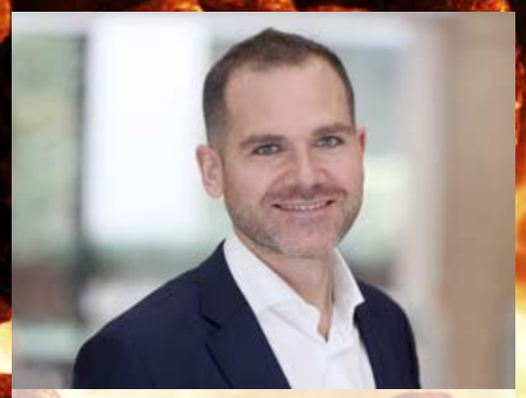
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Enero 2021 - nº 37

El ataque a SolarWinds pone en jaque a medio mundo



‘Todas las empresas iremos hace SASE’ (Carlos Manchado, Naturgy)

‘2021, el año de la IA y la automatización’ (Pedro Pablo Pérez, Telefónica Tech)

‘El modelo Zero Trust es una utopía’ (Francisco Valencia, CEO de Secure&IT)

IT Trends. 2021, retomando el futuro interrumpido

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

it Digital Security

SolarWinds, o el ataque que pone en evidencia las vulnerabilidades de las agencias gubernamentales estadounidenses

Aunque pesar de contar con más de 300.000 clientes repartidos por todo el mundo, SolarWinds era una empresa relativamente desconocida. Suele ocurrir cuando te dedicas a una cosa muy concreta, y aunque el producto sea un referente dentro del mercado. La compañía, víctima de uno de los peores ciberataques que se recuerdan, se ha convertido en protagonista de lo que el presidente norteamericano Biden asegura que es “un grave riesgo de seguridad nacional”, un ataque cuyo alcance podría ser peor de lo esperado y que afecta a multitud de organismos gubernamentales, lo que pone de manifiesto la vulnerabilidad de estos organismos.

Todo apunta a que detrás del ataque hay un estado-nación que, durante nueve meses, se ha aprovechado de la ubicuidad de la plataforma Orion de SolarWinds para espiar gobiernos y empresas de todo el mundo, aunque principalmente de Estados Unidos. Inicialmente hay 18.000 víctimas potenciales, que son las que, la primavera pasada, se descargaron una actualización del producto que incluía un malware al que se ha bautizado como SunBurst.

El verdadero alcance de la campaña y sus motivaciones aún se desconocen, y es posible que durante los próximos meses sigamos añadiendo detalles. Existen indicadores de que puede ser parte de una campaña aún más amplia que se extiende más allá del software de SolarWinds.

Hay quienes aseguran que ya se había avisado a SolarWinds, en noviembre de 2019, de que el sitio web de descarga de software de la empresa estaba protegido mediante una contraseña simple. Los secretos se irán desvelando próximamente y las consecuencias legales y reglamentarias dependerán de lo que SolarWinds sabía o debería haber sabido sobre el incidente, cuándo y cómo respondió.

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

it Digital Security

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

it Digital MEDIA GROUP

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

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

En Portada

El ataque a SolarWinds pone en jaque a la industria

itds

Sumario

Actualidad

Revista IT Trends

Brechas de Seguridad, ¿hay opciones?

Entrevistas

Carlos Manchado, Naturgy

Pedro Pablo Pérez, Telefónica Tech

Francisco Valencia, CEO de Secure&IT

Carlos Ferro, Thycotic

No solo IT

La industria del Ransomware: discreción, mucha paciencia y buenos sistemas de información

Un cuento de Navidad... o sueñan los androides con ovejas eléctricas

Índice de anunciantes

Resiliencia, SOCs y Cooperación, las claves de la nueva estrategia europea de ciberseguridad

La Unión Europea ha dado un impulso a su estrategia de ciberseguridad para reforzar la resiliencia colectiva contra las amenazas mediante la adopción de nuevas medidas y normas, anunciadas a finales de diciembre por la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, Josep Borrell.

La ciberseguridad es clave para el desarrollo digital de la sociedad y la economía, y Bruselas lo tiene claro desde hace años. El pasado 16 de diciembre se desvelaron las nuevas medidas y normas que se irán poniendo en marcha y que sirven para actualizar los ejes de su anterior programa en este ámbito, que data de 2013, y bajo cuyo paraguas se aprobaron diversas iniciativas y regulaciones. Por ejemplo, Directiva SRI, en vigor desde 2016, que fue la primera ley en materia de ciberseguridad a escala de la Unión y contribuyó a alcanzar de manera uniforme un elevado nivel de seguridad de las redes y los sistemas de información en toda la UE. Además, el Reglamento de Ciberseguridad, en vigor desde 2019, dotó a la UE de un marco de certificación de la ciberseguridad de los productos, procesos y servicios, y reforzó el mandato de la

THE NEW EUROPEAN CYBERSECURITY STRATEGY

CLICAR PARA VER EL VÍDEO

La nueva Estrategia de Ciberseguridad busca promover un ciberespacio global, abierto, estable y seguro, basado en el estado de derecho y los derechos humanos

Agencia de la Unión Europea para la Ciberseguridad (ENISA).

La nueva estrategia de ciberseguridad gira en torno a tres ejes: resiliencia, liderazgo y soberanía tecnológica; capacidad operacional para prevenir, detectar y responder; y cooperación para promover y avanzar hacia un ciberespacio abierto.

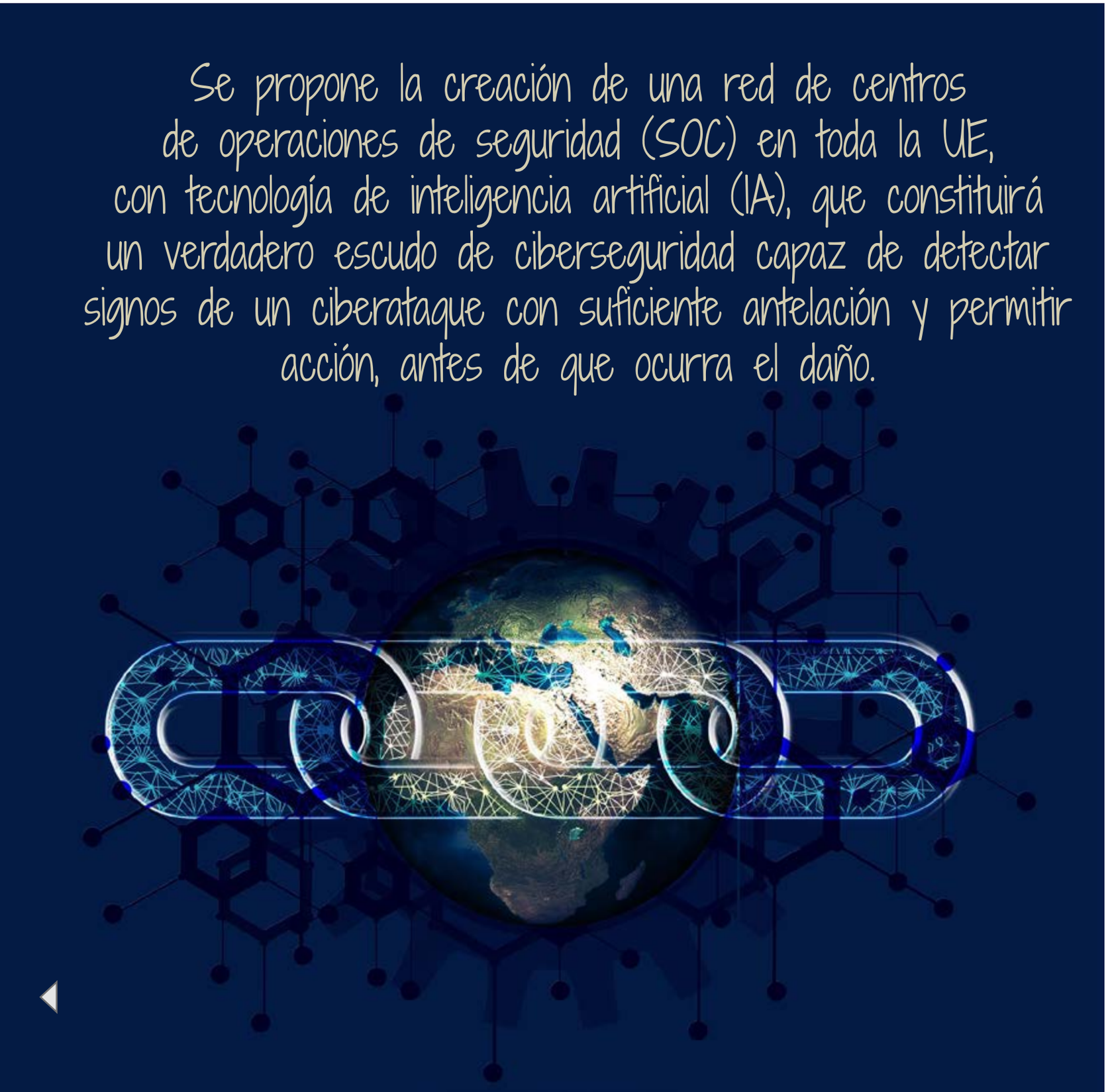
La UE se compromete a apoyar esta estrategia mediante un nivel de inversión sin precedentes en la transición digital de la UE durante los próximos siete años. Esto significa cuadriplicar los niveles anteriores de inversión, lo que demuestra el compromiso de la UE con su nueva política tecnológica e industrial.

