posible. Además, la propia transformación digital busca una mejora de los proceso apoyándose en soluciones que aporten productividad y agilidad. El empleado conectado y productivo requiere de un nuevo entorno de trabajo.



#ITWEBINARS

Tecnologías de ciberseguridad que no debes perder de vista en 2022

Este año veremos más ataques. El ransomware se volverá más osado; el phishing más perfeccionado; el modo de trabajo será híbrido; los datos, el activos más buscado por los ciberdelincuentes; la gestión de vulnerabilidades, inabordable; seguiremos preocupados por el IoT, y por la movilidad, y por todo lo que se marcha a la nube sin que podamos evitarlo; seguiremos añadiendo IA a todo lo que podamos, sin saber en realidad si hacemos sistemas más inteligentes o solo más espabilados. Y seguirá habiendo escasez de profesionales, demasiadas herramientas que gestionar y una consolidación que va a un ritmo más lento del esperado. En cuanto a tecnologías, ¿cuáles habremos de tener en cuenta?

Se ha dicho en multitud de ocasiones: el de la ciberseguridad es un sector tremendamente fragmentado y tremendamente dinámico. No dejan de aparecer nuevas tendencias, tecnologías y jugadores, lo que complica tremendamente una consolidación que se hace cada vez más necesaria. El modelo 'best of breed', que invitaba a escoger lo mejor de cada fabricante, añadiendo una capa de gestión y orquestación se vuelve ingobernable ante una realidad: la complejidad es un riesgo de seguridad.

Los últimos estudios indican que una empresa pequeña gestiona entre 15 y 20 herramientas de seguridad; una medias puede llegar a 60 y una gran compañía superar el centenar, y no por ello los responsables de seguridad se sienten tranquilos. Más del 50% de los expertos en IT no tienen confianza en la capacidad de sus organizaciones para detener una brecha de seguridad y un 75% no cree que el equipo de seguridad de su empresa sea capaz

El principio básico de la Blockchain Security es que todas las partes de una transacción deben autenticarse

LAS PRINCIPALES TECNOLOGÍAS DE SEGURIDAD DE APLICACIONES QUE SE ADOPTARÁN EN 2021

Las aplicaciones constituyen la mayor superficie de ataque de todas las capas de la pila empresarial. Además, son los más difíciles de defender porque son los más accesibles y los más expuestos al mundo exterior. Este documento técnico presenta tres tecnologías de seguridad de aplicaciones que es importante implementar para mantener la postura de seguridad de las aplicaciones.

de responder a un incidente de ciberseguridad en un día.

Más herramientas significan más errores de configuración, más parches que gestionar y más contraseñas y privilegios que controlar. Pero los ciberdelincuentes no cesan en su empeño por atacar todo tipo de empresas y el juego sigue adelante. Sumémonos a él e identifiquemos algunas de las tendencias tecnológicas que se habrán de tener en cuenta este 2022 y que se sumarán a todas las existentes.

Cybersecurity Mesh

Como Zero trust y SASE, Cybersecurity Mesh no es una tecnología en sí misma, sino un concepto, una estrategia de ciberdefensa que busca proteger de forma independiente cada dispositivo con su propio perímetro, lo que permite extender la seguridad allá donde se necesite.

De manera más específica, Cybersecurity Mesh consiste en diseñar e implementar una infraestructura de seguridad de TI que no se centra en construir un único “perímetro” alrededor de todos los dispositivos o nodos de una red de TI, sino que establece perímetros individuales más pequeños alrededor de cada dispositivo o punto de acceso. Esto crea una arquitectura de seguridad modular y más receptiva que cubre puntos de acceso físicamente dispares de la red.

Cybersecurity Mesh es, en realidad, uno de los baluartes de Zero Trust al cambiar el enfoque de proteger un perímetro de TI tradicional a un enfoque más modular que centraliza la orquestación de políticas. En este escenario los departamentos de TI pueden crear perímetros individuales más pequeños que protegen los puntos de acceso distribuidos, lo que permite a los administradores de red ofrecer

En general, las organizaciones planean aumentar su adopción de tecnologías de seguridad en 2022

diferentes niveles de acceso a diferentes componentes y activos, y dificulta que los ciberdelincuentes exploten una red completa.

