it TRENDS

ENERO 2021

2021, retomando el futuro interrumpido

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

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

2021,
a por la aceleración digital y la continuidad del negocio

El año que acabamos de terminar tiene múltiples lecturas. Independientemente de la situación vivida, la tecnología se ha revelado como uno de los puntales sobre los que se ha asentado la continuidad de la vida de las personas (la conectividad y los dispositivos móviles han permitido mantener el contacto con el entorno en periodos de aislamiento) y de las empresas (el teletrabajo, la disponibilidad de las aplicaciones, el desarrollo de nuevos negocios digitales...). Ha sido un año difícil, pero de grandes lecciones aprendidas.

En términos generales, la transformación digital de las organizaciones se ha visto acelerada "en 6 o 7 años", tal y cómo nos han dicho algunos portavoces con los que hemos compartido impresiones en estos últimos meses. Aunque el gasto en tecnología se ha visto reducido con respecto a las previsiones, la aplicación de ese presupuesto en proyectos inmediatos que significaban la única vía para seguir desarrollando la actividad empresarial servirá como base para los que se adopten en este 2021, un año en el que las organizaciones deberán seguir la senda de su digitalización con paso firme y ante los nuevos escenarios que se le plantean: asentamiento del teletrabajo y acceso remoto, usuarios y clientes más digitales y exigentes, mayor necesidad de proteger la información almacenada ante el aumento de los ciberataques...

En los Encuentros IT Trends que celebramos en diciembre del pasado año para evaluar los planes adoptados y los futuros, expertos de Veeam Software, f5 Networks, Micro Focus, VMware, One Identity, ESET, Check Point, y Entrust, nos dejaron las pistas para construir unas estrategias de TI fuertes, consolidadas, en línea con las demandas de los usuarios de negocio y clientes externos. Puedes ver estas sesiones en "IT Trends 2021. La TI salva el negocio" y "2021, ¿el año de la ciberdefensa?".

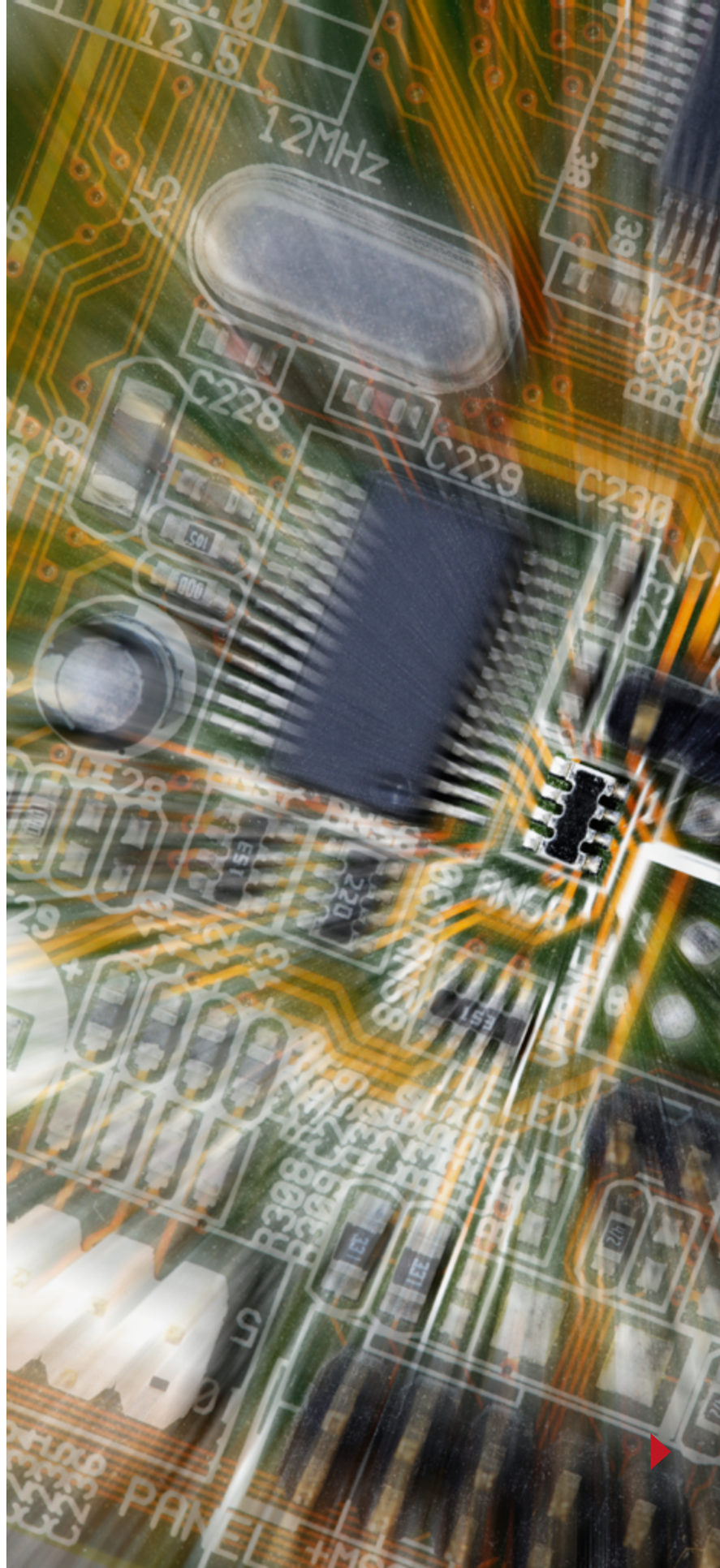
También en estos últimos meses ha aumentado el consumo de contenidos digitales y las compras vía ecommerce, dos áreas en las que la entrega y disponibilidad de contenido y aplicaciones se han revelado como fundamentales para hacer disfrutar a los clientes de una experiencia que les convierta en fieles a la marca. En la sección de Customer Experience, patrocinada por Fastly, puedes leer diversas formas de proporcionar a tu negocio online esa continuidad que los usuarios están demandado.

Gracias a todos los que colaboran y apoyan la elaboración de nuestros contenidos -patrocinadores y lectores-, porque nos permiten tomar el pulso a la evolución tecnológica desde todas las vertientes. Que 2021 sea un año en el que podamos seguir desarrollando, con salud, nuestras estrategias. ■

Arancha Asenjo
Directora de IT Televisión y Lead Gen Programs

www.ittrends.es

10 tendencias tech que transformarán el mercado en 2021



2020 se caracterizó por la incertidumbre que causó la pandemia, provocando una contención del gasto por parte de empresas y gobiernos para superar la crisis. Pero al mismo tiempo se produjo un avance significativo de algunas aplicaciones y escenarios digitales que permitieron a las empresas seguir funcionando, lo que ha influido en el progreso de las tecnologías subyacentes. Esto ha introducido cambios en las tendencias previstas para la industria tecnológica antes de la crisis.

Los ecosistemas digitales están en constante evolución: en 2020 la tecnología cobró una especial relevancia a raíz de la grave crisis sanitaria y se produjeron grandes cambios en el sector tecnológico. Los investigadores de la firma de análisis de mercado TrendForce destacan las diez que más progresarán en este año 2021.

1 EVOLUCIÓN DE LAS TECNOLOGÍAS DE FABRICACIÓN DE MEMORIA. Los proveedores de chips de memoria están introduciendo nuevas tecnologías de fabricación que les están permitiendo diseñar productos más evolucionados, tanto en el campo de la memoria DRAM como en el almacenamiento NAND Flash. En cuanto a la memoria de trabajo, los princi-

pales fabricantes (Samsung, SK Hynix y Micron) avanzan a buen ritmo en la transición hacia las tecnologías de proceso 1Znm y 1alpha nm, pero quizá el cambio más importante vendrá de la tecnología EUV, un avance en el que Samsung se encuentra a la cabeza. Este tipo de tecnología de litografía permite una mayor eficiencia en la fabricación y una mejor optimización de los costes, lo que tendrá un impacto muy positivo en los mercados de memoria. Se espera que esto permita a los proveedores de DRAM fabricar más barato y resistir mejor las fluctuaciones que puedan surgir en el mercado de memoria, que tiene una gran influencia en el devenir del mercado general de semiconductores.

Por su parte, la memoria NAND Flash está evolucionando mucho, y los expertos de TrendForce destacan que, tras superar este año las 100 capas de celdas de memoria en sus chips, en 2021 rebasarán la barrera de las 150 capas.

SIETE TENDENCIAS TECNOLÓGICAS QUE MOLDEARÁN 2021

Esto permitirá fabricar productos de mucha más capacidad en el mismo formato, generando una competencia más fuerte en ciertos segmentos de almacenamiento dominados hasta ahora por los discos HDD tradicionales, tanto en el ámbito del gran consumo como muy especialmente en los centros de datos e infraestructuras TI empresariales. Además, se espera un progreso rápido en la implementación de compatibilidad con el nuevo estándar PCI Express 4, que ya se encuentra presente en todo tipo de computadores e, incluso, en las videoconsolas de nueva generación que llegarán al mercado este invierno.

2 ASENTAMIENTO DE LAS REDES MÓVILES 5G. En 2020 comenzó el despliegue masivo de tecnologías 5G, aunque la pandemia causó un ligero retraso en los planes anteriores a la crisis. Pero para este 2021, en TrendForce están convencidos de que los operadores móviles darán un gran paso adelante en la implementación de estaciones base 5G SA, dejando atrás las tecnologías basadas en 4G, que todavía dominan los mercados más evolucionados. El progreso de las nuevas arquitecturas verdaderamente 5G les permitirá ofrecer soluciones de conectividad de gran ancho de banda y muy baja latencia que no solo beneficiarán a los consumidores, sino que tienen como principal target los nuevos usos empresariales.

Mientras tanto, se espera que los grandes pioneros en las redes, que actualmente son Corea del Sur y Japón, comiencen el despliegue de los primeros pilotos de lo que en el futuro serán las redes 6G. Esto tendrá como objetivo principal explorar las posibilidades que ofrecerán las redes móviles en los campos que ahora son más exigentes para las comunicaciones, como son la realidad virtual, aumentada y mixta (con resoluciones 8K y superiores), las comunicaciones holográficas realistas, la telemedicina, la educación a distancia, el trabajo remoto y otras tendencias que están ganando fuerza y que podrían rebasar los límites de lo que puede ofrecer 5G.

TAMBIÉN NOS CUENTAN...

TECNOLOGÍAS ESTRATÉGICAS PARA 2021, SEGÚN GARTNER

La complicada situación que vive el mundo empresarial está llevando a las organizaciones a replantearse sus estrategias operativas para reforzar su resiliencia y poder afrontar mejor cualquier crisis. Esto ha modificado muchas de las perspectivas y tendencias tecnológicas anteriores; los expertos de Gartner han elaborado una lista con las tendencias tecnológicas estratégicas que tendrán una mayor influencia en este 2021.

Leer

IDC: TENDENCIAS DE INVERSIÓN TECNOLÓGICA PARA LA NUEVA NORMALIDAD

La pandemia ha generado importantes cambios en las empresas a nivel operativo, y muchas han acelerado ciertos aspectos de su transformación digital para hacer frente a la crisis y preparase para la nueva normalidad que comenzará este año. Las organizaciones están cambiando sus prioridades y sus estrategias de inversión en tecnología, algo que en un futuro se verá influenciado por una serie de tendencias, especialmente en los sectores más afectados por la crisis. A continuación, puedes leer las recomendaciones de IDC.

Ir al artículo

TENDENCIAS TECNOLÓGICAS QUE NO VERÁN LA LUZ EN 2021 (ABI RESEARCH)

A pesar del avance que se está produciendo en el desarrollo de ciertas tecnologías emergentes, como la IA explicable, en realidad todavía falta mucho para que se puedan considerar tendencias establecidas. Los investigadores de ABI Research han elaborado una lista con las principales tendencias tecnológicas que finalmente no se harán realidad en 2021.