Resiliencia y soberanía

En lo que se refiere a las normativas, la unión Europea ha presentado propuestas de actualización de la Directiva SRI para abordar tanto la resiliencia física como la ciberresiliencia de entidades críticas y redes. La Directiva SRI revisada o «SRI 2» se actualizará con medidas de supervisión más estrictas, nuevas sanciones y multas, informes de incidentes simplificados y más.)

Además, se pondrá en marcha una nueva red de centros de operaciones de seguridad en toda la UE que se basarán en la inteligencia artificial y pretende aumentar la capacidad de detección de incidencias de seguridad y poder adoptar medidas proactivas antes de que se produzcan.

Habrá más apoyo para las pymes como parte de la iniciativa Digital Innovation Hubs, un mayor enfoque en la mejora de las habilidades de los trabajadores, más énfasis en atraer y retener talento en ciberseguridad, así como inversión en una investigación e innovación abierta, competitiva y basada en la excelencia.



Capacidad operacional - SOC

Además de la red de centros de operaciones, la comisión está preparando una nueva unidad informática conjunta con el fin de reforzar la cooperación entre los organismos de la UE y las autoridades de los Estados miembros encargadas de la prevención, la disuasión y la respuesta a los ciberataques, que incluyen a las comunidades civiles, policiales, diplomáticas y de ciberdefensa.

La UE también se ha fijado el objetivo de seguir mejorando la cooperación en el campo de la ciberdefensa y el desarrollo de capacidades de vanguardia en este campo, a partir del trabajo realizado por la Agencia Europea de Defensa, así como de animar a los Estados miembros a que hagan pleno uso de la Cooperación Estructurada Permanente y del Fondo Europeo de Defensa.

Cooperación internacional

El último de los ejes se centra en la colaboración internacional en diferentes líneas de trabajo como fortalecer el orden mundial basado en normas, promover la seguridad y la estabilidad internacionales en el ciberespacio, y proteger los derechos humanos y las libertades fundamentales en línea.

La estrategia tendrá como objetivo trabajar con organismos internacionales, como las Naciones Unidas, para ayudar mejor a los esfuerzos de ciberseguridad a nivel mundial a través de una agenda externa de creación de capacidad cibernética. Formará una red global de ciberdiplomacia para “promover su visión del ciberespacio”.

También promete una “inversión sin precedentes” en la transición digital en la UE durante los próximos siete años. La comisión dijo que a través de fondos como el Programa Europa Digital y Horizonte Europa, su objetivo es alcanzar hasta 4.500 millones de euros de inversión combinada de la UE, los estados miembros y la industria.

5G también cuenta

La nueva estrategia europea de ciberseguridad incluye también el avance en iniciativas que ya están en marcha como la aplicación de medidas para minimizar los riesgos de seguridad asociados a 5G. En este sentido la Comisión está animando a todos los estados miembros a finalizar la implementación de EU 5G Toolbox, que establece un enfoque europeo coordinado destinado a mitigar los principales riesgos de ciberseguridad de las redes 5G. La integración debería estar completada en el segundo trimestre de 2021.

La comisión dijo que la nueva estrategia se implementará en los próximos meses, con informes de progreso regulares que estarán disponibles para el Parlamento Europeo, el Consejo de la Unión Europea y otras partes interesadas relevantes. El objetivo es alcanzar 4.5000 millones de euros de inversión combinada de la UE, los Estados miembros y la industria, especialmente en el marco del Centro de Competencia en Ciberseguridad y la Red de Centros de Coordinación, y garantizar que una parte importante llegue a las PYME.

Enlaces de interés...

- Nueva estrategia de ciberseguridad
- Directiva sobre resiliencia en entidades críticas
- ENISA, Agencia Europea para la Ciberseguridad

> La Comisión está preparando, a través de un proceso progresivo e integrador con los Estados miembros, una nueva Unidad Cibernética Conjunta, para reforzar la cooperación entre los organismos de la UE y las autoridades de los Estados miembros responsables de prevenir, disuadir y responder a los ciberataques

Compartir en RRSS

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

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

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Thales unifica las líneas de producto KeySecure y Vormetric en CipherTrust Data Security Platform, una plataforma que ayuda a resolver algunos de los desafíos a los que se enfrentan las empresas, como son la complejidad de la seguridad de los datos causada por la adopción de múltiples nubes, la evolución de las regulaciones de privacidad, así como el riesgo de violaciones de datos por amenazas externas e internas. La nueva plataforma de seguridad de datos CipherTrust permite unificar el descubrimiento, la clasificación y la protección de datos, junto con fuertes controles de acceso y gestión centralizada de claves.

CipherTrust Database Protection, descubrir, proteger y controlar los datos más sensibles donde quiera que residan

CIPHERTRUST DATA SECURITY PLATFORM — **CLICAR PARA VER EL VÍDEO**

Las empresas han tenido que cambiar radicalmente su estrategia en poco tiempo, y lo que ha supuesto un reto para muchas, también ha sido un reto para otras, dice Alfonso Martínez, country manager para la región de Iberia de Thales Digital Identity & Security (CPL), cuando le preguntamos por su experiencia durante la pandemia sanitaria de 2020. Asegura que ha sido un año de cambio, un año de adaptación, y menciona de manera específica el trabajo en remoto, un modelo que requiere seguridad en los accesos, autenticación fuerte, gestión de identidades, etc.

Sobre el mercado de cifrado, dice Alfonso Martínez que la tendencia existía antes de la pandemia, pero que se han dado cuenta de que no es suficiente. Explica que lo habitual es que la gente cifre la información y que, una vez cifrada, la información deja de ser sensible; “lo sensible entonces son las claves de cifrado y por eso hay que poner medidas para custodiar esas claves criptográficas”. Añade que los que tenían la tendencia, les ha sido más o menos fácil continuar e incrementar lo que ya tenían cifrado, pero los que partían de cero “se han encontrado con un mundo” porque “la criptografía es un arma muy potente, pero igual que puede ser sencilla puede ser un caos si no la gestionas de manera apropiada”.

Cipher Trust Data Security Platform

Thales lleva años dedicada al cifrado de la información sensible, el problema para muchas empresas no es tanto el cifrado como el paso anterior: saber dónde tienen toda la información sensible. Explica Alfonso Ramírez que en el mercado se pueden encontrar soluciones que cifran los datos, otras que ayudan a buscar datos sensibles, otras que te los enmascaran…. Y lo que ha hecho Thales es unificar las líneas de producto KeySecure y Vormetric en su plataforma CipherTrust Data Security Platform, una suite que permite, desde una única consola, hacer todas estas tareas.

"Hace ya unos años que no distinguimos entre empresas grandes o pequeñas. Distinguimos entre empresas con datos sensibles o no"

Alfonso Martínez, country manager para la región de Iberia de Thales Digital Identity & Security (CPL)

En general CipherTrust Data Security Platform unifica los elementos más importantes de la seguridad de datos (descubrimiento, protección y control de datos) en una sola plataforma integrada, proporcionando potentes herramientas para hacer frente a las crecientes regulaciones globales y regionales en materia de privacidad, así como el repunte de la adopción de servicios en la nube intensificado por el teletrabajo.

Explica el directivo que “gracias a nuestra sonda vamos a poder descubrir información sensible en cualquier repositorio que haya en la empresa, ya sean bases de datos, archivos y carpetas, servidores, etc.”, y añade que incluso se puede determinar qué es información sensible “porque para cada empresa será sensible una cosa”. La solución incorpora una serie de plantillas con las que se puede determinar, por ejemplo, qué es sensible para GDPR.

Una vez descubierta la información, el usuario puede acceder a una serie de informes que le dicen dónde se encuentra esa información para aplicar una serie de acciones, como puede ser eliminar o mover información de donde no queremos que esté o “cifrar esa base de datos, enmascarar esas tarjetas de crédito, tokenizarlas, etc.”.

Según IDC, para 2025 se crearán más de 175 zetabytes de datos y, en la actualidad, más de la mitad de todos los datos corporativos se almacenan en la nube

Gestión de claves

Uno de los elementos clave de CipherTrust Data Security Platform es que permite gestionar las claves criptográficas. “Con CipherTrust podremos tanto gestionar nuestras claves, las que hemos utilizado para los distintos cifrados, como claves de terceros. Y esto es interesante porque al final los clientes ya tienen soluciones de otros fabricantes que implementan cifrados nativos, pero las claves criptográficas las guardaremos nosotros y haremos esa custodia y gestión del ciclo de vida de la clave”, que no es otra cosa que saber cuándo ha sido generada la clave, a quién pertenece, cuándo caduca… porque no se puede tener cifrada para siempre una información con la misma clave”.

Según IDC, para 2025 se crearán más de 175 zetabytes de datos y, en la actualidad, más de la mitad de todos los datos corporativos se almacenan en la nube. CipherTrust Data Security Platform ofrece potentes funciones para asegurar y controlar el acceso a los datos confidenciales almacenados en bases de datos, archivos y contenedores. Las tecnologías específicas que incluye la plataforma son CipherTrust Transparent Encryption, encargada de cifrar los datos en diferentes entornos y con controles de acceso exhaustivos y registros de auditoría; CipherTrust Database Protection, que proporciona un cifrado transparente a nivel de columna de los datos confidenciales y estructurados; CipherTrust Application Data Protection, que ofrece una API para que los desarrolladores agreguen cifrado y criptofunciones a sus aplicaciones de manera rápida, mientras los procedimientos operativos de seguridad controlan las llaves cifradas; CipherTrust Tokenisation, que proporciona servicios de tokenización de datos, con o sin bó-

CipherTrust Data Security Platform unifica los elementos más importantes de la seguridad de datos (descubrimiento, protección y control de datos) en una sola plataforma integrada

veda, a nivel de aplicaciones; y CipherTrust Batch Data Transformation, que proporciona servicios de enmascaramiento estático de datos para eliminar los datos confidenciales de las bases de datos de producción, de manera que las preocupaciones de cumplimiento y seguridad se mitigan al compartir una base de datos con terceros con el fin de realizar tareas de análisis, pruebas u otros procedimientos.