¿Quién necesitaría adoptar una estrategia de Cybersecurity Mesh? Todas, desde que el remoto es el nuevo modelo de teletrabajo y desplazamos datos fuera del perímetro tradicional. La infraestructura de seguridad empresarial ahora debe ser lo suficientemente ágil para cubrir los a los empleados remotos, que acceden a los recursos y propiedad intelectual de las empresas desde su hogar.

Identity-first security

La identidad se ha convertido en uno de los elementos más importantes a proteger. El teletrabajo y la migración a aplicaciones en la nube han solidificado la tendencia de la identidad como perímetro. La seguridad que prioriza la identidad no es nueva, pero adquiere una nueva urgencia a medida que los atacantes comienzan a apuntar a las capacidades de administración de identidades y accesos para lograr una persistencia silenciosa.

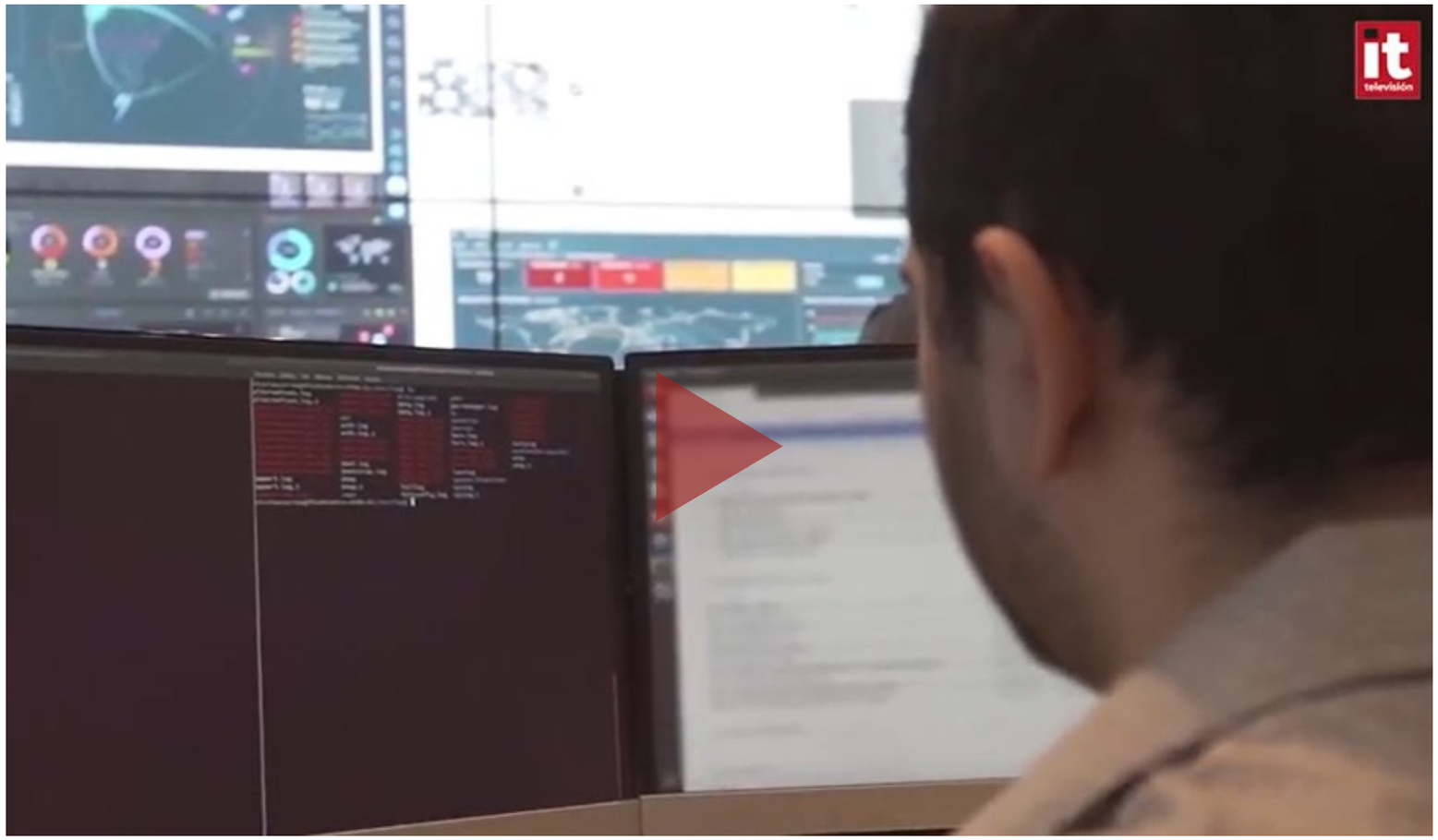
El robo de credenciales es una de las acciones más perseguidas por los ciberdelincuentes porque con ellas pueden ganar acceso a los sistemas y robar datos. Las credenciales mal utilizadas son ahora la técnica más utilizada en las infracciones.