Sigue leyendo

3 EL CONCEPTO DE IOT EVOLUCIONA HACIA LA "INTELIGENCIA DE LAS COSAS".

Internet of Things ya forma parte de la vida de las personas a través de los, cada vez más, numerosos dispositivos conectados que se están expendiendo en el hogar, los vehículos y otros entornos. Pero en las organizaciones también, ya que este concepto se aplica a muchos niveles, tanto en oficinas como en fábricas y en toda clase de instalaciones e infraestructuras. Esto ha ido evolucionando y el siguiente paso, que según los expertos se expandirá considerablemente este año 2021, es la integración de inteligencia en los dispositivos conectados, lo que dará lugar al nuevo paradigma de “Inteligencia de las cosas”.

Esto permitirá crear redes de inteligencia artificial en el que los aparatos generarán información, la contextualizarán y procesarán mediante IA y la compartirán con otros dispositivos IoT inteligentes, acelerando y mejorando el desempeño de las aplicaciones y sistemas basados en inteligencia artificial. Los expertos de TrendForce aseguran que esta tendencia irá cogiendo fuerza en numerosos verticales, y ponen énfasis en el desarrollo de la fabricación inteligente y la atención médica inteligente, dos campos en los que la IA de las cosas tiene un futuro muy prometedor.

La industria manufacturera apostará por esta innovación para mejorar en resiliencia, flexibi-

lidad y eficiencia, equipando a sus fábricas con dispositivos muy modernos, como los cobots (robots de colaboración) y los drones potenciados por IA que no solo proporcionarán un mayor nivel de automatización, sino también una gran autonomía. En cuanto a la atención médica inteligente, la IA en los dispositivos conectados ayudará a acelerar y mejorar la interpretación de los datos recogidos por los dispositivos de diagnóstico y monitorización de pacientes.

Esto optimizará numerosos procesos y permitirá ampliar mucho las áreas de servicios de las organizaciones de la salud, dentro y fuera de los centros hospitalarios y de atención primaria. Y esta forma de integrar la IA se convertirá en un aliado indispensable en el campo del diagnóstico por imagen, ya que la visión por ordenador permite identificar automáticamente todo tipo de enfermedades y dolencias, ayudando mucho a los médicos en la toma de decisiones clínicas, ya sea en los centros médicos o a través de la telemedicina y las aplicaciones se asistencia quirúrgica remota.

4 INTEGRACIÓN DE GAFAS AR Y SMARTPHONES. Aunque no sea exactamente algo nuevo, la integración de las gafas de realidad aumentada con los dispositivos móviles va a traer una auténtica revolución. Se espera que en este 2021, tanto los dispositivos móviles de gama alta de nueva generación como las nuevas gafas de realidad aumentada se puedan integrar de forma muy sencilla, habilitando un nuevo mundo de posibilidades en campos como el ocio, la formación o el comercio.

Esto se logrará gracias a que los nuevos terminales de gama alta tendrán la suficiente potencia como para mover con fluidez las aplicaciones AR modernas, algo difícil de lograr con la inmensa mayoría de modelos actuales disponibles en el mercado. Además, se está produciendo un gran avance en el campo de las gafas de AR, lo que permite a los fabricantes construir aparatos mucho más livianos, que encontrarán un gran público entre los consumidores, pero también en muchos ámbitos empresariales. Esto hará que tanto los fabricantes de smartphones como los operadores móviles se adentren en este mercado y veamos este año lanzamientos de nuevas propuestas de dispositivos y servicios para las aplicaciones de AR móvil.

COVID-19 REVALORIZA EL MERCADO DE LOS ROBOTS INDUSTRIALES

5 AVANCE DE LOS DISPOSITIVOS DE MONITORIZACIÓN DEL CONDUCTOR. Aunque los vehículos autónomos no serán la norma hasta dentro de unos cuantos años, los coches conectados son una realidad palpable, y las aplicaciones vinculadas a este ecosistema digital en crecimiento son cada vez más. Una de ellas es la de Sistemas de Monitorización del Conductor (DMS), que permiten captar las condiciones del conductor y ayudan a prevenir accidentes. Sumando esto a la monitorización de las condiciones ambientales externas se puede lograr un nuevo nivel de conocimiento y de seguridad.

Esto implica la integración de ciertas capacidades de IA en los vehículos, que permitirán ir más allá de las actuales capacidades en el ámbito del entretenimiento digital a bordo o asistencia básica en los viajes. Los analistas de TrendForce afirman que, en 2021, aumentará de forma notable el número de nuevos vehículos dotados de un Sistema Avanzado de Asistencia al Conductor (ADAS), pero por el momento esto se usará más para dar servicios adicionales como la monitorización del estado del conductor, y no para habilitar una conducción autónoma que todavía está sujeta a numerosos fallos, como demuestran los accidentes ocurridos hasta la fecha.

Afirman que a partir de 2021 se verá un impulso de estas funciones de monitorización avanzada, centrándose en el desarrollo de sistemas de cámaras más activos, confiables y precisos, capaces de detectar signos de somnolencia y falta de atención a la carretera por seguimiento de iris, entre otras innovaciones. Esto servirá para afianzar el papel de los DMS en los sistemas de conducción autónoma del futuro, ya que muchos de ellos pertenecen a niveles de automatización de vehículos en los que se requiere la presencia y atención constante u ocasional del conductor.

6 ADOPCIÓN DE NUEVAS PANTALLAS PLEGABLES. El tamaño de pantalla de los dispositivos móviles siempre ha estado reñido con su portabilidad, algo que los fabricantes quieren solucionar a través del uso de pantallas plegables. Más allá de los primeros diseños conceptuales y prototipos, ahora ya existen propuestas interesantes de los principales fabricantes de móviles, y el año que viene se producirá una expansión de este concepto, que acabará trascendiendo el ámbito de los smartphones. Las previsiones que manejan los expertos de TrendForce son que el año que viene la mejora de precios de este tipo de tecnologías podría capturar una porción mayor del mercado de móviles, que actualmente está muy saturado y necesita recurrir a la innovación constante para generar un impulso de renovación entre los clientes.

LA DUDA DEL GASTO EN TI

La situación por pandemia de COVID-19 no dejó bien parado al mercado tecnológico en 2020, que vio cómo, a pesar de la aceleración de ciertas estrategias de transformación, el gasto caía en picado. En España, IDC tuvo que corregir las cifras esperadas al inicio del pasado año para concluir que terminaría con una caída del 4,1%, con 45,3 mil millones de euros, frente a la previsión de 49,3 mil millones de euros. Para 2021 se espera que la cifra sea aún menor; concretamente, un 0,8% por debajo con un mercado de 44,9 mil millones.

Gartner, por su parte, publicaba a mediados de octubre del pasado año su valoración del mercado. Según la consultora, desde que se declaró la pandemia el mercado de TI se vio sometido a muchas fluctuaciones y, como resultado, los ingresos descenderían un 5,4% con respecto a 2019, quedando en unos 3,6 trillones de dólares. Según su último informe, el pronóstico es que para este 2021 se recuperará la senda del crecimiento, con previsiones de que los ingresos crezcan un 4% en general (3,8 trillones de dólares).

Se espera que, en los próximos años, los fabricantes de móviles den grandes pasos para lanzar teléfonos plegables de diferentes gamas, un aspecto que podría convertirse en fundamental para los móviles del futuro. Y no solo en el mercado de smartphones, sino que los fabricantes de ordenadores portátiles están mirando con buenos ojos hacia esta tecnología para ofrecer nuevas características en ciertas categorías de productos. Así, se espera que la industria de pantallas AMOLED flexibles vea un incremento de los pedidos de fabricantes de portátiles a partir del año que viene.

7 PROGRESO DE LAS TECNOLOGÍAS MINI LED Y QD-LED. Desde hace algunos años la punta de lanza de la innovación en la retroiluminación de pantallas era la tecnología de led orgánico (OLED), que ofrecía una alternativa de buen rendimiento, bajo consumo y sostenibilidad a las pantallas LED convencionales, con algunas mejoras de rendimiento. Pero ahora han surgido dos competidores fuertes, que son la retroiluminación Mini Led y QD-LED, que según los expertos este próximo año podrían capturar buena parte del mercado actual de OLED, especialmente en los televisores y dispositivos móviles, aunque también en ciertas categorías de monitores y equipos portátiles.

Estas tecnologías, con sus diferencias, permiten un mejor control de las zonas de distribución de la luz, y están siendo adoptadas por fabricantes de primera línea como Samsung, que ya está fabricando paneles Mini LED para competir en precio y rentabilidad con sus homólogos basados en OLED Blanco. Al mismo tiempo, Samsung Display está utilizando la tecnología QD-LED para diferenciarse de la competencia ahora que ha cerrado su división de fabricación de paneles LCD, tratando de establecer esta tecnología como nuevo caballo de batalla de su oferta de pantallas de nueva generación.

8 NUEVAS TECNOLOGÍAS DE EMPAQUETADO DE SEMICONDUCTORES. A pesar de las dificultades experimentadas por buena parte de la industria tecnológica en 2020, el progreso de las tecnologías de empaquetado de chips no se detuvo, y los fabricantes siguieron lanzando nuevos y altamente avanzados chips HPC y módulos AiP (antena en paquete). Las modernas técnicas de empaquetado que ciertos fabricantes están usando en estos semiconductores han atraído la atención de los gigantes de la industria como TSMC, Intel, ASE o Amkor.

Estos proveedores están evolucionando sus técnicas para proporcionar chips más avanzados, mejor fabricados y más rentables, que encontrarán aplicaciones en muchas industrias, desde la computación perimetral a las redes móviles, los dispositivos IoT o los smartphones, campos donde estas tecnologías tienen un gran margen de evolución de cara a los próximos años.

9 EXPANSIÓN DEL MERCADO AIoT. En los últimos tiempos, tecnologías como 5G, inteligencia artificial, Internet of Things, el edge computing y la nube están convergiendo, dando como resultado importantes avances tecnológicos como el concepto de "Inteligencia Artificial de las Cosas" (AIoT). Este se basa en dispositivos conectados que integran capacidades de inteligencia artificial para trabajar por sí mismos con los datos que capturan y generan, comunicándose con otros aparatos similares en redes de inteligencia artificial complejas y con una estructura más "neuronal".

La gran diversidad de posibilidades que ofrece el incipiente ecosistema AIoT ha llevado a los proveedores de chips más avezados a ampliar sus miras y trascender las fronteras impuestas por lo que los expertos denominan una industria oligopólica. Porque la mayoría de las áreas tecnológicas están dominadas por unos pocos proveedores que absorben a otras empresas para limitar la competencia, pero estos nuevos paradigmas tecnológicos permiten nuevas posibilidades de desarrollo y expansión, y las em-

presas que están sabiendo navegar por estas aguas encontrarán en el ecosistema AIoT un campo fértil en el que desarrollar su actividad, enfocándose en los numerosos ámbitos de aplicación de esta idea, que ganará peso en las estrategias IoT de muchos sectores a lo largo de estos próximos doce meses.

10 LLEGADA MASIVA DE TELEVISORES MICRO LED DE MATRIZ ACTIVA. En los últimos años la tecnología Micro LED se ha convertido en la gran promesa de los principales fabricantes de televisores, como Samsung, LG o Sony, que ya están preparados para introducir la nueva generación en sus modelos más avanzados. Según TrendForce, en 2021 este será el principal atractivo con que los líderes del mercado de televisores tratarán de impulsar las ventas de las gamas superiores. Y destacan especialmente a Samsung y sus pantallas Micro LED de matriz activa, una tecnología que probablemente se convertirá en el nuevo referente de la industria. ■

MÁS INFORMACIÓN

- Inteligencia Artificial para un transporte más eficiente y ecológico
- Las tecnologías de IoT Industrial seguirán expandiéndose hasta 2025
- Aumenta la demanda de chips de procesamiento de imágenes
- Continúa el crecimiento en el mercado de comunicaciones unificadas y colaboración
- El crecimiento digital impulsa un nuevo récord en el gasto de capital de los operadores hiperescala
- La migración a la nube potencia las ventas de firewalls y puertas de acceso seguras

Si te ha gustado este artículo, compártelo

itTRENDS

Claves tecnológicas para 2021:

La TI salva el negocio

ENCUENTROS IT TRENDS

Claves tecnológicas para 2021: la TI salva el negocio

2020 estuvo marcado por la pandemia y la migración masiva al teletrabajo. La TI salvó el negocio, convirtiéndose así en soporte vital para su continuidad. En 2021 vamos a continuar viendo cómo aumenta la penetración de modelos tecnológicos alrededor de cloud; se perfeccionan las estrategias de puesto de trabajo digital iniciadas a marchas forzadas en 2020; se buscan nuevos planteamientos para garantizar la continuidad del negocio y para reducir costes y optimizar la TI empresarial; se replantea la seguridad de los datos y aplicaciones...