Habla Alfonso Ramírez de una “súper plataforma” que además “va por módulos”, lo que significa que un cliente puede empezar cifrando una base de datos, “mañana puede comprar el módulo para descubrir y clasificar información sensible, y dentro de seis meses puede tokenizar una base de datos de tarjetas de crédito…”.

Tecnologías de CipherTrust Data Security Platform

Incidiendo en el mensaje de Alfonso Martínez de proteger las claves de cifrado, la gestión corporativa de llaves de CipherTrust Data Security Platform permite a las empresas administrar y establecer estrictos controles de manera centralizada en las políticas y llaves de cifrado para el cifrado de datos in situ y a través de servicios en la nube.

Incluidos en la plataforma encontramos CipherTrust Manager, que centraliza las políticas de claves, gestión y acceso de datos para todos los productos de CipherTrust Data Security Platform y está disponible en un diseño tanto físico como virtual cumpliendo con los estándares FIPS 140-2 de

"La criptografía es un arma muy potente, pero igual que puede ser sencilla puede ser un caos si no las gestionas de manera apropiada"

nivel 3; CipherTrust Cloud Key Manager, que ofrece la gestión del ciclo de vida en la nube con su propia llave (BYOK) para muchos proveedores de infraestructura (IaaS), plataforma (PaaS) y software como servicio (SaaS) en la nube; CipherTrust KMIP Server, que centraliza la administración de llaves para el Protocolo de Interoperabilidad de administración de llaves (KMIP) usado habitualmente en soluciones de almacenamiento; y CipherTrust TDE Key Manager, que centraliza la administración de llaves para el cifrado de Oracle, SQL, y Always Encrypted SQL.

Explica Alfonso Martínez que CipherTrust Data Security Platform es ideal, entre otros, para un proveedor de servicios. Entre las ventaja el poder establecer dominios, de forma que "en el domino A se da servicio a la empresa A, y sólo esa empresa tiene acceso a esas claves"; es, añade el directivo, "una especie de virtualización dentro de CipherTrust de manera que ni el propio administrador de CipherTrust tiene acceso a las claves".

No significa esto que la solución sólo sirva para proveedores de servicio; "hace ya unos años que no distinguimos entre empresas grandes o pequeñas. Distinguimos entre empresas con datos sensibles o no, porque al final las multas le llegan a todos", asegura Martínez.

Resume el directivo que la compañía "aporta mucho valor en las zonas más sensibles de la empresa", como es descubrir dónde está la información sensible, la protección y gestión de las claves, incluidas las de terceros, incluso las que hay en la nube "y que vamos a poder hacerlo todo desde una única consola, que es nuestro gran valor".

De cara a 2021 el objetivo es "acompañar a las empresa a la nube híbrida e intentar facilitarles la vida en todo lo que tiene que ver con el cifrado".

Enlaces de interés...

- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)
- Desayunos ITDS - La seguridad de los entornos multicloud

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

CounterCraft, **cinco años y un producto diferenciador**

Cinco años han pasado ya desde que se creó CounterCraft. Cinco años en los que la compañía ha incrementado el número de clientes y de territorios en los que opera. En 2020 no sólo ha conseguido una ronda de financiación de cinco millones de dólares, sino que su tecnología se ha probado, con éxito, en la OTAN.

Desde el año pasado CounterCraft opera en Estados Unidos, en otros países de Europa, e incluso en Australia, nos cuenta David Barroso, co-fundador y CEO de CounterCraft. Durante estos cinco años de andadura “hemos conseguido tener un producto diferenciador, estable y maduro”, y además se han firmado acuerdos con diferentes tipos de partners, desde PwC, Deloitte o Telefónica, a Thales, Indra o IBM.

El perfil de cliente también ha evolucionado dentro de la compañía. Si se empezó con clientes grandes, y se continuó con gobiernos y organismos militares, desde el año pasado se trabaja con empresas menos grandes gracias al acuerdo con los partners antes mencionados que ofrecen el producto en modo servicio.

El pasado mes de junio la compañía consiguió una inyección de capital de 4,5 millones de euros que han servido fundamentalmente “para potenciar el negocio internacional”. En Estados Unidos la compañía ya cuenta con dos personas y ampliará la plantilla en Europa. La cifra, además, impulsa la estrategia para 2021: acelerar las ventas potenciando los mercados de Estados Unidos y Centroeuropa. En España… “vamos a incrementar el equipo técnico para la parte de desarrollo de producto”.

2020 no sólo es el año en que la compañía cumplió un lustro, sino el año de la pandemia. Las

La tecnología de CounterCraft ha llegado a la OTAN, con quien se ha realizado un proyecto de seis meses en una simulación contra potenciales ciberataques

empresas se lanzaron a cubrir el teletrabajo, plataformando equipos, estableciendo conexiones seguras, habilitando herramientas de colaboración, etc. ¿Han tenido tiempo de hacer deception, de poner trampas y engaños a los ciberdelincuentes? “Es cierto que a partir de marzo o abril todo el mundo ha estado comprando VPN y a nosotros se nos retrasaron proyectos que se iban a iniciar en esas fechas”, dice David Barroso, añadiendo que el parón ha sido más en España que en el resto del mundo. Esto “nos llevó a intentar cambiar nuestro mensaje, nuestra posición de valor”, y por eso el pasado mes de mayo lanzaron una nueva gama de servicios “que han crecido y permiten crear campañas de engaño de forma remota”, dice el CEO de CounterCraft. Los nuevos servicios “que permiten generar campañas de engaño que se pueden automatizar fácilmente son”:

VPN Threat Intelligence Service, un servicio de detección de ciberataques a conexiones VPN y de acceso remoto, que tradicionalmente no han sido un vector de ataque muy destacado, pero que en muchos casos no son lo bastante seguras o no se utilizan como deberían, lo que las convierte en la puerta de entrada perfecta para las amenazas externas. Este servicio de CounterCraft recaba inteligencia desde el momento en que un atacante interactúa con el “cebo” o el activo de Cyber Deception de CounterCraft.

Pre-Breach Activity Threat Intelligence Service recoge inteligencia sobre la fase previa para acometer un incidente de robo de información, la fase más complicada y vital de detectar para evitar o

- **2016.** David Barroso, Fernando Braquehais y Dan Brett fundan CounterCraft en diciembre, después de meses estudiando la viabilidad del proyecto y el potencial de la tecnología.
- **2017.** Superando a otras 60 empresas, la compañía consigue una plaza en el NCSC Cyber Accelerator del Reino Unido, parte del Centro de Innovación de Cheltenham. Durante tres meses pudieron consultar a los mejores expertos del país para mejorar su producto.
- **2018.** La compañía pasa de cinco a 19 miembros, se crea el primer equipo de ventas y empiezan a operar en Inglaterra. Además, teniendo en cuenta los comentarios de sus clientes, se lanza la versión 2.0 del producto.
- **2019.** La compañía consigue su primer cliente en Estados Unidos tras superar una serie de procesos que le convirtió en la mejor opción por la proactividad en su respuesta a los actores de amenazas. Esto les lleva a abrir oficina en Estados Unidos
- **2020.** El año de la pandemia ha sido un año de financiación para CounterCraft. Además, la compañía ha lanzado nuevos servicios y sigue su proceso de internacionalización.

reducir el impacto del ataque. Al lanzar este servicio, el usuario puede descubrir sus vulnerabilidades y obtener información precisa y valiosa sobre las técnicas y procedimientos que el adversario quiere emplear.

Para luchar contra campañas de phishing dirigido, CounterCraft lanza **Spear Phishing Threat Intelligence Service,** un servicio diseñado para obtener información concreta y proactiva sobre este tipo de amenazas sin consumir recursos adicionales por parte de la organización.

Deception

Las tecnologías de deception, de engaño, de poner trampas a los atacantes para retrasarlos y averiguar sus intenciones, no son nuevas. Hace ya muchos años que se habla de los “honeypots” y de las “honeynets” y que lo que se reconoce a CounterCraft

El pasado mes de junio la compañía consiguió una inyección de capital de 4,5 millones de euros que han servido fundamentalmente para potenciar el negocio internacional

es que haya profesionalizado el concepto, que haya automatizado la tecnología.

Dice David Barroso que el tema de los honeypots es de los ’90 y que casi todas las medianas y grandes empresas han hecho alguna cosa internamente. “Nosotros podemos ayudarles a escalar y automatizar todo eso para que no sea algo que estás montando manualmente y con unas capacidades limitadas”, dice el directivo.

La tecnología de CounterCraft ha llegado a la OTAN, con quien se ha realizado un proyecto de seis meses en una simulación contra potenciales ciberataques. Nos cuenta David Barroso que la organización quería probar las capacidades del producto “y la mejor manera era montarlo, establecer varios equipos de Red Team y pedirle a varias naciones de la OTAN que atacaran para ver si éramos capaces de, por un lado influenciar sus operaciones

La solución de Cyber Deception utiliza técnicas de engaño y contrainteligencia para crear entornos que imitan a los reales pero que en realidad están sembrados de trampas

para hacerles cambiar de objetivo; por otro lado, sacarles la mayor cantidad de información para poder conocer qué objetivos tienen, qué herramientas utilizan… y por último, el poder interactuar con ellos sin que lo supieran”.