Los atacantes a nivel de estado nación están apuntando al directorio activo y la infraestructura de identidad con gran éxito. La mayor preocupación por la protección de la identidad está impulsando el mercado de autenticación multifactor.

El mayor reto al que se enfrenta la gestión de identidades es su configuración, mantenimiento y monitorización para que el usuario siempre tenga los permisos correctos.

Algunos de los principales proveedores de soluciones de gestión de identidades, incluyendo

Las Privacy-Enhancing Technologies, o PET, son las que permiten que los datos puedan ser analizados y compartidos sin exponer su contenido a terceros



EL RANSOMWARE IMPULSA EL MERCADO DE LOS CIBERSEGUROS

CLICAR PARA VER EL VÍDEO

identidades privilegiadas son: Beyond Trust, CyberArk, Entrust, Okta, OneIdentity, OneLogin, Ping Identity, SailPoint, Thales o ThycoticCentrify.

Controlando las máquinas

Cuando en el apartado anterior mencionábamos la importancia de gestionar las identidades adecuadamente, no sólo nos referíamos a las identidades humanas, sino de las máquinas. A medida que avanza la transformación digital, ha habido un crecimiento explosivo en la cantidad de entidades no humanas que componen las aplicaciones modernas. Por lo tanto, administrar las identidades de las máquinas se ha convertido en una parte vital de las operaciones de seguridad.