Además, asistiremos a la progresiva penetración de tecnologías que están ayudando a las organizaciones a innovar y generar nuevos productos y servicios, así como modelos de negocio, aprovechando los datos, la automatización, la inteligencia...

Sobre todo ello reflexionaron Víctor Pérez de Mingo, Systems Engineer de Veeam Software; Juan Rodríguez, director general de f5 Networks; y Luis Colino, director preventa de Micro Focus, durante el Encuentro IT Trends titulado "IT Trends 2021. La TI salva el negocio". ■

VÍCTOR PÉREZ DE MINGO, SYSTEMS ENGENIEER, VEEAM SOFTWARE

“En 2021, esperamos una importante actualización de hardware”

Durante 2020 muchos empleos se pudieron salvar por la posibilidad del teletrabajo y las tecnologías disponibles para llevarlo a cabo. “Los trabajadores dispusieron de herramientas de comunicación como Slack o Zoom para mantener el contacto diario, pero ha habido una parte muy importante en la trastienda como los mecanismos para dar acceso a los datos y protegerlos apoyándose en distintas clouds”, señaló Víctor Pérez de Mingo, Systems Engineer de Veeam Software al analizar lo sucedido a nivel tecnológico en 2020, durante la sesión online “La TI salva el negocio”.

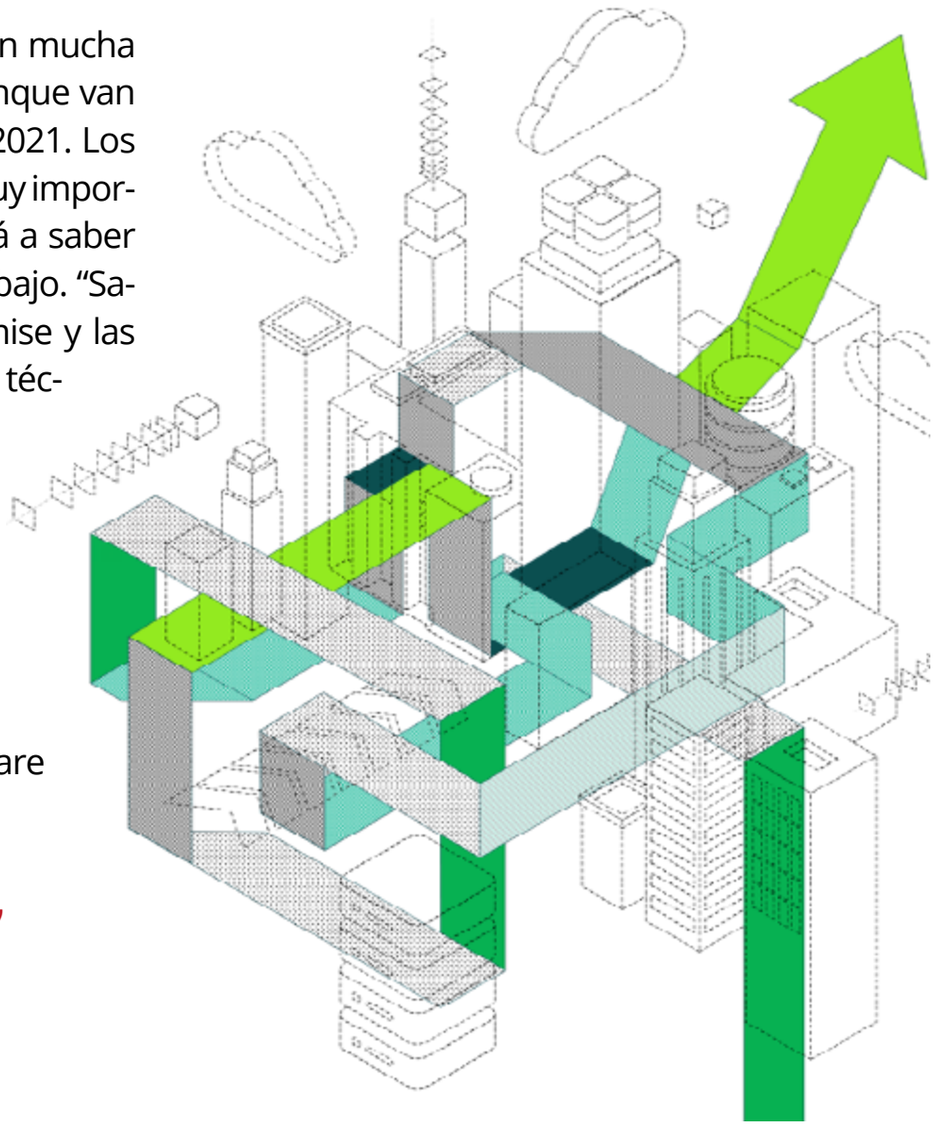
En opinión de este experto de Veeam, “cada vez se van a desplegar menos datos en la nube sin tener claro el plan de contingencia de todos los datos y el reto será añadir dinámicas de protección del dato a las cosas que te llevas a la cloud”.

Las aplicaciones ágiles que permitan poner en marcha servicios escalables en tiempo real será

VÍCTOR PÉREZ DE MINGO, SYSTEMS ENGENIEER, VEEAM SOFTWARE

“Cada vez se van a desplegar menos datos en la nube sin tener claro el plan de contingencia de todos los datos y el reto será añadir dinámicas de protección del dato a las cosas que te llevas a la cloud”

otro de los ejes de 2021. Y 2020 ganaron mucha importancia los equipos de DevOps, aunque van a ser aún más imprescindibles en este 2021. Los procesos de estrategia de datos serán muy importantes para las compañías, y esto llevará a saber cómo y cuándo migrar las cargas de trabajo. “Saber llevar esta estrategia entre on premise y las distintas nubes será vital, igual que las técnicas para ponerlo en marcha”, señaló Pérez de Mingo, quien añadió que, si bien en 2020 muchos presupuestos se congelaron y dedicaron a cuestiones como protección, “en 2021 esperamos un incremento de los presupuestos TI del 10% y buena parte irá dedicada a la modernización del hardware que en 2020 se quedó aparcada”. ■



Si te ha gustado este artículo, compártelo

TENDENCIAS DE LA PROTECCIÓN DE DATOS Y POR QUÉ IMPORTA LA GESTIÓN DE DATOS EN CLOUD

Veeam entrevistó a 1.500 líderes de negocio y TI sobre sus retos y éxitos en la gestión de datos, desde la protección de la información. La compañía detectó que un 73% de las compañías era incapaz de satisfacer las demandas de ofrecer acceso a las cargas de trabajo de forma ininterrumpida, que el 44% afirma que el tiempo de inactividad daña su marca e integridad, y que el 51% reconoce pérdida de confianza de sus clientes por esta inaccesibilidad a sus recursos.

JUAN RODRÍGUEZ, DIRECTOR GENERAL, F5 NETWORKS

“La conectividad será uno de los principales motores en 2021, junto con la transformación digital”

A estas alturas nadie duda de que la covid-19 ha sido el medio por el cual las empresas han tenido que acelerar la transformación digital. La banca, los seguros o las empresas de telecomunicaciones estaban más preparadas que otro tipo de sectores que han tenido que hacer grandes cambios en menos tiempo. “Ahora va a haber una gran inversión en empresas que den valor de extremo a extremo, es decir, desde donde está la aplicación hasta la experiencia final del usuario para minimizar la fricción del acceso en datos en cualquier tipo de entorno y servicio”, indicó Juan Rodríguez, Director General de F5, durante el Encuentro IT Trends junto a Veeam y Micro Focus para debatir las tendencias tecnológicas que a nivel empresarial dominarán en 2021.

El directivo resaltó también que un 75% de las empresas que tienen medidas avanzadas de autenticación y ciberseguridad seguirán

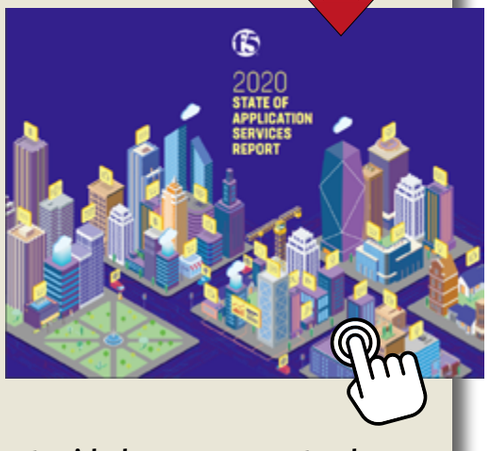
JUAN RODRÍGUEZ, DIRECTOR GENERAL, F5 NETWORKS

“Va a haber una gran inversión en empresas que den valor de extremo a extremo”

siendo objetivo de ataques, “por lo tanto las que no tienen alta protección serán mucho más ciberatacadas durante 2021. Todos los atacantes son peligrosos, pero existen tres tipos de ciberdelincuentes que pueden hacer más o menos daño a las empresas: los que utilizan servicios públicos de ciberdelincuencia por pocos euros son los menos dañinos cuando existen mínimas capas de seguridad, pero también hay ciberdelincuentes que tienen un cierto control y usan herramientas muy complicadas. También existen los ciberdelincuentes más especializados que son desarrolladores y saben de ingeniería inversa de una página o una plataforma y pueden cambiar los patrones”.

De cara a futuro, destacó, entre otros, el posicionamiento de España como uno de los países más avanzados en 5G, y la tendencia de la conectividad como uno de los pilares de 2021. ■

INFORME SOBRE EL ESTADO DE LOS SERVICIOS DE APLICACIONES EN 2020



Para la sexta encuesta anual elaborada por F5, se han preguntado a casi 2.600 profesionales de todo el mundo, de diversas industrias, tamaños de empresas y roles, sobre los desafíos y oportunidades que presenta el proceso continuo de transformación digital. Sus respuestas proporcionan una visión única de las tendencias que configuran el panorama de las aplicaciones.

Si te ha gustado este artículo, compártelo

LUIS COLINO, DIRECTOR PREVENTA, MICRO FOCUS

“Facilitar servicios al empleado y clientes, mejorar esa interfaz tecnológica, será clave en 2021”

Todos los cambios que se produjeron durante 2020 fueron muy rápidos en muchos casos. Por eso, los expertos esperan que se asienten en 2021. La TI híbrida será una herramienta para que la organización sea transparente con un enfoque en el que se puedan gestionar todos los servicios de forma unificada, incluida la gestión del cloud para que las empresas no sufran cuando se hagan cambios. “Se incorporarán nuevas tecnologías donde no las había como la automatización, las herramientas con más seguridad, la unificación de procesos y controlar toda la cadena, además de la inteligencia artificial y la robotización, no solo a nivel de infraestructura sino de procesos”, destacó Luis Colino, director preventa de Micro Focus durante su intervención en el Encuentro IT Trends “La TI salva el negocio”.

El experto de Micro Focus señaló que la incorporación de la IA y el machine learning

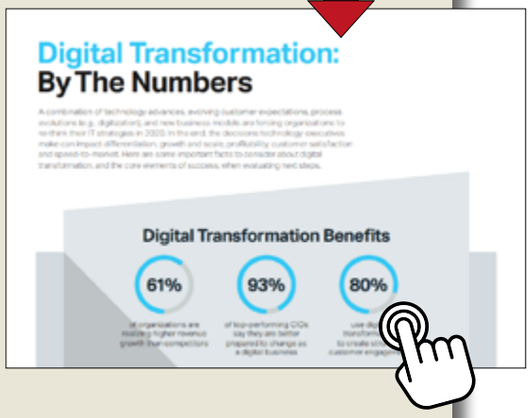
LUIS COLINO, DIRECTOR PREVENTA, MICRO FOCUS

“El próximo año veremos cómo se aplica con mayor insistencia la parte cognitiva de la Inteligencia Artificial a la parte de robotización de procesos”

tanto en el desarrollo de operaciones como en la gestión del dato será otra de las claves de 2021; aún más, “el próximo año veremos cómo se aplica con mayor insistencia la parte cognitiva de la Inteligencia Artificial a la parte de robotización de procesos”.