La solución de Cyber Deception utiliza técnicas de engaño y contrainteligencia para crear entornos que imitan a los reales pero que en realidad están sembrados de trampas. Se trabajó con varias naciones y los resultados del proyectos permitieron demostrar que se puede conseguir información para “tomar decisiones en tiempo real cuando está ocurriendo un incidente”.

Los resultados han sido buenos por dos razones. Por un lado, se espera que el próximo año se repita la experiencia “involucrando más naciones y durante más tiempo y la idea es que podamos tener las capacidades y ofrecer ese tipo de información”. Por

otro, se han generado ideas que se han añadido al roadmap de la compañía, “como el poder pasar de ser una mera herramienta técnica que extrae información de los atacantes a intentar subir un poco el lenguaje y que se puedan tomar decisiones en base a lo que se vea, como puede ser intentar definir si un ataques es una nación o una persona sin conocimientos; determinar qué es lo que está buscando… Responder preguntas de alto nivel”.

Durante estos cinco años la compañía también ha protegido “algunas elecciones europeas”, dice Barroso explicando que como el producto es capaz de desplegar trampas por todos lados, estas se desplegaron no sólo en los colegios electorales, sino donde se recuentan los votos, en las redes internas y servidores donde se realiza todo el proceso electoral… Dice el directivo de CounterCraft que al no saber por dónde se puede venir el problema “encajamos muy bien porque podemos desplegar trampas por todos lados”.

Además de acelerar las ventas y consolidar el posicionamiento de la compañía en mercados internacionales, 2021 verá el lanzamiento de la versión 3.0 del producto.

Enlaces de interés...

- Threat Intelligence: ¿tienes lo que necesitas?, ¿necesitas lo que tienes?
- CounterCraft colabora con la OTAN con sus técnicas de cyber deception y contrainteligencia
- CounterCraft protege el teletrabajo con tres nuevos servicios
- CounterCraft cierra una ronda de financiación de 5 millones de dólares

Compartir en RRSS

STORMSHIELD

Primer cortafuegos en obtener ambas certificaciones del CCN.

Producto Cualificado y Producto Aprobado

Stormshield, filial participada al 100 % de Airbus CyberSecurity, propone soluciones de seguridad completas e innovadoras para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). www.stormshield.com/es/

“SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección”

(Carlos Manchado, Naturgy)

Texto: Rosalía Arroyo
Fotos: Ania Lewandowska

Naturgy Energy Group es una empresa española que opera en los sectores eléctrico y gasístico. Su actividad se remonta a 1841, cuando la que hoy se conoce solo como Naturgy empezó a alumbrar las calles de la ciudad de Barcelona. Previamente había instalado las farolas de gas en el centro de Madrid, y después construiría la primera fábrica de gas manufacturado de España. A lo largo de los años y hasta la actualidad se adentró en el mercado de la electricidad, se fusionó con varias empresas y cambió de nombre hasta el actual, adoptado un 27 de junio de 2018, cuando una Junta General de Accionistas acordó que Gas Natural Fenosa pasara a denominarse Naturgy Energy Group. Actualmente la compañía es una de las principales distribuidoras de gas y electricidad del

mercado de Iberia, opera en otros nueve países europeos y suma casi doce mil empleados, todo ello protegido bajo la coordinación de Carlos Manchado, CISO de Naturgy desde hace casi tres años y con experiencia en consultoras de la talla de Deloitte y Accenture.

Capacidad técnica, capacidad estratégica y capacidad de gestión son, en opinión de Carlos Manchado, las grandes cualidades que debe tener un buen CISO. Explica que un responsable de ciberseguridad debe tener capacidad de trabajar en distintas dimensiones, incluida la operativa, “y eso requiere tener un gran conocimiento técnico para para poder entender distintas problemáticas, amenazas e incidentes”. Añade que “para tomar decisiones estratégicas, y dada la naturaleza de la exposición, con un escenario de amenazas muy agresivo y dinámico, o tienes el conocimiento técnico o te asesoras muy bien”. Tener conocimientos técnicos no parece a priori una tarea fácil si tenemos en cuenta la rapidez con la que evoluciona la tecnología; al respecto dice Carlos Manchado que su trabajo “tiene tanto de profesión como de pasión” y que para desempeñar bien esta labor “no solamente vale ser disciplinado y tener conocimiento, sino que te tiene que gustar, te tiene que apasionar”.

Hablando de estrategia asegura el CISO de Naturgy que hay que tener muy claro hacia dónde quieres ir, cuál es la dirección, “aunque el escenario sea muy dinámico” tanto a nivel de ciberamenazas como regulatorio.

Planteamos si la ciberseguridad se ha convertido en una prioridad dentro de las empresas españolas, sobre todo después de todos los cambios que se han producido a raíz de la pandemia. Para Carlos Manchado “aunque no ha alcanzado la posición que por naturaleza debiera tener, sí que se piensa más en la seguridad”. Los diferentes incidentes que copan los titulares cada semana han ayudado a ello, así como desafíos como el que ha generado la COVID-19, que “ha supuesto un impulso para la transformación digital, para todas las iniciativas de movilidad y por supuesto, para el tema de ciber”, asegura Carlos Manchado añadiendo que mientras los malos han convertido la pandemia en un caldo de cultivo, “las empresas nos hemos tenido que poner a correr”, algo que se ha percibido en los consejos y en la dirección general de las empresas.

"Un servicio gestionado de seguridad es tan bueno como tú quieras hacerlo, y querer hacerlo requiere esfuerzo"

"Capacidad técnica, estratégica y de gestión son las grandes cualidades que debe tener un buen CISO"

Durante años la relación entre el CIO, o responsable de TI, y el CISO, ha sido tirante. ¿Ha cambiado esa relación? Reconoce Carlos Manchado que "sobre el papel hay un claro conflicto de interés", porque el CIO va a velar por la funcionalidad, la usabilidad y la disponibilidad de las aplicaciones, y el CISO por la ciberseguridad o la seguridad de la información de las aplicaciones en las plataformas, "y cuanto más seguro es algo, más complejo, y más difícil para los usuarios". En todo caso, y a pesar de ese conflicto de interés, parece que la relación entre ambas figuras ha mejorado "porque al final se están dando cuenta de que el escenario actual es el que es, es el que vemos en las noticias".

También hablamos con Carlos Manchado sobre la adopción del cloud. Asegura el CISO de Naturgy que "entre algunas compañías y personas hay una falsa creencia de que el cloud es seguro de por sí", independientemente de que detrás haya un gran proveedor. Lo habitual es que se ofrezcan controles de seguridad básicos y que sean los clientes de ese proveedor cloud los que tengan que completar esos controles. Esa falsa sensación de seguridad es "para mí, donde radica el problema" porque "sí que hay un tendencia al cloud, que tiene cosas buenísimas, pero todos deberíamos tener en la retina que el cloud por defecto no es seguro".

¿Cómo se está abordando el tema del IoT dentro de Naturgy?

"La hiperconectividad que nos trae IoT es impresionante", dice Carlos Manchado, añadiendo que hay

que tener en cuenta conectividades como 5G, SD-WAN… En Naturgy por el momento se están definiendo arquitecturas y marcos “para que las cosas que se hagan bien desde el principio”. Apunta este directivo que en el caso del IoT “tendrían que ser los propios fabricantes los que nos ayudan a securizar esos elementos desde el principio, porque si no, es muy difícil”.

Hablar de IoT no sólo es hablar de los dispositivos, sino de la red y la arquitectura en su conjunto, incluidas las plataformas que están al otro lado gestionando los datos, “y aunque nosotros intentemos plantear todo bien de cero, si uno de los elementos no es securizable, es bastante más complejo”. Para Carlos Manchado “es necesario una estandarización de los distintos dispositivos para que tengan cierta certificación y cumplan ciertas medidas de seguridad”, además, “los reguladores deberían establecer ciertos criterios y hacer de obligado cumplimiento algunos controles”.

Servicios y Tecnologías

“Se puede internalizar algunas partes de la ciberseguridad que son clave”, dice Carlos Manchado, pero “siempre vas a tener un servicio o varios servicios gestionados de seguridad”.

Aceptado que los servicios de seguridad gestionados se han vuelto imprescindibles para la labor de un CISO, dice el de Naturgy que requieren tener cierta calidad; “yo siempre digo que un servicio gestionado de seguridad es tan bueno como tú quieras hacerlo y querer hacerlo requiere esfuerzo, dedicación, porque lo tienes que moldear para que encaje con la cultura y la forma de proceder de tu compañía”.

Preguntamos a Carlos Manchado cuáles son, en su opinión las tecnologías imprescindibles a día de hoy. Menciona el primer lugar el EDR (Endpoint Detection and Response) “por el modus operandi de los ciberdelincuentes”; dice además que no sólo se trata de un EDR, sino que tenga un servicio por detrás “que lo opere, explote y gestione de manera adecuada”, o lo que es lo mismo un MRD (Managed Detection and Response). Por cierto, “si además de un MDR tienes un servicio de Threat Hunting, fenomenal”.

Otro elemento importante para el CISO de Naturgy es la protección de la navegación (proxy cloud, Security Gateway…), “es decir controlar muy bien dónde navegan los usuarios y saber qué traen y qué llevan esos flujos de red. Es una segunda capa que se complementa muy bien con el EDR, el saber qué está pasando”.