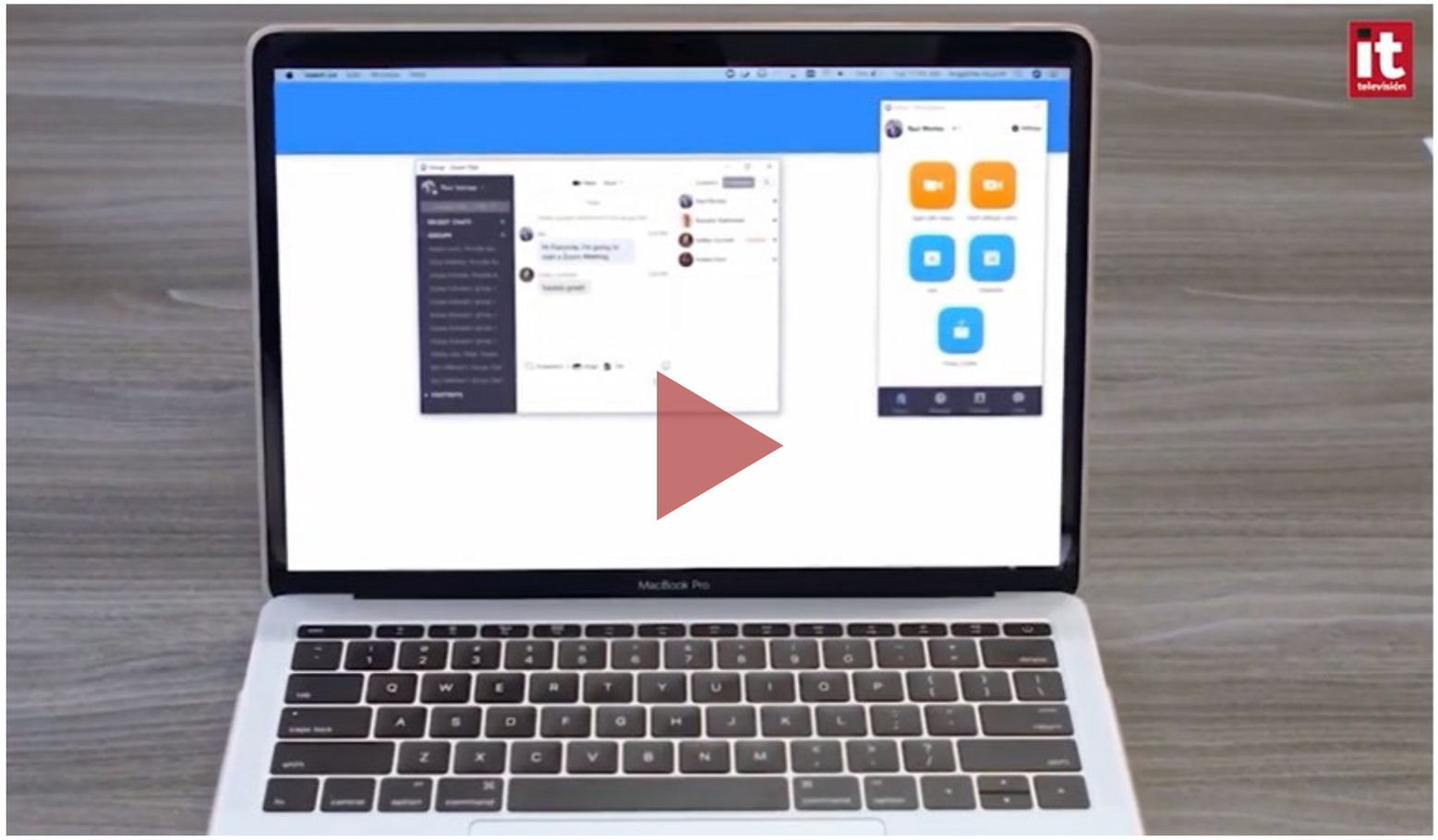
Todas las aplicaciones modernas se componen de servicios que están conectados por una API, o interfaz de programación de aplicaciones. Cada

uno de estos servicios debe ser autenticado y monitorizado, ya que los atacantes pueden usar el acceso API de sus proveedores a datos críticos para su beneficio. Las herramientas y técnicas para la gestión de identidades de máquinas en toda la empresa aún están surgiendo. Sin embargo, una estrategia empresarial para administrar identidades, certificados y secretos de máquinas permitirá a su organización asegurar mejor su transformación digital.

BAS – Breach and Attack Simulation

Las tecnologías de simulación de brechas y ataques de seguridad, que ayudan a las empresas

Las herramientas BAS ofrece pruebas y validaciones continuas de los controles de seguridad



ASÍ SE TRANSFORMARÁ LA OFICINA EN EL 2022

CLICAR PARA VER EL VÍDEO

El robo de credenciales es una de las acciones más perseguidas por los ciberdelincuentes

a validar su postura de seguridad no son nuevas, pero su uso está creciendo.

Las herramientas BAS ofrece pruebas y validaciones continuas de los controles de seguridad, y ofrecen evaluaciones especializadas. Por eso hay que se refiere a ellas como la próxima generación de las herramientas de gestión de vulnerabilidades, y por eso en algunas listas de proveedores de BAS aparecen nombres como Qualys y Rapid7.