“En Micro Focus se han incorporado aplicaciones para que los desarrolladores creen sistemas en los que no tengan que intervenir demasiado. Así que hemos lanzado toda la IA en absolutamente todas las opciones, no solo de una parte determinada”, dijo Colino. De esta manera las empresas ayudan a tener esa visión holística del dato y del machine learning, además de las soluciones on premise y las nuevas plataformas de IoT. Asimismo, Colino destacó como prioritario para el próximo año “mejorar la interfaz que nos conecta con el empleado y el cliente, para dar continuidad a esa relación que hemos visto en 2020”. ■

LA TRANSFORMACIÓN DIGITAL, EN NÚMEROS



Una combinación de avances tecnológicos, expectativas de clientes en evolución, y el progreso de procesos y modelos de negocio están forzando a las organizaciones a reconsiderar sus estrategias de TI en 2020. Al final, las decisiones de tecnología pueden marcar la diferenciación, el crecimiento, la rentabilidad, la satisfacción de los clientes y la velocidad para llegar al mercado de una empresa. Esta infografía presenta algunos hechos a considerar con respecto a la transformación digital y los principales elementos para el éxito cuando evalúe sus siguientes pasos.

Si te ha gustado este artículo, compártelo

itTRENDS

2021, ¿el año de la ciberdefensa?

ENCUENTROS IT TRENDS SEGURIDAD

2021, ¿el año de la ciberdefensa?

Reducir las vulnerabilidades, proteger el teletrabajo, los accesos y las identidades; hacer uso de las tecnologías de monitorización y automatización para controlar el comportamiento de personas y máquinas; controlar los datos, estableciendo la trazabilidad segura de los mismos; hacer del threat hunting un arte... todo esto debería ser prioritario en 2021 para mejorar la ciberdefensa.

La automatización y una necesaria proactividad son algunas de las tecnologías que Raúl D'Opazo, Solutions Architect de One Identity; Francisco Verdugo, Ingeniero de Sistemas de VMware; Mario García, Country Manager de Check Point; José María Pérez Romero, Sales Engineer Southern Europe de Entrust, y Josep Albors, Responsable de investigación y concienciación de ESET, pusieron sobre la mesa como necesarias para hacer frente a un 2021 que se prevé más duro en lo que a cantidad y calidad de los ciberataques se refiere, en el Encuentro IT Trends titulado 2021, ¿el año de la ciberdefensa? que se celebró a mediados de diciembre en IT Trends para conocer los retos a los que los responsables de ciberseguridad tuvieron que enfrentarse durante la pandemia, o el impacto de la definitiva disolución del perímetro de seguridad, dando lugar a hablar de dónde se colocarán las inversiones de ciberseguridad el próximo año. ■

RAÚL D'OPAZO, SOLUTIONS ARCHITECT, ONE IDENTITY

"Las empresas necesitan definir estrategias de seguridad centradas en la identidad"

Antes de hablar de lo que nos depara 2021 a nivel de ciberseguridad, arrancamos el debate hablando del impacto que ha tenido la pandemia. Menciona Raúl D'Opazo, Solutions Architect de One Identity, que la crisis de COVID-19 ha acelerado muchos proyectos que sí que se tenían en el roadmap, pero que se "han tenido que adoptar de manera un tanto precipitada", como el teletrabajo, que "ha impactado en las medidas y controles tradicionales de los entornos on-premise y que ha generado retos muy importantes en muy poco tiempo para que el negocio pudiese continuar".

"Para nosotros el foco de la seguridad recae en la identidad del empleado y en los accesos y los permisos que tiene en todas las aplicaciones", dice el directivo de One Identity, añadiendo que, en realidad, cuando hablamos de identidades hablamos tanto de personas como

RAÚL D'OPAZO, SOLUTIONS ARCHITECT, ONE IDENTITY

“En 2021, gran parte del presupuesto se va a centrar en mejorar lo que es la identificación del dispositivo que se utiliza para conectarse a las aplicaciones”

de cosas, que pueden ser procesos automatizados, robots, etc.

En la conversación se planteó que uno de los impactos de la pandemia ha sido la aceleración en la adopción del cloud. ¿Cómo lo han afrontado los clientes? Asegurando que la estrategia de la compañía ha sido “movernos en entornos híbridos, que es donde creemos que actualmente están las empresas”, explica Raúl D’Opazo, añadiendo que este año la diferencia ha sido que “esa oferta que teníamos se ha empezado a utilizar y hemos empezado a desplegar más infraestructura y más productos en cloud”. Y añade que, de cara a 2021, “esta tendencia se acelerará aún más”.

Mencionando el papel de los proveedores de servicios, dice también el ejecutivo de One Identity que son muchas las empresas que realmente no tienen experiencia en ese viaje hacia el cloud, hacia las nuevas aplicaciones y servicios, y que existen cada vez más empresas que están ofreciendo servicios “con un grado de experiencia y conocimiento mayor que el que un cliente tradicional puede asumir”.

Este año, dice D’Opazo, se ha visto mucha actividad en torno a los accesos remotos, “y yo creo que en 2021 gran parte del presupuesto se va a centrar en mejorar lo que es la identificación del dispositivo que se utiliza para conectarse a esas aplicaciones; se va a seguir invirtiendo mucho en que esa persona es quien dice ser con diferentes técnicas de autenticación, y espero que en proyectos de gestión de identidades, pero no solo orientados a esa gestión sino más al gobierno de esa identidad”.

De cara al próximo año Raúl D’Opazo aconseja que las empresas empiecen a definir “estrategias de seguridad centradas en la identidad”. Alrededor de este concepto hay muchas cosas a tener en cuenta, como reconocer el dispositivo desde el que se accede, automatizar la gestión del ciclo de vida de la identidad, la detección de posibles robos de credenciales con tecnologías que puedan ir desde un análisis de comportamiento a grabación de sesiones; “sobre todo que cuando las compañías empiecen a repensar en esas inversiones que quieren hacer, lo hagan siempre pensando un poco en ese vértice: la identidad”. ■

it whitepapers

CÓMO ABORDAR LA COMPLEJIDAD DE UN PROGRAMA DE GESTIÓN DE IDENTIDADES Y GOBERNANZA

El mayor reto de la gestión de identidades (IAM) se basa en la diversidad de los sistemas que deben ser controlados, la complejidad de las soluciones puestas en marcha por parte de las empresas para permitir el acceso seguro, el panorama cambiante de los usuarios y las formas en las que los consumidores deciden acceder a las plataformas.

Si te ha gustado este artículo, compártelo

FRANCISCO VERDUGO, INGENIERO DE SISTEMAS, VMWARE

“El perímetro de seguridad está en el dispositivo, en la identidad y en la aplicación”

A nivel tecnológico se ha aprendido “poca cosa”, afirmó Francisco Verdugo en el Encuentro IT Trends sobre ciberseguridad, cuando le preguntamos qué ha ocurrido durante este año de pandemia. El mayor reto, asegura el ejecutivo de VMware, ha sido el tiempo del que se ha dispuesto y el estado de madurez de tecnologías que permitieran agilizar y dar ese servicio de trabajo remoto, cumpliendo con el criterio de Zero Trust.

Una de las cosas que han quedado claras durante este año es que el perímetro de seguridad está disuelto, un perímetro que ahora “está en el dispositivo, está en la identidad y está en la aplicación, indistintamente de que esté en el cloud o esté en el datacenter”, apuntó Francisco Verdugo, añadiendo que “ahora mismo podemos decir que todo es un perímetro”.

“2021 va a ser una continuación de lo que hemos visto y vivido en 2020”, responde este

FRANCISCO VERDUGO, INGENIERO DE SISTEMAS, VMWARE

“Cada vez se va a pedir menos infraestructura y más servicios”

ingeniero de sistemas de VMware cuando le preguntamos por el binomio cloud y seguridad. Asegura que llevan muchos años ayudando a sus clientes en el tránsito hacia un modelo cloud en el que la seguridad es muy importante. La apuesta al respecto por parte de VMware es seguridad a nivel de red y seguridad a nivel de ciberdefensa y procesos, y todo ello a través de una plataforma única y abierta. “Cada vez se va a pedir menos infraestructura y más servicios”, dice Verdugo, añadiendo que VMware se está posicionando en ese modelo de negocio que supone una oportunidad para los partners. “Tenemos herramientas de ciberseguridad muy avanzadas que pueden ser utilizadas por cualquier socio que quiera ofrecer ese servicio a sus clientes de una forma segura”, añadió.

“No podría deciros con exactitud dónde se va a invertir en ciberseguridad, pero sí dónde me gustaría que se invirtiera, y me gustaría que se invirtiera en inteligencia y en contexto”; esto se traduce en soluciones de seguridad de nueva generación que sepan detectar los ciclos del ataque, que estén preparados para un entorno distribuido en el cual no hay perímetro, y que en cierta medida asegure tanto el dispositivo como el usuario, como el dato o la aplicación que se está intentando consumir. El objetivo, añadió el ejecutivo de VMware, es tener visibilidad y automatismo para hacer frente a las amenazas de manera proactiva.

De cara a 2021 “pediríamos a nuestros clientes que le dieran una oportunidad a un nuevo modelo de seguridad que, en vez de estar basado en capas, lo esté en algo que venga en el ADN de las distintas soluciones, que vayan a ese modelo intrínseco y que empiecen a integrar a los equipos de infraestructuras, y que, en definitiva, la seguridad sea un deporte en equipo”. Agregó Verdugo que hay que darse cuenta de que el modelo determinista ha fallado y hay que apostar por soluciones capaces de detectar la amenaza “por su comportamiento”. ■

SIMPLIFIQUE Y FORTALEZCA SU ESTRATEGIA CON SEGURIDAD INTRÍNSECA

A pesar de las crecientes inversiones de TI en seguridad, los estudios muestran que la probabilidad de que se produzcan infracciones aumenta constantemente cada año. Parece que lo único que aumenta más rápido que el gasto en seguridad empresarial son las brechas de seguridad. Necesitamos comenzar a pensar de manera diferente sobre la seguridad.

Si te ha gustado este artículo, compártelo

JOSÉ MARÍA PÉREZ ROMERO, SALES ENGINEER SOUTHERN EUROPE, ENTRUST

“Un sistema va a ser tan seguro como la protección que le demos a las claves criptográficas”

“No va a sobrevivir el más fuerte, sino el que mejor se adapte al cambio”, dijo José María Pérez Romero, Sales Engineer para Entrust, al ser preguntado por lo aprendido este año. Apuntó, además, que, cuando las cosas se hacen con prisas, no se piensa en la seguridad y que “es un buen momento para reevaluar cómo es la seguridad en el teletrabajo, qué posibilidades tiene cada uno de los usuarios de traer amenazas desde el exterior, etcétera”.

Asegurando que es el usuario el que hace clic en los emails, el que descarga contenido y, al final, quien se está exponiendo, “el perímetro es cualquier elemento con el que el usuario esté en contacto, y como tal, hay que protegerlo”, destacó el portavoz de Entrust durante la sesión, añadiendo que hay que tener mucho cuidado con todas las claves que pueden estar en todas las aplicaciones y en todos los dispositivos.

JOSÉ MARÍA PÉREZ ROMERO, SALES ENGINEER SOUTHERN EUROPE, ENTRUST

“La seguridad cada vez es más amplia y cuenta con más campos, y tener especialistas en cada uno de esos campos es tremendamente difícil”.