Si tuviese un talón en blanco, y el tiempo no fuera un problema, Carlos Manchado apostaría por… “una arquitectura SASE / Zero Trust clarísimamente”. Explica el directivo que llevamos décadas utilizando lo mismo y de la misma manera, “aunque haya habido mejoras y nuevas versiones”; está convencido de que “hay que cambiar el paradigma” y optaría por una arquitectura SASE con una gestión centralizada donde se apliquen todos los controles, desde la protección contra amenazas, fugas de información, temas de CASB… exactamente lo mismo a un ordenador corporativo de un interno que a una tablet de

"Es necesaria una estandarización de los dispositivos IoT para que tengan cierta certificación y cumplan ciertas medidas de seguridad"

un externo". SASE, asegura Carlos Manchado, "no será algo que pase de refilón, y todas las empresas iremos para allá. Así como Zero trust".

Después de un año 2020 movidito, ¿qué se espera de 2021? "Que podamos consolidar todo lo que se ha hecho de manera precipitada en 2020", dice Carlos Manchado, añadiendo que "no hay varitas mágicas para hacerlo en tan poco tiempo y que esté perfecto". it

Enlaces de interés...

- 'En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar' (Jesús Alonso Murillo, Ferrovial Servicios)
- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)
- 'No tiene sentido ver la seguridad como un gasto' (Rubén Fernández, Grupo DIA)
- 'Está demostrado que cada vez que inviertes en educación el nivel de fraude baja' (Iker Osorio, Cetelem)
- 'El Shadow IT sigue siendo un grandísimo problema hoy en día y con cloud todavía más' (Globalia)
- "Un servicio gestionado puede ser tan bueno como estés dispuesto a hacerlo" (Iván Sánchez, Sanitas)
- "La figura del CISO ha evolucionado bastante, y más que tiene que evolucionar" (Mónica de la Huerga, Sopra Steria)

Compartir en RRSS

La aniquilación del ransomware

No permitas que un ransomware paralice tu negocio.

‘2021 va a convertirse en el año de la inteligencia artificial y la automatización de procesos’

(Pedro Pablo Pérez, Telefónica Tech)

Rosalía Arroyo

Hace mucho tiempo que algunas telcos apuestan por el negocio de la ciberseguridad, “pero a futuro van a apostar prácticamente todas”, asegura Pedro Pablo Pérez, CEO Business Security Unit en Telefónica. La operadora española de telecomunicaciones lleva tiempo, desde 2003, apostando por este mercado; en 2010, coincidiendo con la creación de Telefónica Digital ya se apostó por tener ciberseguridad “no sólo en España, sino en más sitios”, y el año pasado la ciberseguridad fue uno de los pilares de la nueva Telefónica.

La evolución hacia la ciberseguridad, acelerada bajo la presidencia de José María Álvarez Pallete, ha llevado a un crecimiento sostenido de doble dígito y por encima del mercado durante los últimos cinco años, a contar con más de 1.500 profesionales en este ámbito, a realizar compras como las de Govertis o iHackLabs, o la creación de Telefónica Tech Ventures como vehículo de inversiones en ciberseguridad. Al final, el crecimiento llega “porque tenemos profesionales, porque tenemos catálogo, porque se tiene el volumen adecuado y, sobre todo, porque esto se hace de manera orgánica e inorgánica”, dice Pedro Pablo Pérez.

Intelligence MSSP

Nacida a finales de 2020, Telefónica Tech Ventures es el resultado de fusionar la actividad de Wayra, la aceleradora de la operadora, con Telefónica Innovation Ventures, el brazo inversor general. La nueva unidad nace con un portfolio de nueve compañías entre las que cabe mencionar 4iQ, una empresa creada por el fundador de Alienvault, vendida a AT&T en 2018 por 600 millones de dólares. El objetivo de Innovation Ventures en los próximos tres años es invertir en otras 15 empresas, tanto en edades tempranas como en otras fases más maduras. Con ello busca no sólo un retorno claro de la inversión en un sector en pleno crecimiento como el de la seguridad, sino estar en contacto con el ecosistema, analizando las tendencias del mercado.

"Evidentemente no somos Israel a la hora de invertir en ciberseguridad, ni España es Silicon Valley, pero hay un impulso notable desde las administraciones públicas"

Nos cuenta el directivo de Telefónica que se autodefinen es como un Intelligence MSSP (Managed Security Service Provider), un proveedor de servicios de seguridad gestionada que se mueve en cuatro ejes: Make, Buy, Partner o Invest, o lo que es lo mismo “hacerlo nosotros, invertir, hacer un partnership o comprar una empresa”. Donde se realizan más inversiones, añade, es en tecnologías que van a destacar a dos, tres o incluso cinco años; “productos que pueden ser más o menos maduros en la actualidad, pero que tienen una mayor proyección a futuro”, y menciona de manera específica el mercado de seguridad industrial o seguridad ligada a inteligencia de amenazas.

En lo que se refiere a adquisiciones, dice Pedro Pablo Pérez que se realizan “en capacidades que creemos que ya deberíamos tener, pero que, por lo que sea, no hemos sido capaces de desarrollarlas

"La adopción de la cloud, y la seguridad asociada a la misma, no va a parar de crecer"

de manera orgánica". Identificando que deberían ser más fuertes en consultoría de seguridad, se compró Govertis, "un jugador que dentro del mundo de la ciberseguridad en España es bastante relevante en consultoría".

¿Dónde se realizan los acuerdos de partnership? "En los temas que ya creemos que están suficientemente maduros y que nosotros, por mucho que invirtamos o compremos, no vamos a ser relevantes", como puede ser el mercado de firewalls, o de antivirus.

Pandemia y su impacto

La pandemia ha provocado que la digitalización se haya acelerado, lo que ha llevado a que el teletrabajo, por ejemplo, se democratice, o que determinados temas que había en el datacenter se muevan a la nube. Añade Pedro Pablo Pérez que en esta evolución la seguridad se ha convertido "en el compañero perfecto para que el teletrabajo o el movimiento hacia la nube sea tan o más seguro que el anterior modo de funcionamiento, que la ciberseguridad sea el principal compañero dentro de la transformación digital".

Por otra parte, la pandemia ha dejado en evidencia "las carencias generalizadas que había en cuanto a planes de continuidad. Es decir, ya sea dentro de lo que es la identificación, la protección, la detección, la respuesta o la recuperación, "al final necesitamos que el plan de continuidad esté en consonancia con personas, infraestructuras y procesos".

Al mismo tiempo, "las empresas se han dado cuenta que hace falta una concienciación", porque por muchos controles que pongamos, "tenemos que garantizar que la ciberseguridad llega también a las personas".

No se olvida el responsable de ciberseguridad de Telefónica Tech de la falta de profesionales de ciberseguridad. "Las empresas se han dado cuenta de que en este traspaso de capacidad de cómputo a la nube o el teletrabajo necesitaban empresas que les ayuden, y Telefónica ha estado ahí con muchísimas empresas. Prueba de ello es que este año, incluso con la complejidad que ha habido, el negocio de Cloud y Ciberseguridad ha crecido".

Al final, dice el directivo, "las organizaciones de lo que se han dado cuenta es de que tienen que ser ciber-resilientes. Es decir que la resiliencia es muy importante y que la digitalización les ayuda a ser más eficiente. Al mismo tiempo, esa digitalización sin seguridad les puede abocar a un problema bastante grave".

¿Qué demandan las empresas?

Con miles de clientes en el mercado de todo tipo y condición Telefónica Tech tiene una amplia visión de lo que está demandando el mercado. Nos cuenta Pedro Pablo Pérez que una de las tendencias más claras dentro de las empresas es la digitalización, que "está asociado a temas de trabajo en remoto y migración a la nube".

Una vez que todo está digitalizado o tienen altos componentes de digitalización, "lo que se bus-

"Tenemos recorrido para que la ciberseguridad sea una industria muy relevante en el país"

ca es la eficiencia, una eficiencia que llega de la automatización de procesos y nuevas tecnologías como puede ser la aplicación de machine learning o cualquier técnica de inteligencia artificial. En el fondo lo que buscan las empresas es una mayor productividad". Añade el directivo de Telefónica que esa mayor productividad que viene de la digitalización va a tener varias vertientes, ya sea la automatización de procesos o la aplicación de inteligencia artificial.

"Hay un punto clave, que curiosamente no es tecnología o casos de uso, sino la demanda de profesionales expertos, ya sean para la contratación o para recepción de servicios", añade Pedro Pablo Pérez. Esta falta de profesionales es uno de los puntos clave por los que, a raíz de la compra de iHackLabs, se ha anunciado, durante la celebración de los últimos Security Innovation Days, la CiberAcademy+, una academia de ciberseguridad orientada a desarrollar y potenciar el talento con una propuesta basada en la formación, entrenamiento y certificación de sus profesionales en el ámbito de la ciberseguridad.

Innovación

SASE (Security Access Service Cloud), Zero Trust, Threat Hunting, XDR… son algunas de las tecnologías o modelos de seguridad que se han puesto de moda en los últimos años. Ahora somos 'SASE Believers', ahora todo es confianza cero y la tendencia clara es la de detectar para poder responder. Las empresas españolas ¿son innovadoras a la hora de adoptar tecnologías de seguridad? Más que de empresa española, "hay que hablar de sectores", dice Pedro pablo Pérez, que coloca en la parte superior de la pirámide a bancos y aseguradoras "porque tienen un modelo de madurez altísimo"; en el otro extremo de esa pirámide lo que nos encontramos son pymes que "básicamente se meten en los temas de ciberseguridad o porque han tenido una mala experiencia o porque la regulación les empuja".

Y en medio hay un gran grupo que engloba tanto a administración pública como a grandes empresas o intereses industriales, y aquí "hay empresas que en un determinado sector pueden estar invirtiendo en ciberseguridad un 7% y otras un 1%".