Es un mercado que ha crecido mucho y muy rápido. A medida que la industria se desarrolla, es cada vez más común referirse a estas soluciones como de 'validación de seguridad'. La inteligencia artificial y el aprendizaje automático son una parte cada vez más importante de este mercado, ya que las herramientas de ciberseguridad automatizadas deben poder adaptarse a medida que surgen nuevas amenazas.

Algunos de los principales proveedores de soluciones BAS son: AttackIQ, CyCognito, Cymulate, DXC Technology, FireEye's Mandiant, FireMon, Qualys o Rapid7.

Autenticación, integrada en hardware y multifactor

El uso de pines y contraseñas para mantener nuestros datos a salvo ya no es suficiente. Son muchas, cada vez más, las brechas de seguridad que implican el uso de credenciales robadas. Incluso con una política de contraseñas fuerte, la combinación tradicional de nombre de usuario y contraseña por sí sola no es suficiente para proteger las cuentas. La autenticación multifactor agrega una capa adicional de protección al requerir que los usuarios confirmen sus identidades utilizando varios medios. Un sistema de inicio de sesión de MFA busca algo que el usuario tenga, sea o sepa, y verifica las credenciales correctas.

Además, el uso de tokens de hardware para autenticar a los usuarios no es una nueva tecnología de seguridad, pero los ciberataques están haciendo que su uso se esté ampliando.

Cuando hablamos de autenticación integrada por hardware también hay que hacer referencia a la apuesta de Intel con su solución Authenticate, incluida en su nuevo procesador Core vPro de sexta generación. Puede combinar una variedad de factores mejorados por hardware al mismo tiempo para validar la identidad de un usuario.

PET – Privacy-Enhancing Technologies

Las Privacy-Enhancing Technologies, o técnicas de mejora de la privacidad son las que permiten que los datos puedan ser analizados y compartidos sin exponer su contenido a terceros. Según Gartner, para 2025, el 50% de las grandes organizaciones

it whitepapers

14 PREDICCIONES DE CIBERSEGURIDAD PARA 2022

Cuando hablamos de ciberseguridad, las expectativas son críticas. Una cosa con la que siempre podemos contar es el nivel de incertidumbre en el ámbito cibernético. Los atacantes cambian regularmente sus tácticas, técnicas y procedimientos (TTP) para evadir la detección, lo que deja a los defensores luchando por mantenerse al día. Este informe, elaborado por Mandiant, enumera 14 predicciones de ciberseguridad para 2022 y más allá.

implementarán tecnologías de este tipo que mejoren la privacidad para procesar datos en entornos no confiables y casos de uso de análisis de datos de múltiples partes.

Con la maduración del cumplimiento de la privacidad y las regulaciones más generalizadas, tanto las pequeñas como las grandes empresas tendrán que proteger los datos en uso. Según Gartner, este tipo de seguridad se presenta en tres formas; el primero, que podría implicar proporcionar un entorno confiable en el que los datos se puedan procesar o analizar a través de entornos de ejecución de terceros y confiables en el hardware.

El segundo tipo de PET se refiere al procesamiento y análisis descentralizados a través del aprendizaje automático federado o consciente de la privacidad. Por último, se plantea también un computación que transforme los datos y los algoritmos antes del procesamiento o el análisis, incluida la prueba de conocimiento cero, la computación segura de varias partes y el cifrado homomórfico.

El cifrado homomórfico (HE) utiliza técnicas de cifrado para permitir que terceros procesen datos cifrados y devuelvan un resultado cifrado al propietario de los datos sin proporcionar ningún conocimiento sobre los datos o el resultado. En la práctica, este tipo de cifrado no es lo suficientemente rápido para las implementaciones comerciales.