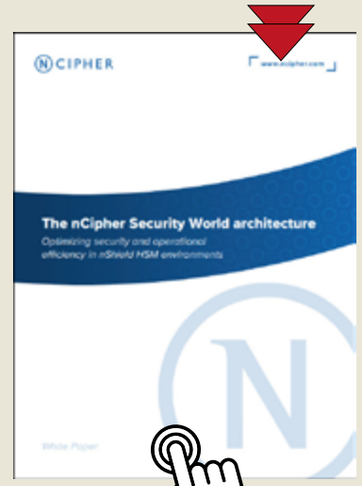
Durante 2020, la adopción del cloud se ha acelerado y, como fabricantes de HSM, lo que los clientes han pedido a Entrust es HSM en el cloud; “es decir, llevar a cabo todo el proceso de protección criptográfica que ya se estaba realizando en el datacenter del propio cliente al cloud, poniendo el foco en el proceso de migración para que pueda haber una migración progresiva”, explica este ingeniero de ventas, añadiendo que los clientes también han solicitado ser los únicos propietarios de las claves criptográficas pese al uso de HSM (módulos de seguridad por hardware) o aplicaciones en el cloud.

Pérez destacó también otra de las tendencias del mundo de la ciberseguridad, la de los servicios gestionados, que se han ido adoptando de forma progresiva. “La seguridad cada vez es más amplia y cuenta con más campos, y tener especialistas en cada uno de esos campos es tremendamente difícil, por lo que es muy importante que las empresas adopten esos servicios gestionados que tienen personal cualificado y expertos en cada uno de los campos de los que se va a ofrecer ese servicio”, añadió.

“Me gustaría que se invirtiese mucho en la protección de claves”, porque en este entorno de teletrabajo los usuarios van a trabajar con aplicativos, cada uno de los cuales va a tener sus claves criptográficas, “y es muy importante que esas claves estén protegidas para poder realizar de forma segura comunicaciones, para poder delegar en lo que es el cifrado. Creo que va a tener mucha relevancia en 2021 el tema de la firma electrónica cualificada”. La realidad, dice José Pérez, es que vamos a trabajar con muy diversas aplicaciones, y éstas, al final, tienen detrás claves criptográficas; “ya sea para establecer una VPN, para autenticar a un usuario ante un portal, en un certificado de un servidor… En cualquier elemento hay claves criptográficas, y un sistema va a ser tan seguro como la protección que le demos a esas claves criptográficas”; un punto en el que juegan un rol muy importante los HSM. ■

Si te ha gustado este artículo, compártelo

THE NCIPHER SECURITY WORLD ARCHITECTURE



La arquitectura nCipher Security World admite un marco de gestión de claves especializado que abarca toda la familia nShield de HSM de propósito general. Esta arquitectura proporciona una experiencia unificada de administrador y usuario e interoperabilidad garantizada ya sea que el cliente implemente uno o cientos de dispositivos.

MARIO GARCÍA, COUNTRY MANAGER, CHECK POINT

“Vale ya de detectar y vamos a empezar a prevenir”

“Que el teletrabajo existe y se puede hacer” es una de las grandes lecciones aprendidas de esta pandemia, aseguró Mario García, Country Manager de Check Point, en el Encuentro IT Trends titulado 2021, ¿el año de la ciberdefensa? Añadió, asimismo, que el teletrabajo se ha hecho deprisa y corriendo, a veces cogiendo atajos, “y eso ha traído muchos problemas de seguridad que los ciberdelincuentes han aprovechado”. Apuntó también Mario García que la pandemia pasará, pero que sus efectos, como el haberse convertido en el primer responsable de la digitalización de las empresas, van a permanecer. Cree, además, que el perímetro se ha roto hace tiempo, pero que mucha gente no se había dado cuenta y que ahora más que perímetro “hay elementos a proteger, y hay que proteger cada uno de esos elementos de la manera adecuada, con las medidas de seguridad correctas dentro de una estrategia de seguridad, que es quizá lo que falta”.

MARIO GARCÍA, COUNTRY MANAGER, CHECK POINT

“Los clientes empiezan a darse cuenta de que es imposible manejar 20, 25 o 30 fabricantes de servicios de ciberseguridad”

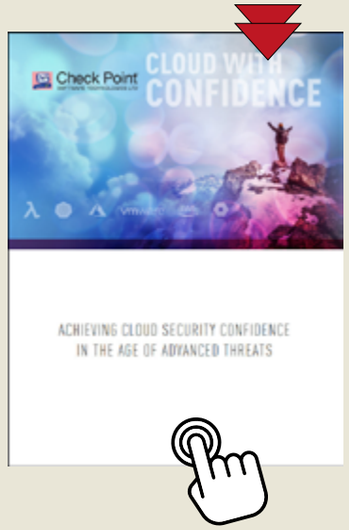
En opinión del director general de Check Point en España, en 2021 se va a acelerar la migración al cloud: “ha habido un cambio radical en cómo se hacen las cosas en la nube” porque, ahora sí, se empiezan a aprovechar las capacidades nativas de la cloud y “tienes que cambiar la forma de implementar la seguridad, de verla, de gestionarla, de manejarla”.

Sobre el papel de los MSSP (proveedores de servicios gestionados de seguridad) en 2021, García opina que la tendencia es la de contratar la gestión de la seguridad, lo que no significa “que los clientes renuncien a controlar qué es lo que tienen”. Asimismo, apunta que habrá varias tendencias que veremos el año que viene: la primera sería la consolidación del acceso remoto, porque “una cosa es poner a trabajar a la gente en remoto y otra poner a trabajar a la gente en remoto de forma segura”. El segundo foco de inversión tendrá que ver con la ciberseguridad relativa a la nube que empezará desde el principio, porque “voy a empezar a controlar el ciclo de desarrollo e implantación de las aplicaciones”. La tercera tendencia es hacia la consolidación, porque “los clientes empiezan a darse cuenta de que es imposible manejar 20, 25 o 30 fabricantes de servicios de ciberseguridad”. Por último hay que intentar ir un paso por delante: “vale ya de detectar y vamos a empezar a prevenir”, y eso implica cambios importantes en la política de seguridad.

Los consejos de ciberseguridad de Check Point van muy alineadas con esas tendencias que apuntaba Mario García. Dice el directivo que si voy a empezar a consolidar la seguridad y a compartir la inteligencia, el primer consejo es “déjate ayudar”. Mencionó también los 8.000 ataques de Día Cero diarios que detectan sus laboratorios y que, “bajo este punto de vista, o tu estrategia de ciberseguridad cambia y es mucho más inteligente y evolutiva, o simplemente no te vas a poder defender”. No hay que olvidarse, añadió, de la formación, tanto de los técnicos como de los usuarios, porque “si no podemos hacer equipo con tus usuarios para mejorar la ciberseguridad, nada de lo que hagamos tiene sentido”. ■

Si te ha gustado este artículo, compártelo

CLOUD CON CONFIANZA



Las empresas habitualmente se quedan cortas en la implementación de seguridad en la nube que pueden ver, administrar y confiar. Este documento técnico ofrece información sobre cómo se puede lograr una prevención óptima de amenazas en la nube y establecer la mejor postura posible de seguridad en la nube para su empresa.

JOSEP ALBORS, RESPONSABLE DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET

“Las empresas fallan en reconocer cuáles son los activos realmente críticos para su funcionamiento”

Sea el uso de la pandemia para realizar las amenazas, la mala preparación de las empresas a la hora de implementar el teletrabajo, la migración precipitada a la nube o la imposición de conexiones remotas desde escenarios que no estaban previstos, como los hogares, “lo que ha venido a confirmar este año de pandemia es que los atacantes van a aprovechar cualquier oportunidad”, dijo Josep Albors, responsable de investigación y concienciación de ESET, en su intervención.

Coincidió Albors en que el perímetro de seguridad hace años que desapareció y que, además de los dispositivos, hay que plantearse proteger los accesos y “limitar los permisos que se le están dando a los usuarios que están accediendo remotamente a la red corporativa porque, cuando son comprometidos, los atacantes utilizan esas cuentas para moverse lateralmente, sin ningún problema ni impedi-

JOSEP ALBORS, RESPONSABLE DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET

“La necesidad de seguridad es vital, pero no todos tienen la capacidad de implementarla in-house”

mento, hasta acceder a los recursos más críticos de la empresa”.

Sobre el binomio seguridad y cloud dijo el ejecutivo de ESET que lo que les han pedido sus clientes ha sido el tener la posibilidad de controlar las herramientas a través de la nube, “algo que ya veníamos implementando desde hace tiempo, pero que se ha acelerado”. De cara al futuro, la compañía tiene previsto “seguir implementando nuevas funcionalidades y herramientas que permitan un mejor control y gestión de todo lo que se maneja, pero desde un entorno cloud”. La adopción de servicios gestionados está creciendo porque “la necesidad de seguridad es vital, pero no todos tienen la capacidad de implementarla in-house”, explicó Josep Albors, añadiendo que son muchos los negocios que prefieren contratar la seguridad a empresas que ya estén trabajando en esta área y que pueden ofrecerle lo que necesitan para protegerse.

La evolución de este año ya indica qué nos deparará el próximo en lo que a inversiones de ciberseguridad se refiere: el representante de ESET apuntó a la protección del endpoint, sobre todo a los que están ubicados fuera del entorno tradicional de la empresa; además “estamos viendo también mucho interés en el tema de cifrado de información para evitar que, si se filtra, pueda ser usada; en el tema de autenticación de identidades; y en gestión de copias de seguridad, de backup, para poder recuperarse de un posible incidente”.

Como consejo de ciberseguridad para 2021 propone Josep Albors algo muy básico “porque estamos viendo que muchas empresas fallan en algo fundamental, como es reconocer cuáles son los activos que son realmente críticos para su funcionamiento y saber cómo protegerlos”. En necesario “saber localizar qué acciones se están haciendo sobre sus activos de forma sospechosa”. Añadió el responsable de investigación y concienciación de ESET que las empresas deben dejarse ayudar, tanto en formación, como en inteligencia o en gestión; “podemos ayudar a todo tipo de compañías que quieran aportar esa capa de seguridad que ahora mismo les falta y que no saben cómo implementar”. ■

Si te ha gustado este artículo, compártelo

TENDENCIAS DE CIBERSEGURIDAD 2021: MANTENERSE SEGURO EN TIEMPOS INCIERTOS

A punto de dar un paso hacia el nuevo año, debemos hacer una pausa y pensar en cómo ha evolucionado el panorama de amenazas de ciberseguridad y cómo los riesgos pueden reformarse y agravarse aún más en el futuro. Mirar hacia atrás y extrapolar con cautela los eventos y tendencias recientes sigue siendo la mejor manera de tener una idea del futuro.

Patrocinado por fastly

Factores a tener en cuenta para diseñar una estrategia de cliente exitosa

Hoy, más que nunca, los clientes toman decisiones basándose en sus experiencias y las marcas deben adaptarse. El cliente tiene en sus manos los medios y la tecnología con la que puede acceder a más opciones que nunca; quieren hacer las cosas a su manera, y las marcas deben proporcionales lo que quieren, de la manera que quieren y cuando lo quieren (y esto es generalmente en tiempo real).

La experiencia de cliente está ganando mayor peso en las decisiones de compra, por lo que la capacidad de las marcas para ofrecer una experiencia que encandile a sus usuarios será el verdadero valor que genere negocio.

Esto se ha vuelto aún más decisivo a raíz de la COVID-19: un 59% de los consumidores se preocupa más por la experiencia cuando deciden a qué empresa apoyar o comprar; al 38% le importa lo mismo que antes de la COVID (que era mucho). En otras palabras, la experiencia del cliente dictará las compras en 2021.

EXPERIENCIA DE CLIENTE VS. SERVICIO AL CLIENTE

Muchas empresas se aproximarán a la experiencia de cliente en 2021 con la misma mentalidad que lo hacían en 2020, pero todo ha

Patrocinado por fastly

cambiado. El mundo empresarial debe reeducarse para entender las necesidades de un usuario que ha pasado buena parte del pasado año encerrado entre las paredes de su casa, teletrabajando, aislado.