Volviendo a la innovación, dice Pedro Pablo Pérez que su negocio está invirtiendo en ello; "a día de hoy somos responsables del 15% de las patentes generadas en Telefónica, que son en ciberseguri-

dad; lanzamos herramientas de desarrollo propio" y además se cuenta con seis centros de innovación en ciberseguridad. Menciona también el directivo como ejemplo de la innovación de Telefónica Tech a Deeder, la primera spinoff de un desarrollo propio de ElevenPaths, la firma de ciberseguridad de Telefónica Tech, que propone "poder cerrar contratos o hacer una transacción con validez jurídica a través de WhatsApp y de Telegram" y que "ha multiplicado su valor por tres en el último año".

"Evidentemente no somos Israel a la hora de invertir en ciberseguridad, ni España es Silicon Valley, pero hay un impulso notable de la ciberseguridad desde la parte pública y creo que hoy podemos

"De lo que se han dado cuenta las organizaciones durante la pandemia es de que tienen que ser ciber-resilientes"

estar bastante orgullosos de que las cosas se están haciendo bien, y tenemos recorrido para que la ciberseguridad sea una industria muy relevante en el país", asegura pedro Pablo Pérez.

De manera concreta Telefónica está centrando parte de su innovación en torno a OT, que no es otra cosa que la seguridad operacional asociada a la seguridad industrial. Telefónica Tech ha invertido en empresas como Nozomi Networks, un referente en este mercado, o en Alias Robotics, una compañía alavesa que ha desarrollado un antivirus inteligente para proteger los robots.

También pone foco Telefónica Tech en la seguridad cloud, porque en un mundo en el que casi todas las cargas computacionales se están moviendo a la nube "la arquitectura de seguridad tiene que ser distinta". Además, se está invirtiendo en todo lo que es la parte de identidad digital. La identidad es el

"La pandemia ha dejado en evidencia las carencias generalizadas que había en cuanto a planes de continuidad"

nuevo perímetro de seguridad "y todos los procesos que hay alrededor de la identidad digital es algo en lo que también estamos invirtiendo".

Por último, asegura el directivo, se pone foco en todo lo que es inteligencia de amenazas.

Qué nos depara 2021

De cara a 2021, la adopción de la cloud, y la seguridad asociada a la misma, "no van a parar de crecer", asegura el responsable del negocio de ciberseguridad de Telefónica Tech. Ese viaje a la nube, que se ha acelerado por la pandemia, se iba a hacer igualmente "y no hace falta una bola de cristal para verlo, sólo hace falta ver las valoraciones que tienen en Bolsa todas las empresas que se dedican a esto".

También apunta Pedro Pablo Pérez hacia el crecimiento de las amenazas en el mundo OT. A mayor conectividad, mayor exposición, dice el directivo, añadiendo que en 2021 "apostaría sin riesgo a equivocarme que el mundo de la seguridad industrial, la seguridad OT e IoT, van a estar en portada".

2021 será, además, "el año de empezar a sacar partido, ya de verdad, a todo lo que son los temas de inteligencia artificial y de automatización". Añade Pedro Pablo Pérez que 2021 va a ser el año en que las tecnologías de inteligencia artificial, las tecnologías ligadas al machine learning, incluso la propia compartición de indicadores de compromiso entre las distintas empresas, van a estar maduras; va a ser el año en el cual va a estar suficientemente madura la tecnología de inteligencia artificial, suficientemente madura la concienciación de los usuarios de que hay que automatizar los procesos y, sumado el problema de que no hay profesionales en ciberseguridad, se va a crear una tormenta perfecta para que 2021 vaya a convertirse en el año de la inteligencia artificial y la automatización de procesos".

Enlaces de interés...

- Pedro Pablo Pérez dirigirá el negocio de seguridad de Telefónica Tech
- La nueva Telefónica
- Telefónica colabora con Alias Robotics para llevar la ciberseguridad a la robótica
- Telefónica Tech Ventures canalizará su inversión en startups de seguridad de la multinacional
- Propuesta conjunta de Siemens y Telefónica en ciberseguridad industrial

Compartir en RRSS

ALSID FOR ACTIVE DIRECTORY

Fix weaknesses before hackers exploit them
Detect & respond to attacks in real-time

“Las empresas no pueden ser negligentes en la gestión de dato”

(Francisco Valencia, Secure&IT)

Rosalía Arroyo

Conciso, con las ideas claras y un tanto irreverente. Así es Francisco Valencia, CEO de Secure&IT, la empresas que fundó hace más de 10 años, “con un maletín, un portátil y un tarjetero de contactos”. Tuvo claro desde el principio que lo suyo iba a ser la ciberseguridad cuando detectó un nicho importante de “empresas que no estaban siendo atendidas”. Había oferta para la gran cuenta, para el mundo telco, las administraciones públicas, incluso las micro-pymes tenían algo, “pero las empresas medianas se las tenían que ingeniar porque no había una oferta clara para ellos”.

Por aquel entonces apenas había en el mercado empresas que ofrecieran servicios de ciberseguridad, “y durante un tiempo nos vimos solos y con un mercado por adoctrinar”, recuerda Francisco Valencia.

La situación actual es diferente porque la ciberseguridad está en los telediarios y hay una mayor preocupación, se van haciendo cosas, el mercado está intentando comoditizar la seguridad, a pesar de que “esto es un servicio que no es fácilmente comoditizable”.

Sobre el coste de la seguridad, tiene claro Francisco Valencia que de lo que se trata es de “en qué momento te encuentres cómodo con la seguridad que tienes”, y esto se puede hacer de dos formas, la empírica o haciendo un análisis de riesgos de forma que incluso se puedan comparar los riesgos de ciberseguridad con otros riesgos como los financieros, los humanos, los geopolíticos, etc.

Aunque ahora hay una mayor preocupación por la ciberseguridad, y se van haciendo cada vez más cosas, “históricamente nuestro mejor comercial ha sido el legislador”, responde Valencia cuando le preguntamos qué tipo de servicios de seguridad se demandan. Añade que “la gente le tiene más miedo a la multa que a lo que le pueda pasar”, cuando en realidad “el impacto de un ciberataque es mayor que una sanción administrativa”.

Frente a la pregunta, tristemente repetida, de “¿qué es el mínimo que tengo que hacer para cumplir la ley?”, dice Francisco Valencia que las empresas tienen que aprender a que “la ley lo que pretende es defender ciertos activos, algunos tuyos y otros de terceros, y que tú deberías preocuparte por proteger los activos entendiendo el riesgo como propio”.

"Se tiene más miedo a que un empleado robe datos que a que un tercero venga y se los lleve"

Hablar de leyes es hablar de RGPD, que tuvo un impacto importante y generó muchos proyectos de seguridad, pero ya se está enfriando el miedo y se ha vuelto a la normalidad. El impulsor ahora es “el miedo a ser atacado”, siendo el mayor el miedo a los ataques internos; “la gente tiene más miedo a que un empleado robe datos que a que un tercero venga y se los lleve”.

A nivel tecnológico explica Francisco Valencia que se ha pasado de proteger redes y sistemas, con firewall y antivirus, a la protección del dato con soluciones de criptografía, de IRM, DLP: “después de pasó a proteger al usuario” con soluciones de protección del endpoint, de MDM para los móviles, etc., “y ahora hemos tenido que trabajar en la protección de amenazas avanzadas, que nos ha dado un empujón grande”. Al mismo tiempo, “se ha tenido que avanzar hacia la protección de un entorno divergente en el que la información está distribuida”.

Este entorno divergente no es otro que el híbrido. “Todo el mundo tiene cloud, lo que pasa es que no es consciente”, dice Francisco Valencia, y añade que el reto es “cómo protejo tu información si tú mismo la estás esparciendo por un montón de sitios que son difíciles de proteger, y que además parten de la premisa de que nos han vendido que son seguros”.

"Hay un montón de servicios cloud y todas las empresas están en la nube. Y quien diga que no, miente"; dice también Francisco Valencia que se ha pasado esta fase de desconfianza, pero que hay que tener en cuenta que "el proveedor cloud se protege, no te protege, y eso es proteger la caja, no el dato. Y las empresas no pueden ser negligentes en la gestión de dato cuando se le da a un tercero del que no saben nada. No puedes pensar que tu empresa no tiene responsabilidad legal por el hecho de que te hayan subido a la nube".

Entre los proveedores cloud, dice también Francisco Valencia, hay una asignatura pendiente, que es la "interoperabilidad de nubes". Reconoce que los proveedores cloud tienen sus propios intereses de mercado, pero que estaría muy bien "que estuvieses en una nube y pudieras migrar a otra de una forma sencilla. Y eso no ocurre". No será fácil, "pero al final el mercado les terminará obligando porque las empresas sí que tienen esa necesidad". Añade que deben confiar más en los proveedores de seguridad cloud "como nosotros o empresas de nuestro color".

Para complicar aún más las cosas, se añade el mundo OT/IoT. Sobre este tema dice el CEO de Secure&IT que "todo el mundo está intentando hacer un dispositivo de IoT, se dediquen a lo que se dediquen", y que "esos dispositivos, que cuestan dos o

"La deception pone de manifiesto que ni el EDR ni el threat hunting funcionan bien"

Previsiones 2021

"2020 ha sido bastante desastroso y espero que en 2021 se ejecuten mucho proyectos que se han quedado parados porque las empresas han estado haciendo otras cosas", dice Francisco Valencia. En 2020 les ha ido muy bien a las empresas que venden cosas asociadas al teletrabajo mientras en la tele se hablaba de coronavirus y de seguridad; las amenazas han crecido este año, "por lo que es de esperar que haya más proyectos de seguridad en 2021".