Seguridad Blockchain

Esta tecnología de ciberseguridad relativamente nueva está ganando terreno a un ritmo acelerado. El principio básico de la Blockchain Security es que todas las partes de una transacción deben autenticarse. Cada bloque agregado a la cadena tendría un código de identificación único, y todos en la cadena pueden ver la información que se agrega a su libro mayor. Si se edita la cadena, se hace evidente en todos los dispositivos de la cadena. Por lo tanto, si un ciberdelincuente intentara violar un bloque de la cadena, el sistema reconocería la violación y la cerraría. Los ciberdelincuentes tendrían que modificar todos los bloques de la cadena en todas las versiones distribuidas.

Servicios gestionads

En realidad, los proveedores de servicios gestionados de seguridad no son una tendencia tecnológica

Más herramientas significan más errores de configuración, más parches que gestionar y más contraseñas y privilegios que controlar

propiamente dicha, pero ayudarán en la adopción de todas las que hemos hablado. Están, han estado y estarán presentes el próximo año. Según un estudio realidado por Spyceworks en Norteamérica y Europa, la mitad de los responsables de los decisores de compra en las empresas ampliarán su presupuesto TI un 26% respecto a 2021.

Se espera que la mayor parte de los presupuestos del próximo año se destinen al hardware (alrededor del 30% del gasto total en TI), seguido del software (28%) y los servicios en la nube (26%). Comparativamente, el gasto en servicios gestionados representará solo una pequeña parte del total: solo el 17% del presupuesto total. Sin embargo, esa proyección para 2022 es un aumento con respecto a este año y a 2020. Y dentro de la categoría más amplia de “servicios gestionados” hay algunas tendencias interesantes.

Según el autor del informe, se espera que la seguridad, alojamiento administrado, almacenamiento/ respaldo administrado, soporte de hardware, infraestructura en la nube y aplicaciones comerciales gestionadas representen la mayor parte de los presupuestos de servicios gestionados en 2022. “Impulsadas por la necesidad de proteger a los trabajadores remotos y la continua amenaza del ransomware, las empresas seguirán adelante con la inversión en soluciones de seguridad emergentes”, puede leerse en el informe.

En general, las organizaciones planean aumentar su adopción de tecnologías de seguridad, pero las cinco categorías principales son: Herramientas de formación y concienciación para los empleados (76% de las empresas); Soluciones anti-ransomware (76%); Autenticación basada en hardware (68%); Detección y respuesta de infracciones (59%) y Soluciones de seguridad Zero Trust (57%).

Destacar también que la seguridad en la nube representó el 5% de los presupuestos de la nube en 2020, un porcentaje que se espera que crezca hasta el 7% en 2022.

Enlaces de interés...

- La ciberseguridad será un área de oportunidad para los emprendedores en 2022
- Las empresas priorizarán la automatización de la ciberseguridad en 2022
- Zero Trust se impondrá en las estrategias de seguridad en 2022
- ¿A que nos podríamos enfrentar en 2022? Cuando la sombra de los ciberataques planea en nuestro día a día - 20 DIC 2021
- ¿Se verán en 2022 los resultados de establecer estrategias Zero Trust?

Compartir en RRSS

it User
TECH & BUSINESS

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

MÀRIUS ALBERT GÓMEZ

Marius Gómez en su columna éTICa, sintetiza la voluntad de compartir unas reflexiones que nos ayuden a entender un mundo digital caracterizado con esos grandes “trending topics” actuales como son el Big Data, la Inteligencia Artificial, la IOT o la computación en general, y que son vistos desde un marco de consideraciones éticas, humanistas y sociales. Dichas reflexiones se realizan desde la actitud y el desempeño multidisciplinar, tanto individual como empresarial, y tienen el objeto de contribuir a “aportar un pequeño granito de arena en el proceso de repensar el papel que las TIC deben jugar en la vida de nuestros hijos, en su formación, en su trabajo, en su día a día... con un punto de vista que supere el meramente tecnológico”.