En numerosas ocasiones, las empresas siguen igualando la experiencia de cliente con el servicio al cliente, creyendo que es algo en lo que se puede instruir a sus empleados, pero solo combinando cultura, procesos y tecnologías centrados en el cliente podrá construirse la experiencia que el usuario espera. De hecho, muchas compañías carecen de un líder de experiencia de cliente y las que lo tienen, deberían considerar este cargo como uno de los más estratégicos de la organización, posicionándolo en primera línea y dotándole de poder de decisión.

El servicio al cliente debe ser una parte fundamental de la experiencia de éste con nuestra marca, sí, pero ésta se consigue hoy por múltiples canales y todos ellos deben formar parte de una estrategia que marque la diferencia y garantice el éxito del negocio.

5 TENDENCIAS QUE MARCARÁN EL FUTURO DEL ECOMMERCE

UNA EXPERIENCIA INTEGRADA

Los clientes se relacionan hoy con las marcas por múltiples vías. Ya sea en el espacio físico o virtual, la experiencia que se le ofrezca debe ser coherente entre todos los canales por los que se comunica con el usuario.

Además, el consumidor es, hoy más que nunca, digital. Se maneja con dispositivos de diferente índole, consume contenidos desde distintos puntos, compra en muy diferentes momentos del día, y espera que los canales de venta y relación con la compañía estén integrados: si un visitante a una tienda física solicita a un vendedor una consulta sobre un producto y la aplicación que a éste le ofrece la información, falla y tarda, el potencial cliente terminará abandonando la tienda y no adquiriendo el producto. Lo mismo pasará si hace una consulta vía web o aplicación sobre la disponibilidad de un producto y cuando llega a la tienda, éste no está disponible.

El cliente es cada vez más exigente y el mínimo detalle puede hacer que se decante por una marca u otra. Por eso, definir bien una estrategia de experiencia del cliente será el primer paso para la supervivencia empresarial en 2021, especialmente para grandes organizaciones y marcas icónicas, aunque también para los organismos públicos, a cuyos servicios acceden cada vez más los ciudadanos de forma remota.

Además, uno de los efectos de la pandemia es la necesidad de interactuar sin contacto, de for-

Patrocinado por fastly

ma remota y en modo autoservicio. Pagos contactless, menús en códigos QR, o aplicaciones de videoconferencia amigables con el usuario, que no se interrumpen durante la conexión, son elementos que se han convertido en habituales en nuestras vidas y que también forman parte de la experiencia de un cliente con una marca.

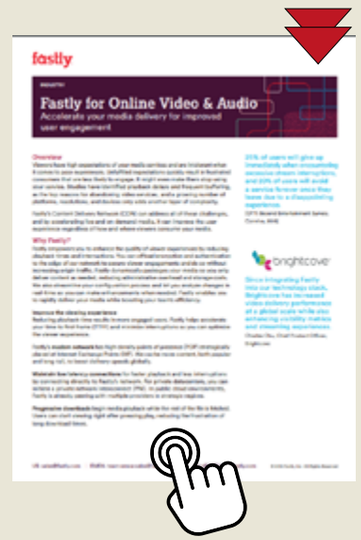
Por eso, las inversiones en tecnología digital para mejorar la experiencia de cliente se dispararán en los próximos años. Según estimó IDC en agosto de 2019, a medida que las empresas se centran en satisfacer las expectativas de sus clientes y proporcionarles una experiencia de cliente diferenciadora, el gasto en CX se dispararía hasta los 641.000 millones de dólares en 2022. La consultora no ha ofrecido una actualización del dato, pero seguramente, tras la experiencia COVID, ésta haya ascendido considerablemente.

El horizonte de la experiencia de cliente se atisba muy dinámico. Inteligencia artificial, chatbots, analítica de datos, realidad virtual, la voz, el vídeo... Todos estos elementos contribuirán a crear experiencias de cliente personalizadas, con un toque emocional y que cubran todo el viaje que el cliente hace en su interacción con una marca. Es, además, una oportunidad para presentarse como una compañía innovadora, que sabe entender la transformación digital y aprovechar las tecnologías para generar empatía con sus clientes que, al fin y al cabo, son quienes le garantizarán el negocio. ■

MÁS INFORMACIÓN

- Contenido sin esperas en los medios de comunicación digitales
- Acelerar la entrega de contenido para mejorar la fidelidad de los usuarios
- El 54% de los españoles cree que los departamentos de ventas, atención al cliente y marketing no comparten información
- La ciberseguridad es clave para la fidelidad: el 59% de los consumidores cambiaría de compañía ante un ciberataque
- 19 millones de españoles han comprado por Internet durante los tres últimos meses

ACELERAR LA ENTREGA DE CONTENIDO PARA MEJORAR LA FIDELIDAD DE LOS USUARIOS



Los espectadores tienen grandes expectativas en sus canales de comunicación y no toleran las experiencias poco atractivas. No cumplir los deseos de los consumidores suele frustrarles y provocar que sean menos propensos a seguir visualizando un canal o plataforma determinada. Incluso puede hacer que dejen de usar el servicio indefinidamente. La red de entrega de contenido de Fastly mejora la experiencia de usuario independientemente de la ubicación o del dispositivo desde donde se conecte.

Si te ha gustado este artículo, compártelo

it TRENDS

Convirtiendo la red moderna para las aplicaciones de próxima generación: una necesidad para la junta directiva

Nick Cross,
Vicepresidente de redes, seguridad y automatización, VMware

Hay un dicho en el fútbol que dice que nunca se nota a un buen árbitro. Sin embargo, tienen el trabajo más importante: garantizar que el partido se desarrolle de la manera más fluida posible. Sin un árbitro que controle la acción, innumerables partidos se convierten en un caos. El mismo principio se aplica a la red de TI. Su función tradicional es dirigir y entregar datos de manera fluida y rápida, desde el centro de datos hasta la nube, desde el borde hasta el dispositivo, de manera transparente y eficiente. Y al igual que al árbitro en un partido de fútbol, no se puede sobrevalorar su poder e importancia.

Sin embargo, en la sala de juntas puede ser difícil hablar específicamente sobre redes. Pero, en el mundo empresarial actual, simplemente no es posible ejecutar aplicaciones modernas nativas de la nube y ponerlas (con el creciente volumen de datos que consumen) en manos de los usuarios sin la red adecuada. Por extensión, las redes son fundamentales para permitir que los empleados trabajen desde cualquier lugar y mejorar la experiencia del cliente y, por lo tanto, mejorar los ingresos y la competitividad. En ese sentido, queda muy claro que el trabajo en red merece un lugar de honor en la agenda de la junta directiva.

Con una fuerza laboral cada vez más dispersa y distribuida, y nuestra dependencia de las aplicaciones modernas, las nubes y los nuevos dispositivos, las organizaciones deben reconocer el valor incremental que ofrece una red modernizada. Una red moderna se entrega en software y es autónoma, autoabastecida, autorreparable, intrínsecamente segura y,

sobre todo, escalable. Pero, ¿cómo y por qué han evolucionado las redes hasta este punto en sus esfuerzos por facilitar la TI empresarial moderna?

“Las redes son fundamentales para permitir que los empleados trabajen desde cualquier lugar y mejorar la experiencia del cliente, los ingresos y la competitividad”

TRABAJO EN RED EN EL CONTEXTO DE DATOS Y APLICACIONES MODERNAS PARA TENER ÉXITO EN LOS NEGOCIOS

Hay dos agentes clave de cambio que impulsan la transformación de la red, el primero es el usuario final. Los usuarios están cada vez más hambrientos de datos y esperan una experiencia cada vez más rica, lo que significa que las aplicaciones deben entregar datos en mayores volúmenes, a más lugares, en más dispositivos, con más frecuencia y en un formato más fácil de usar y consumible.

La naturaleza de todos estos datos y el lugar donde se encuentran ha cambiado radicalmente en los últimos años. Los datos ahora están en todas partes, existiendo en cualquier lugar, desde el centro de datos hasta el borde, endpoints y en cualquier lugar intermedio, creando “centros de datos” distribuidos en lugar de centros de datos tradicionales. En general, IDC predice que entre 2019 y 2025, la cantidad de datos nuevos que se capturan, crean y replican cada año crecerá a una tasa de crecimiento compuesto del 61%.

El segundo agente clave del cambio en la transformación de la red son las aplicaciones, el principal vehículo moderno para entregar datos y experiencias a los usuarios finales. Para 2024 habrá más de tres cuartos de mil millones de solicitudes, un aumento de seis veces en solo diez años. Esto es enorme. Al igual que los consumidores en cualquier otro ámbito de la vida, los usuarios quieren que estas nuevas aplicaciones se entreguen cada vez más rápido a medida que cambian sus necesidades.

Los desarrolladores, por lo tanto, necesitan desarrollar nuevas aplicaciones rápidamente. Necesitan una red que admita este nuevo proceso de rápido desarrollo y que se adapte de forma automática y sin fisuras a las necesidades de las nuevas aplicaciones. Cada vez es más obvio que las infraestructuras de red tradicionales ya no son adecuadas para su propósito en este sentido.

Con tanto depender del éxito de estas nuevas aplicaciones nativas de la nube, las empresas deben comprender el valor que puede ofrecer una infraestructura de red modernizada y brindarles la consideración a nivel directivo que merecen.

NETWORKING EN EL CONTEXTO DE LA DESPERIMETRÍA

La seguridad y las redes han ido juntas siempre, pero a medida que el panorama de las amenazas se ha deteriorado y las demandas de las redes han crecido, estamos viendo una convergencia aún más rápida. Como resultado, la desperimetría (la difuminación de los límites de la red de una organización con el mundo exterior) se está convirtiendo en la norma, ya sea por accidente o por diseño. ¿Por qué? Debido a la creciente adopción de la nube y a que las aplicaciones nativas de la nube modernas se basan cada vez más en arquitecturas distribuidas, como microservicios y contenedores, que existen fuera de la red central. Los excepcionales eventos de 2020 también han acelerado aún más esta tendencia hacia las aplicaciones modernas.

Sin embargo, la desperimetría presenta desafíos. El primero es la complejidad. Con organizaciones que implementan aplicaciones modernas que, en algunos casos, abarcan entornos locales, en la nube y en el borde, es extremadamente difícil para TI administrar las carteras

de aplicaciones y servicios con cualquier nivel de coherencia. El segundo es una superficie de ataque expandida: el aumento en la comunicación de red dentro y entre las aplicaciones distribuidas crea muchas más oportunidades potenciales para brechas hostiles.

El modelo tradicional de sentirse cómodo únicamente con la seguridad basada en el perímetro, es decir, un exterior protegido por firewall "duro" y un interior de red "suave" en gran parte desprotegido, ahora es en gran medida redundante. Las organizaciones necesitan ir al menos un paso por delante de las posibles amenazas, utilizando capacidades de red, como la microsegmentación, para hacer que su infraestructura y aplicaciones sean intrínsecamente seguras, tanto por dentro como por fuera.

Ofrecer una seguridad mejorada a través de la red, en lugar de una plétora de soluciones de puntos discretos, facilita un enfoque universal de "confianza cero" para la seguridad, y la inteligencia, automatización y agilidad adicionales que proporciona. Este es un atributo clave de una red moderna.

FACTORES CLAVE DE UNA RED MODERNA EXITOSA

Las redes modernas exigen una evolución virtual definida por software de la red física tradicional, que aprovecha cualquier infraestructura existente disponible para admitir aplicaciones modernas dinámicas. En efecto, ahora podemos decirle a la red lo que queremos lograr a través de la política de red y seguridad (en lugar de decirle cómo lograrlo), y dejar que la red continúe implementándolo a través de la automatización impulsada por el aprendizaje automático / inteligencia artificial. Es una evolución que impulsa la conectividad universal y consistente, además de brindar seguridad intrínseca a las aplicaciones modernas y tradicionales, tanto para satisfacer la demanda de los usuarios con rapidez como para respaldar las prioridades comerciales.