Los ciberdelincuentes también han estado confinados con sus ordenadores "y creo que va a venir una campaña de ransomware complicada que no sólo te va a cifrar los datos, sino que amenazará con publicarlos". También espera el CEO de Secure&IT muchas amenazas asociadas a IoT, así como una mayor profesionalización de los ataques de ingeniería social "porque ataques como el fraude al CEO son tremendamente rentables".

De cara a 2021 Secure&IT incidirá en sus servicios de SOC. La compañía cuenta con dos centros de seguridad, uno en Madrid y otro en Arrasate (Gipuzkoa) que da servicio a un montón de empresas, muchas vascas, y ha permitido avanzar en el mercado de servicios de ciberseguridad industrial, "donde queda mucho por hacer".

Asegurando que "si hay un problema con las empresas de seguridad es la captura y retención del talento", dice Francisco Valencia que "pretendemos que Secure&Academy sea un dinamizador de talento en el mercado, lo tenga quien lo tenga, pero al menos que haya perfiles formados".

Sobre el SIEM de la compañía, "sigue siendo nuestro gran desarrollo. El haberlo hecho nosotros, y haberlo hecho a medida de los datos que recibimos, le convierte" en un producto de referencia en el mercado.

tres dólares, son un gran agujero de seguridad". Esta problemática lleva a Secure&IT a estar trabajando en una norma para recomendársela a sus clientes y "con la que pretendemos que todas las compañías que fabrican dispositivos conectados hayan pasado una prueba, una auditoría; de forma que se tenga información precisa de lo que ese dispositivo va a hacer. ¿Te atreverías a securizar un entorno IoT? "Lo que tiene que hacer quien va a ofrecer el servicio es pasar unas pruebas de homologación al producto que compra, de forma que esté testado y tenga un mínimo de seguridad". Dice además Francisco Valencia que esto es algo que el mercado va haciendo poco a poco y que "no creo que tarde mucho en regularse por el daño que esto hace a terceros".

Nuevas tendencias

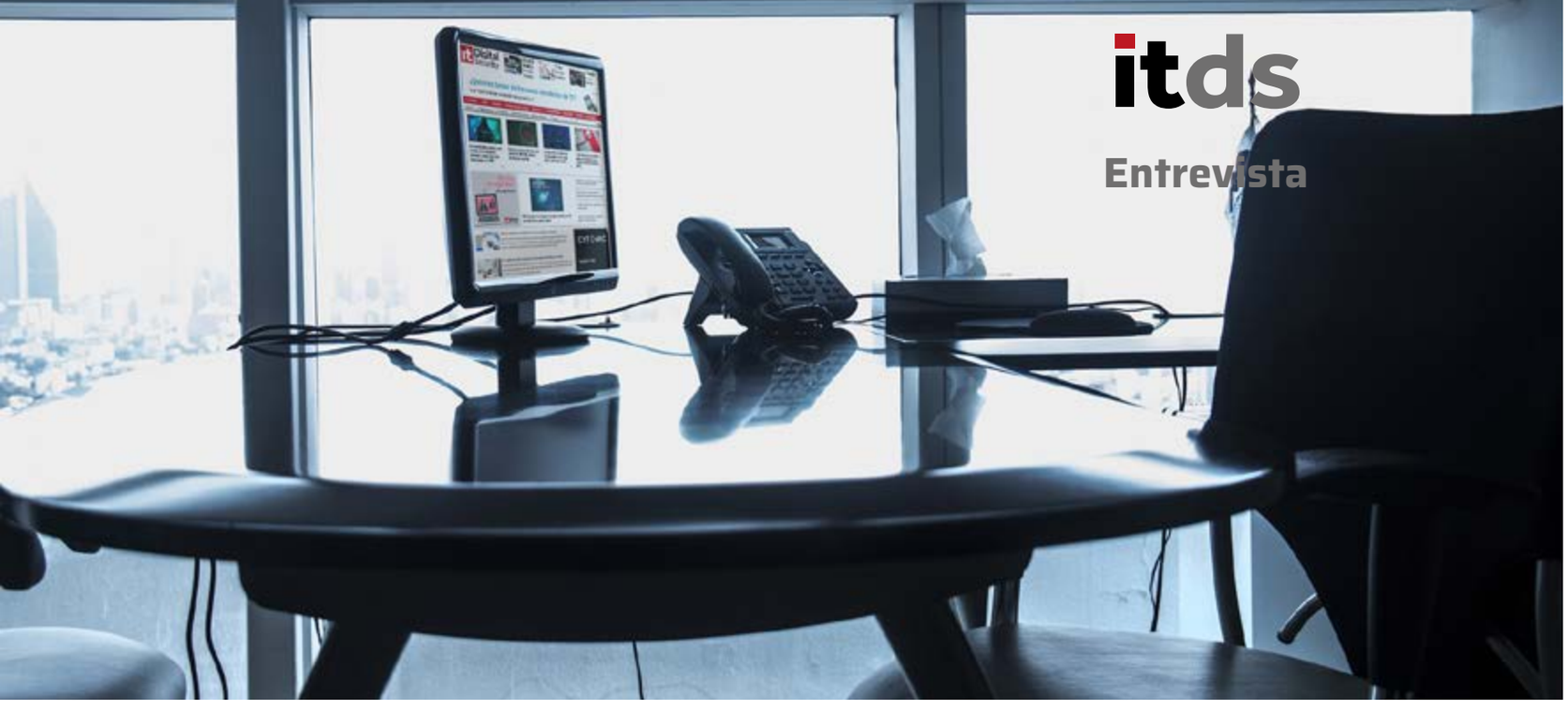
Ahora todo es Zero Trust y somos SASE Believers. ¿Cuán cerca de la realidad, del día a día de los negocios, están este tipo de tecndencias? Habla Francisco Valencia de utopía. Sobre el concepto de Zero Trust, que dice que todo es malo menos lo que sepas que es bueno, asegura que "es una utopía porque lo que sabes que es bueno puede no serlo del todo, y lo que piensas que es malo seguramente tampoco lo sea". Reconoce que "como modelo está muy bien, como meta para ir dando pasos, y como concepto de marketing es genial, pero es una utopía. Jamás alcanzaremos el Zero Trust, igual que jamás alcanzaremos la confidencialidad, son como el horizonte". Finaliza diciendo: "nunca llegarás pero cuando más cerca mejor".

Sobre el EDR (Endpoint, Detection and Response), otra de las grandes tendencias del mercado, dice que ya se están haciendo cosas y que hay muchos clientes con esta tecnología, “pero lo que no entienden es qué hay detrás del EDR, de lo que significa esa etapa de responder a un incidente”. Menciona que en ocasiones lo que hay detrás está vacío, y que también hay mucho marketing; “Si en realidad quieres la ‘R’ de respuesta tienes que ser capaz de poder parar la infección y poder actuar, y eso parte de que el antivirus pueda reconocer el malware y pararlo. Si es capaz de pararlo, el EDR vale para poco, y si no, tampoco vale para mucho, de forma que al final estamos siempre sujetos al antimalware en el puesto de trabajo”.

Hablar de Threat Hunting es distinto “porque cuando integras dentro de un motor de inteligencia único todas las amenazas de tu empresa, y no lo sujetas a un único fabricante, y vas a investigar en tiempo real todo lo que está haciendo tu organización para detectar que tienes una amenaza dentro de la red justo en este momento, que es lo que se hace con un SIEM bien montado, sí que te permite detectar la amenaza”. Añade en todo caso, que “el trabajo de ir a un cliente con sus sistemas, que nos mandan la información que realmente nos tienen que mandar, que nosotros hagamos el análisis que de verdad tenemos que hacer para identificar qué es una amenaza y qué no lo es, es un trabajo que lleva tiempo y no es automático”.

Y aunque, como nos recuerda Francisco Valencia, eso de la deception technology existe de toda la vida, que las honeypots y las honeynets no son nuevas y se utilizan desde hace tiempo en sectores como la banca y aseguradoras, también hablamos con él de esta “nueva tecnología”. Dice el directivo que la entrada de nuevas empresas “que han profesionalizado las honey” está revolucionando un poco el sector; que la deception “no está mal como una herramienta que ayuda al theat hunting” porque son capaces de detectar amenazas en tiempo real; y que en realidad lo que hace es “poner de manifiesto que ni el EDR ni el Threat hunting funcionan bien porque al final necesitas ponerle la trampa al hacker.

"Todo el mundo tiene cloud, lo que pasa es que no es consciente"



Enlaces de interés...

- Secure&IT Blog
- Encuentros ITDS. Los servicios gestionados de seguridad a examen

Sobre los cibecriminales, dice el fundador de Secure&IT que son ahora más inteligentes, que "ninguno intenta meterte un bicho si no lo ha probado antes en VirusTotal", y que las sandbox, que una vez fueron tan necesarias "han dejado de tener tanta relevancia porque es muy fácil evadirlas". Sobre esto último explica que es cuestión de mantener el proceso en ejecución el tiempo suficiente, media hora, un día, hasta que la sandbox, viendo que no hace nada, lo dé por bueno; aunque hay muchos otros trucos.

Fabricantes

"A los fabricantes les doy mucha caña", dice Francisco Valencia sin pelos en la lengua. "Sí que es verdad que hacen bien su trabajo, y que tienen buenas soluciones, pero también es verdad que los ciberdelincuentes no son tontos y cuando [los fabricantes] vienen contando magia me enfada porque el esfuerzo que nosotros hacemos como integrador también es difícil".

Menciona también cómo en empresas más pequeñas se vende el cifrado como la panacea del cumplimiento de GDPR, por ejemplo, generando así una falsa sensación de seguridad porque algunos fabricantes les venden que con eso cumplen las normativa, cuando no es verdad.