Compartir en RRSS

Qué es la filosofía sino quizá ese anhelo de entendimiento y de conocimiento de la realidad que nos rodea. Una realidad donde las TIC representan hoy en día no tan sólo ya únicamente una herramienta, sino que conforman un entorno ineludible e inevitable de la misma. Unas TIC con las que cada vez más hiperconectamos, hipercomunicamos, hipervirtualizamos, hipermovilizamos, e hiperaceleramos cada interacción social, laboral y personal. Con las que desdibujamos cada día más las diferencias entre lo físico y lo virtual. Hemos evolucionado de agentes de consumo básico de información social y corporativa, telenoticias, periódicos... a agentes activos de su producción en los distintos medios de internet, en las grandes plataformas sociales. Compartimos historias y vivencias, interpretamos las mismas y opinamos, calificamos lo que nos gusta y aspiramos a ello, interactuamos e intercambiamos, atendemos noticias push, nos publicitamos y piolamos. Dependemos de la información en todo ello, y seguramente en este sentido, podemos entender una información, eminentemente digital ya, como una de las bases de la filosofía de nuestro tiempo.

Resulta evidente pues lo significante de los beneficios de las TIC en la ya llamada cuarta revolución, lo que representan hoy en día, y lo que pueden representar para las generaciones futuras. Del enorme beneficio del componente de superación de barreas de acceso a la información, de su carácter integrador social, del ejercicio de transparencia

La comunicación ha sido siempre un componente inherente de comprensión de nuestra realidad y nuestra historia, pero para que lo pueda seguir siendo en este contexto actual de la hiperhistoria, vamos a tener que ser capaces de hiperhumanizarnos

Podemos entender una información, eminentemente digital ya, como una de las bases de la filosofía de nuestro tiempo

también unas dinámicas hiperaceleradas de consumo informativo social, cada día más rápido, más instantáneo, más fugaz y efímero. Un consumo a menudo sin un valor trascendental significativo y que conforma visiones muchas veces superficiales e interesadas de nuestra realidad física que son vertidas rápidamente sobre la "caverna platónica" virtual. La imagen sólo por la imagen. El acto sólo por la imagen. Y corremos el riesgo de que eventualmente dichas prácticas sean hiperadoptadas y se conviertan en sistémicas. Y si se convierten en sistémicas, ya no será sólo un tema relacional o comunicativo, lo habremos institucionalizado socialmente como individuos, física y virtualmente.

Escribir mensualmente una tribuna en un medio digital, puede entenderse en ese contexto, como un acto comunicativo más. Pero periodísticamente y desde la humildad, cada tribuna es un ejercicio de reflexión y pretendido entendimiento intelectual de nuestra realidad, de su análisis argumentativo, de preparación y esfuerzo, de visión crítica a veces, aunque siempre constructiva, del que cuestiona y también responde, del que anhela una reacción en su consumo sin esperar absolutamente nada más. Un ejercicio siempre pretendido desde esa visión más trascendental de interpretación de lo social, lo democrático, lo humanista y lo ético.

La comunicación ha sido siempre un componente inherente de comprensión de nuestra realidad y nuestra historia, pero para que lo pueda seguir siendo en este contexto actual de la hiperhistoria, informacional y TIC, digital y virtual, vamos a tener que ser capaces de hiperhumanizarnos. Tengo un amigo que entrañablemente me llama "el filósofo TIC", (algo a lo que probablemente puedan contribuir estas columnas), y a lo que siempre respondo que no me asocie con torres de marfil, pues simplemente somos muchos los que aspiramos a este otro tipo de comunicación no tan fugaz o efímera. Los que intentamos buscar un sentido más ético y trascendental, que no nos sea ajeno y pueda formar parte del día a día de nuestro ejercicio como profesionales TIC, compatible en un mercado competitivo, en la gestión de los proyectos, en la dirección de ventas, en la programación de sistemas, en su operación. Por convicción, humanista.

Les deseo junto con ese pensamiento final, unas felices fiestas y un mejor y próspero 2022.

Enlaces de interés...

- Las dudas que despierta el Metaverso