"Las organizaciones deben reconocer el valor incremental que ofrece una red modernizada"

Una infraestructura de red moderna y exitosa consta de tres elementos cruciales, a saber:

❖ **Servicios de conectividad de aplicaciones modernas.** Una experiencia coherente para el usuario final es un imperativo empresarial. Las organizaciones necesitan saber exactamente qué usuarios están en la red y las aplicaciones que están usando. Una red moderna utiliza capacidades como una red de servicios para que las aplicaciones puedan comunicarse internamente y entre sí, y modelos de seguridad como Secure Access Service Edge (SASE) para brindar a las redes la agilidad de adaptarse a las necesidades comerciales cambiantes en tiempo real.

❖ **Virtualización de redes multicloud.** Una red moderna también debe ser ágil en respuesta a las prioridades comerciales cambiantes. Debe ser autónoma y autocurativa, utilizando inteligencia artificial y aprendizaje automático para reconfigurar las políticas de red y seguridad mientras está en progreso. De nuevo, aquí es donde entra en juego SASE, dirigiendo el tráfico, paquete por paquete, a través de múltiples nubes y ubicaciones para lograr la más alta calidad de experiencia del usuario.

❖ **Independencia de la infraestructura de red física.** La red definida por software es lo que ofrece la agilidad de una red moderna, pero la infraestructura de red física subyacente sigue desempeñando un papel fundamental: la conectividad física para el tráfico de la red. Actúa como una plataforma genérica para todo uso, controlada por la red virtual superpuesta, que se puede reconfigurar y redireccionar según sea necesario en tiempo real, aumentando o disminuyendo la capacidad. La infraestructura física puede ubicarse en cualquier lugar, y su capacidad se agrega o resta sin problemas a la red virtual, sin afectar la seguridad. Esto permite a las empresas hacer

“La experiencia del cliente está directamente relacionada con el éxito empresarial y se alimenta tanto de aplicaciones modernas como de los datos que fluyen a través de ellas”

un uso rentable de las infraestructuras físicas de múltiples proveedores, dondequiera que se encuentren.

LA RED MODERNA EN ACCIÓN: WILLIAM HILL

Una empresa que ha rediseñado su enfoque de redes para admitir aplicaciones modernas para su negocio es William Hill. William Hill es líder en el mercado global del juego y, a menudo, tiene la tarea de escalar cientos de aplicaciones en tan solo segundos alrededor de los principales eventos deportivos, brindando a los clientes una experiencia fiable y receptiva constantemente. Sus aplicaciones e infraestructura manejan cantidades masivas de datos, y su plataforma de juego en línea publica más de 5,1 millones de cambios de precios todos los días.

Su red moderna garantiza la seguridad mediante un firewall definido por software junto con microsegmentación e integrado con su propia plataforma de nube privada. Esto le permite a la empresa saber que su seguridad es lo más estricta posible, pero también que es capaz de implementar aplicaciones rápidamente cuando se producen grandes eventos deportivos y manejar sin problemas las enormes cantidades de datos que se requieren.

Esta red moderna también hace que los desarrolladores de aplicaciones de William Hill sean más ágiles, ya que su familiaridad con la combinación de estas políticas hace que las secuencias de implementación sean más rápidas y fáciles. Mediante la implementación de una red moderna, William Hill ha proporcionado a sus aplicaciones la agilidad, flexibilidad, apertura, seguridad y escala elástica para satisfacer las necesidades del negocio. En resumen, ha ayudado a que los usuarios finales y los datos a los que necesitan acceder sean, en primer lugar, los mismos usuarios cuya satisfacción impulsa los resultados comerciales.

La experiencia del cliente está directamente relacionada con el éxito empresarial y se alimenta tanto de aplicaciones modernas como de los datos que fluyen a través de ellas. Como muestra William Hill, una red moderna exitosa pone al usuario final en primer lugar, adaptándose de manera inteligente y automática para cualquier lugar en el que se encuentre. Al permitir una mayor alineación con los resultados comerciales, las redes modernas proporcionan la base digital invaluable y confiable necesaria para florecer en el mundo impredecible en el que nos encontramos. ■

Si te ha gustado este artículo, compártelo

it TRENDS

Tendencias 2021:

¿Qué nos depara un futuro incierto en materia de ciberseguridad?

Josep Albors,
Responsable de investigación y concienciación de ESET

Nadie puede negar que 2020 ha sido de todo menos normal. En el campo de la ciberseguridad hemos visto la evolución de amenazas conocidas como el ransomware, la migración de otras como los troyanos bancarios en busca de nuevas víctimas o el resurgir de aquellas amenazas relacionadas con el minado no autorizado de criptomonedas. Ahora toca ver qué nos depara el 2021 que estamos a punto de estrenar.

ADAPTÁNDOSE A LA "NUEVA NORMALIDAD"

Si algo nos ha demostrado 2020 es la capacidad de adaptación que han demostrado usuarios y empresas para migrar de un puesto de trabajo concentrado en oficinas al teletrabajo. Esto ha supuesto numerosos desafíos y retos que se han resuelto de mejor o peor manera. Obviamente, los delincuentes no han dejado pasar la oportunidad y muchos de los incidentes que se vienen observando desde el inicio de la pandemia están relacionados directamente con una mala implementación de las políticas de seguridad y de una configuración incorrecta de los accesos remotos o los permisos de los usuarios en una red corporativa.

Esto es algo que, lamentablemente seguirá pasando durante 2021 ya que, a pesar de que los incidentes de seguridad han afectado y siguen haciéndolo a empresas de todos los tamaños, esto no parece ser un aliciente suficiente para que muchas otras empresas e incluso organizaciones y administraciones públicas pongan el foco en la seguridad.

Es de esperar que, conforme avance la vacunación de la población y se acelere el regreso a las oficinas, la superficie de ataque disminuya. No obstante, una vez que se ha demostrado que el teletrabajo es efectivo en muchos de los casos, es más que probable que parte de las plantillas sigan prefiriendo trabajar en remoto, lo que implica proporcionar las medidas de seguridad adecuadas en forma de protección de los dispositivos utilizados para la conexión remota, la autentificación de estos usuarios al conectarse a la red corporativa y la protección de los datos esenciales aplicando medidas de cifrado y copias de seguridad efectivas.

EL RANSOMWARE SEGUIRÁ EVOLUCIONANDO

A finales de 2019 se empezó a observar una tendencia preocupante que ha supuesto todo un revulsivo en el funcionamiento del ransomware durante todo 2020 y lo seguirá siendo durante 2021. Los delincuentes ya no se conformaban con cifrar los datos de sus víctimas y solicitar un rescate por ellos. Ahora utilizan varias amenazas en ataques elaborados y, en ocasiones, muy dirigidos que primero inspeccionan la red corporativa a la que se consigue acceder en busca de información interesante para proceder a su robo y, seguidamente, cifrarla.

De esta forma, la extorsión es doble ya que, en caso de que la víctima no pague, no solo no podrá recuperar su información, sino que se expondrá a que esta se filtre, arriesgándose a una importante pérdida de reputación y a las multas correspondientes por incumplir la legislación regional relacionada con la protección de datos.

Además, durante los últimos meses se han estado observando nuevas tácticas que junto a la popularización del "ransomware as a service" hace que cada vez haya más actores intentando llevarse una parte del pastel que representan este tipo de extorsiones, tendencia que seguirá produciéndose durante 2021.

TROYANOS BANCARIOS Y SU IMPACTO

Otra de las consecuencias que produjo la pandemia y los confinamientos derivados de ella fue que muchos usuarios que, hasta el momento no se habían animado a utilizar la banca online se vieron prácticamente obligados a ello. Con este aluvión de nuevos usuarios, algunos grupos de delincuentes vieron una oportunidad de oro que no han querido desaprovechar y, entre ellos nos encontramos grupos procedentes de América Latina que han ido ampliando sus horizontes saltando de esa región a países europeos, destacando España como uno de los más afectados.

Así pues, desde inicios de año hemos observado como numerosos troyanos bancarios procedentes de esa región han tratado de obtener nuevas víctimas al otro lado del charco. Amenazas como Casbaneiro, Grandoreiro, Mispadu o Mekotio son algunas de las más destacadas, siendo su medio principal de ataque el correo electrónico.

Con el paso de los meses hemos ido analizando numerosas campañas y viendo la evolución de sus tácticas y detectando cómo, entre estos grupos, existe una colaboración para crear nuevas campañas y hacerlas más efectivas. En el futuro cercano no esperamos que disminuya su actividad por lo que creemos que los troyanos bancarios con origen en Latinoamérica seguirán siendo una importante amenaza para los usuarios españoles y también para otros países europeos en los que estos delincuentes han puesto su punto de mira recientemente.

EL RETORNO DE LOS CRIPTOMINEROS

En el momento de redactar este artículo nos encontramos en una situación con respecto a la cotización de las criptodivisas muy parecida a la observada a finales de 2017, con el Bitcoin volviendo a marcar máximos históricos cercanos a los 20.000 dólares. El incremento progresivo de su valor, experimentado por esta y otras criptomonedas justo desde el inicio de los confinamientos estrictos que se empezaron a observar a mediados de marzo, no ha hecho más que reavivar el interés de los delincuentes, tal y como ya vimos hace unos años.

No obstante, las técnicas han cambiado con respecto a las observadas en las campañas de hace unos años y, si bien siguen existiendo botnets (red de equipos informáticos infectados que permite su control remoto), también se observan ataques más elaborados y dirigidos incluso a los propios servicios de criptomonedas.

Es de esperar que, si este aumento en el valor de las criptomonedas sigue produciéndose durante los primeros meses de 2021, veamos como siguen aumentando los ataques que, de forma exclusiva o parcial, buscan obtener mayores beneficios mediante el robo o la minería. Ya hemos visto ejemplos en los casos de los troyanos bancarios y también incluso con casos de ransomware pero estos no son las únicas amenazas que pueden incorporar la criptominería en su arsenal.

Las predicciones expuestas en este artículo se basan en la observación y la evolución de las tendencias de los últimos meses y es probable que, tal y como pasó en 2020, aparezcan factores no contemplados que provoquen la aparición de nuevas amenazas o la predominancia de unas sobre otras. En cualquier caso, conviene estar informado de estas tendencias para así poder protegerse de forma adecuada frente a ellas. ■

Si te ha gustado este artículo, compártelo

it TRENDS

Cómo el cambio remoto está afectando las tendencias de seguridad de TI

Raúl D' Opazo,
Solution Architect EMEA,
One Identity

Este ha sido un año de muchas incertidumbres inesperadas; entonces, ¿qué nos traerá el próximo año? ¿Cómo podemos realmente adivinar, especialmente después de que muchas predicciones hechas para 2020 cambiaron con la pandemia global?

El mayor punto de cambio que está afectando lo que prevemos para 2021 es el trabajo remoto, con las empresas cambiando sus líneas de defensa a los usuarios como un nuevo perímetro en lugar de los puntos finales tradicionales. La nube se ha convertido en el centro de la nueva realidad laboral, creando flexibilidad para los empleados, y las organizaciones tuvieron que abordar los desafíos inmediatos presentados por el paso agresivo a la computación en la nube, principalmente encontrando soluciones que simplificaron la administración y la seguridad de quién tiene acceso a qué y cómo.

Tras los recientes cambios rápidos causados por la transformación digital acelerada y forzada, las organizaciones deben centrarse, cuanto antes mejor, en abordar los aspectos básicos de seguridad para garantizar que su nuevo entorno de trabajo respaldará y no obstaculizará sus operaciones comerciales el próximo año.

ELIMINACIÓN DE ATAQUES PRIVILEGIADOS A TRAVÉS DE UNA ARQUITECTURA DE CONFIANZA CERO

La adopción en toda la industria de la arquitectura de confianza cero hará que sea aún más desafiante para los ciberdelincuentes ejecutar el 80% de las infracciones que aún involucran credenciales comprometidas o débiles. La publicación final de NIST SP 800-207 permitirá que más empresas y agencias gubernamentales adopten el concepto de arquitectura de confianza cero. Este cambio alejará a las empresas de las ideas básicas de los permisos persistentes y el acceso incontrolado tanto de humanos como de computadoras.

El acceso privilegiado ya no necesitará ser persistente o permanente, sino que se asignará y se otorgará acceso por sesión, llevando la vieja idea de "privilegios mínimos" un paso más allá para proteger los datos confidenciales. A través de la arquitectura de confianza cero, las codiciadas cuentas privilegiadas, a las que se apunta comúnmente, se "administran" de manera más efectiva, lo que las hace simplemente no valiosas para el proceso de ataque.

EL AÑO DE LA VIOLACIÓN DE DATOS EN ENTORNOS DE TRABAJO REMOTO

A principios de 2021, habrá un número creciente de empresas que comenzarán a reconocer las violaciones de datos que ocurrieron en 2020. En respuesta, habrá un número drástico de auditorías regulatorias, lo que hará parecer que las violaciones de datos van en aumento. Sin embargo, la gran mayoría de las infracciones que se publicitan no serán nuevas.

En cambio, las brechas que acaparan los titulares serán oportunidades que se aprovecharon

durante el caos y la falta de gestión en el cambio al trabajo remoto. Esto hará que muchas empresas comiencen a realizar arreglos de seguridad rápidos y se centren en la gestión de cuentas privilegiadas para abordar el problema. Sin embargo, las agencias gubernamentales ya habrán reconocido cuán lentas son las empresas para identificar una infracción, lo que resulta en la implementación de prácticas de auditoría más estrictas.

EL NACIMIENTO DE LA IDENTIDAD DIGITAL DE RPA

2021 será el nacimiento de las identidades digitales para la fuerza laboral digital. Lo que muchos profesionales de la seguridad no se han dado cuenta es que las identidades de usuario creadas para que las tecnologías RPA se conecten a la red de una empresa y ejecuten una tarea son tan vulnerables como sus homólogos humanos. A lo largo de 2021, los equipos de identidad y seguridad comenzarán a darse cuenta de los desafíos de seguridad no considerados en entornos RPA, como la forma en que la creación y destrucción de trabajadores digitales da como resultado la cuenta huérfana y el arrastre privilegiado.

Como hemos visto con otras innovaciones, esta falta de conciencia sobre las implicaciones de seguridad de RPA provocará una infracción significativa en 2021, lo que hará que los equipos de seguridad reconozcan la necesidad de una gestión y un gobierno privilegiados de la fuerza de trabajo digital.

LA EDAD DE ORO DE LA NUBE

En 2020 vimos cómo el mundo avanzaba drásticamente en términos de adopción de la nube. Vimos 5 años de adopción de la nube en 5 meses. Las tecnologías en la nube ya no son algo que las empresas consideren opcionales, ahora son la opción preferida. La pandemia y el subsiguiente trabajo remoto ubicuo hicieron del software como servicio y la nube la nueva norma. 2021 será el año del primer mundo personalizable y en la nube. Ya no será un enfoque de todo o nada y la gente ya no hará el intercambio entre la funcionalidad y la nube: querrán la misma funcionalidad independientemente del modelo de implementación.

En cambio, las empresas avanzarán hacia un enfoque más pragmático de la nube en el que eligen el enfoque adecuado para su negocio. Desde la conexión de microservicios entregados en la nube a las soluciones locales y las empresas que se alejan de la infraestructura física para estar completamente en la nube pública, ya no existe una respuesta correcta sobre cómo utilizar la nube. 2021 será el año de la creación de la nube que ofrezca el nivel más alto de valor a la empresa. La protección de esta nueva nube se convertirá en la prioridad número uno para las organizaciones de seguridad.

LA ADOPCIÓN MASIVA DE IGA

Durante el próximo año, las aparentes complejidades de la gobernanza y la administración de la identidad (IGA) se evaporarán. Tradicionalmente, para lograr un programa IGA completo, las organizaciones deben adoptar un marco relativamente pesado dentro de su estrategia de administración de identidad y acceso. Sin embargo, según Gartner, los esfuerzos de implementación de IGA representan aproximadamente el 80% de la automatización de procesos comerciales, y aun las organizaciones continúan utilizando enfoques de implementación centrados en herramientas.

En 2021, las complejidades en torno a las plataformas IGA disminuirán. Al aprovechar sus inversiones existentes, como Active Directory y ServiceNow con los servicios prwestados por IGA, las empresas podrán lograr un nivel de cobertura más completo. Esto permite a las organizaciones una forma más rentable y eficaz de gestionar los riesgos de seguridad y cumplimiento. ■

MÁS INFORMACIÓN

La nube híbrida lidera el viraje hacia una nueva era de las TI

Si te ha gustado este artículo, compártelo

it TRENDS

Cinco aportaciones de una CDN moderna a la promesa del comercio *"headless"*

Jesús Martín Oya,
Sales Director Southern Europe & Middle East, Fastly

Muchas empresas han tenido que adaptarse a la "nueva normalidad", pero en ningún sector ha habido tantos cambios como en el comercio electrónico. El porcentaje de compras online ha subido entre un 20% y 30% en algunos distribuidores, según datos de CNN. Como resultado de estos cambios, un 70% de los participantes en un estudio de Gartner afirma haber acelerado su transformación digital.

Las empresas están acelerando la digitalización migrando a una arquitectura headless para mejorar la experiencia de cliente en el comercio electrónico. De hecho, Gartner ya aseguró a comienzos del pasado año que el comercio electrónico basado en API (o headless) sería una de las 10 principales tendencias del comercio digital de 2020.

¿QUÉ ES LA ARQUITECTURA HEADLESS?

Una plataforma headless es agnóstica en su front-end, permitiendo a los desarrolladores construir varios "encabezados" para canales específicos que se comunican a través de una API común. Las redes de entrega de contenido, las CDN, se utilizan normalmente para mejorar el rendimiento de la web y de los móviles, pero las CDN antiguas no están hechas para soportar arquitecturas headless, enfocadas a las API.

Para sacar realmente partido a la promesa de personalización y rendimiento que ofrece el comercio headless, es necesario utilizar una CDN moderna construida en una plataforma de cloud edge en línea con las necesidades del desarrollo de aplicaciones actuales. Exploremos las cinco formas en las que una cloud

Las empresas están acelerando la digitalización migrando a una arquitectura headless para mejorar la experiencia de cliente en el comercio electrónico

próxima al extremo de la red puede hacer cumplir la promesa del comercio headless.

1. Se optimiza el rendimiento

En la era de la velocidad, los consumidores no toleran las experiencias lentas o el tiempo de inactividad en las webs. El 90% de los compradores abandonan una página web si carga demasiado lento, según una encuesta de Retail System Research.

Las API pueden ser un posible cuello de botella en una arquitectura headless, ya que todas las solicitudes de los clientes convergen en el mismo recurso de API. Por eso es crucial mantener el tiempo de actividad y el rendimiento de las API, un desafío que se hace más difícil a medida que se escala porque si la API de un usuario se cae, todas las webs y aplicaciones dependientes de ella dejarán de funcionar.

Una red de entrega construida en una plataforma cloud edge puede almacenar en caché el contenido dinámico invalidando instantánea y programáticamente las respuestas de la API en el extremo de la red, lo que aumenta el rendimiento y la resiliencia de las aplicaciones de comercio headless. Las empresas que utilizan plataformas de comercio electrónico tradicionales están acostumbradas a aprovechar las CDN para reforzar el rendimiento y la resiliencia, sin embargo, la mayoría de las CDN antiguas no pueden almacenar en caché las respuestas de la API porque son incapaces de invalidar el contenido obsoleto.

2. Los microservicios se usan de manera inteligente

Las API que hay tras el comercio headless están construidas sobre microservicios, por lo tanto, dependen del enrutamiento de las solicitudes directas al servicio de API apropiado. Aunque los balanceadores de carga están diseñados para realizar esta tarea (ya sea desde la nube o desde el hardware), la mayoría de ellos presentan problemas para las arquitecturas headless.

Por ejemplo, la mayoría de los balanceadores de carga basados en la nube (como los que ofrecen la mayoría de las CDN antiguas) están construidos sobre el DNS, por lo que no pueden limitar su capacidad de enrutar el tráfico sólo por la dirección IP o ejecutar cambios de enrutamiento al instante.

Por otra parte, una CDN moderna, construida en una plataforma de edge cloud soporta microservicios permitiendo a las empresas definir decisiones de enrutamiento basándose en el contenido, a la vez que proporciona una convergencia y una recuperación ante errores instantáneas. A diferencia de las soluciones basadas en el DNS, las empresas obtienen un control inmediato y granular. También pueden proporcionar un mejor rendimiento y ahorro de costes con respecto a los ADC, especialmente para el tráfico pico.

3. Personalizar experiencias para una mayor conversión

La personalización de la página web podría aumentar las ganancias del negocio hasta un 15%, según Gartner. La mayoría de las empresas reconocen el valor de ofrecer experiencias personalizadas para aumentar la conversión y el valor medio de los pedidos, pero puede haber un importante desafío técnico en las arquitecturas headless. Con una CDN antigua, no se pueden enviar los datos de los visitantes entre los encabezados y el back-end en tiempo real, por lo que no se pueden personalizar realmente las experiencias de los compradores.

Una CDN moderna puede usar la información del cliente para ajustar rápidamente el contenido que se sirve a los visitantes en función de su ubicación, el tipo de dispositivo o el idioma. Las contestaciones pueden devolverse mediante la respuesta de la API, lo que permite servir diferentes versiones de su página web o aplicación dependiendo de si el comprador está accediendo desde un dispositivo móvil, un portátil, un kiosco de información, un reloj inteligente o un chatbot. También puede ofrecer diferentes experiencias por tipo de visitante, lo cual es útil si desea que los clientes habituales tengan una experiencia diferente a la de los nuevos usuarios para aumentar aún más la conversión.

4. Se descubren y arreglan los problemas más rápidamente

Para garantizar que los visitantes tengan la experiencia deseada en las diferentes aplicaciones y sitios de comercio headless se necesita visibilidad en tiempo real de las solicitudes y respuestas de la API en la capa de red. Sin estos datos, no podrá optimizar la experiencia de los visitantes ni solucionar los problemas de forma eficaz.

Las herramientas de análisis del comportamiento del usuario, como Google Analytics, son insuficientes para las API, y las CDN antiguas normalmente no pueden transmitir registros en tiempo real desde el extremo de la red ni exponer cualquier aspecto de las solicitudes y respuestas.

El 90% de los compradores abandonan una página web si carga demasiado lento

Una CDN moderna puede proporcionar visibilidad completa de la API retransmitiendo los logs de cualquier tipo de petición y respuesta desde el extremo de la red casi en tiempo real. Esto proporciona visibilidad de cómo los visitantes se involucran con tus sites y aplicaciones, permitiendo identificar tendencias y resolver cualquier problema con la entrega de la API. Aún más, se puede monitorizar el impacto de los nuevos despliegues de código o de versiones de las API y, en caso de que surja un problema, volver a una configuración anterior en cuestión de segundos. Esta visibilidad también se puede utilizar para responder a los eventos de seguridad, proporcionándote valiosa información para remediar problemas rápidamente.

5. No hay que sacrificar la seguridad a cambio de la velocidad

Las API y los microservicios proporcionan la estructura de conexión para las aplicaciones modernas. La otra cara de la moneda es que los ciberdelincuentes lo saben y tratan de extraer los datos que se ponen a disposición de los usuarios legítimos y los socios comerciales. Esto queda patente en la predicción de Gartner que afirma que los abusos contra las API se convertirán en el vector de ataque más frecuente en 2022. Por tanto, es fundamental mantener la plataforma segura sin que esto afecte a la experiencia de compra o perder la agilidad que el comercio headless puede ofrecer.

Con una CDN tradicional, hay que hacer sacrificios entre el rendimiento y la seguridad. Sin embargo, las modernas CDN ofrecen una protección avanzada WAF, API, bot y DDoS con una latencia mínima para mejorar experiencia de compra. Aplicar técnicas de rate limiting también ayuda a proteger el coste y la resiliencia de las API. Además, con la mayoría de las CDN modernas la seguridad se consigue enviando el tráfico a través de una red segura, a diferencia de las CDN antiguas, que a veces utilizan una red separada para conseguir un tráfico seguro. Todo esto se combina para ofrecer experiencias de comercio headless libres de ciberdelincuentes sin perjudicar el rendimiento. ■

Si te ha gustado este artículo, compártelo