Metiendo el dedo en la llaga repito a Francisco Valencia una frase escuchada a un fabricante: "El MDR es el resultado del fracaso del canal". El contexto: la incomodidad de algunos canales por la determinación de algunos fabricantes de dar servicios de EDR, o un EDR gestionado que no es otra cosa que el MDR (Managed Detection and Response). Afirmación del fabricante: "al final hemos tenido que desarrollar el servicio porque el canal no ha sido capaz de hacerlo. El canal sigue sin aportar valor".

El CEO de Secure&IT responde con honestidad: "Estoy lamentablemente de acuerdo con ellos. El problema es que no existe un adecuado canal de ciberseguridad en España. Los canales que hay son informáticos. Quien ha vendido tradicionalmente el antivirus ha sido el canal informático, y cuando se le mete la capa de EDR y de MDR, ¿quién la sigue vendiendo?, el canal informático. Y en este canal aún no hay conciencia de seguridad gestionada". Añade que, para empresas como la suya, el que los fabricantes se hagan cargo de dar el servicio de seguridad sí que hace daño, "pero reconozco su parte de razón". Finaliza diciendo que tanto el mercado como los fabricantes tienen que darse cuenta de que "la informática y la seguridad son cosas distintas".

Todo lo que necesita para asegurar su nube.

Simplifique su seguridad en la nube con Trend Micro Cloud One™, la plataforma de servicios de seguridad para desarrolladores líder en el mundo.

Cloud One™
Cloud Security simplificada

La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

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...

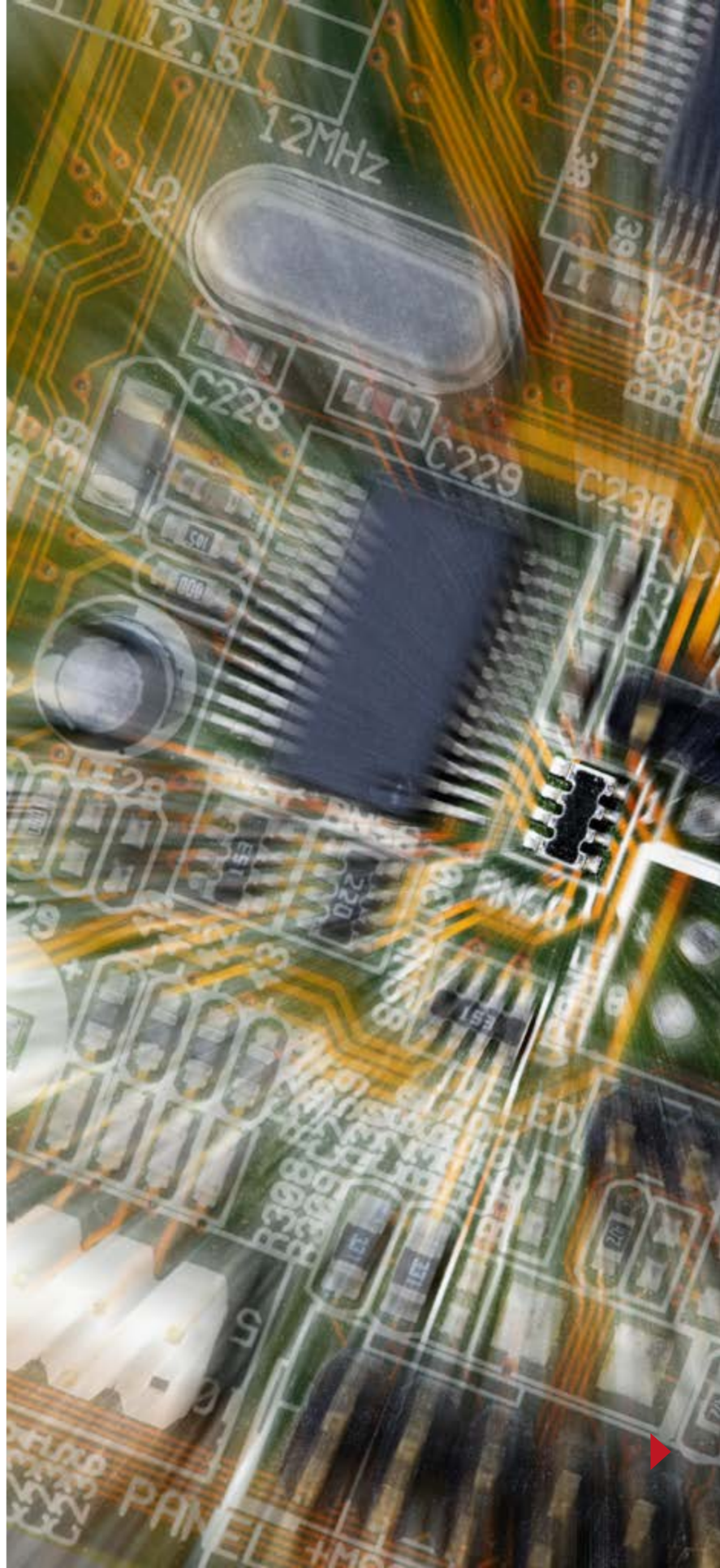
En los Encuentros IT Trends que celebramos en diciembre del pasado año para evaluar los planes adoptados y los futuros, expertos de Veeam Software, f5 Networks, Micro Focus, VMware, One Identity, ESET, Check Point, y Entrust, nos dejaron las pistas para construir unas estrategias de TI fuertes, consolidadas, 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

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.

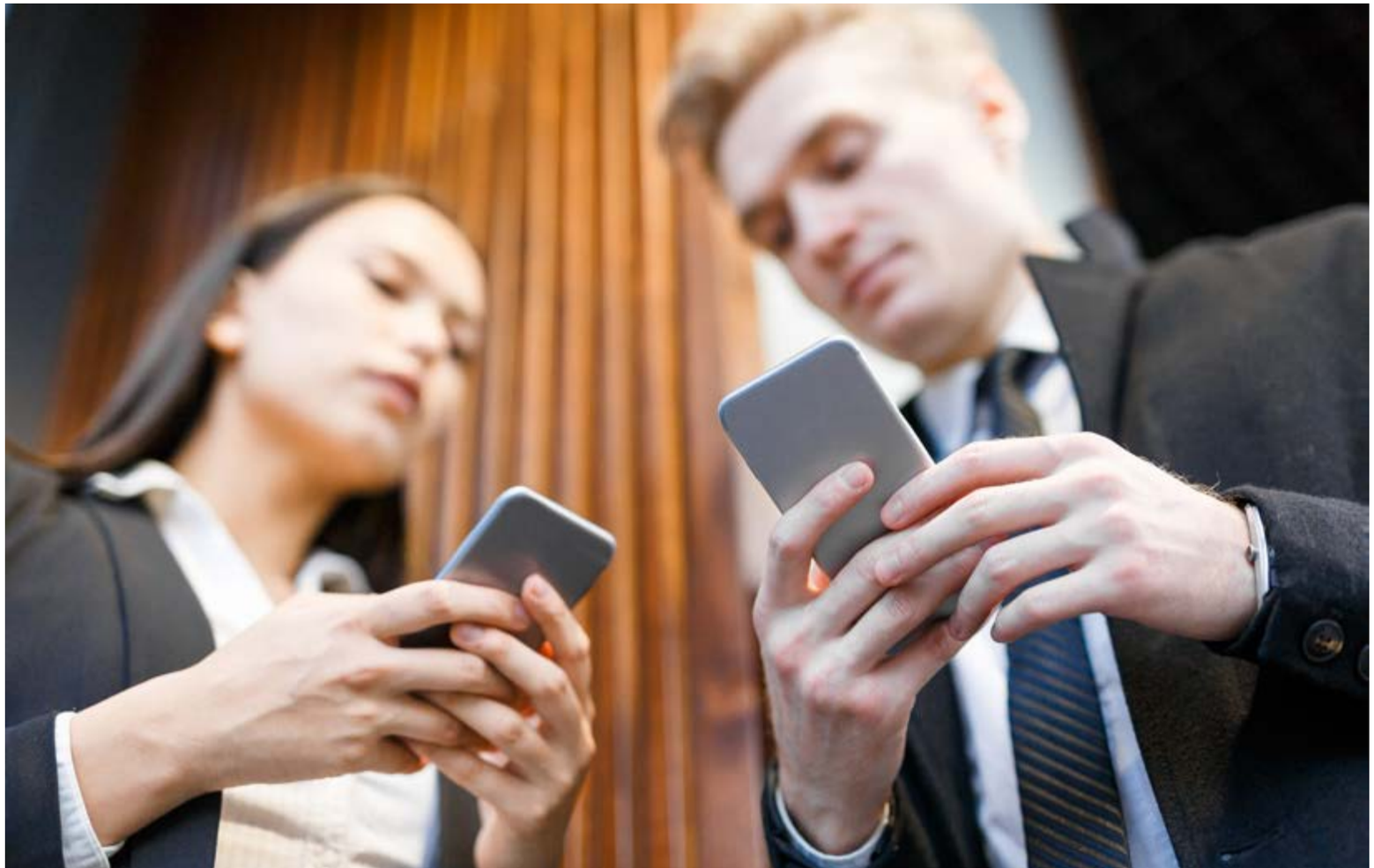
Estos proveedores están evolucionando sus técnicas para proporcionar chips más avanzados, mejor fabricados y más rentables, que encontrarán aplicaciones en muchas industrias, desde la computación perimetral a las redes móviles, los dispositivos IoT o los smartphones, campos donde estas tecnologías tienen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

it TRENDS

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”.

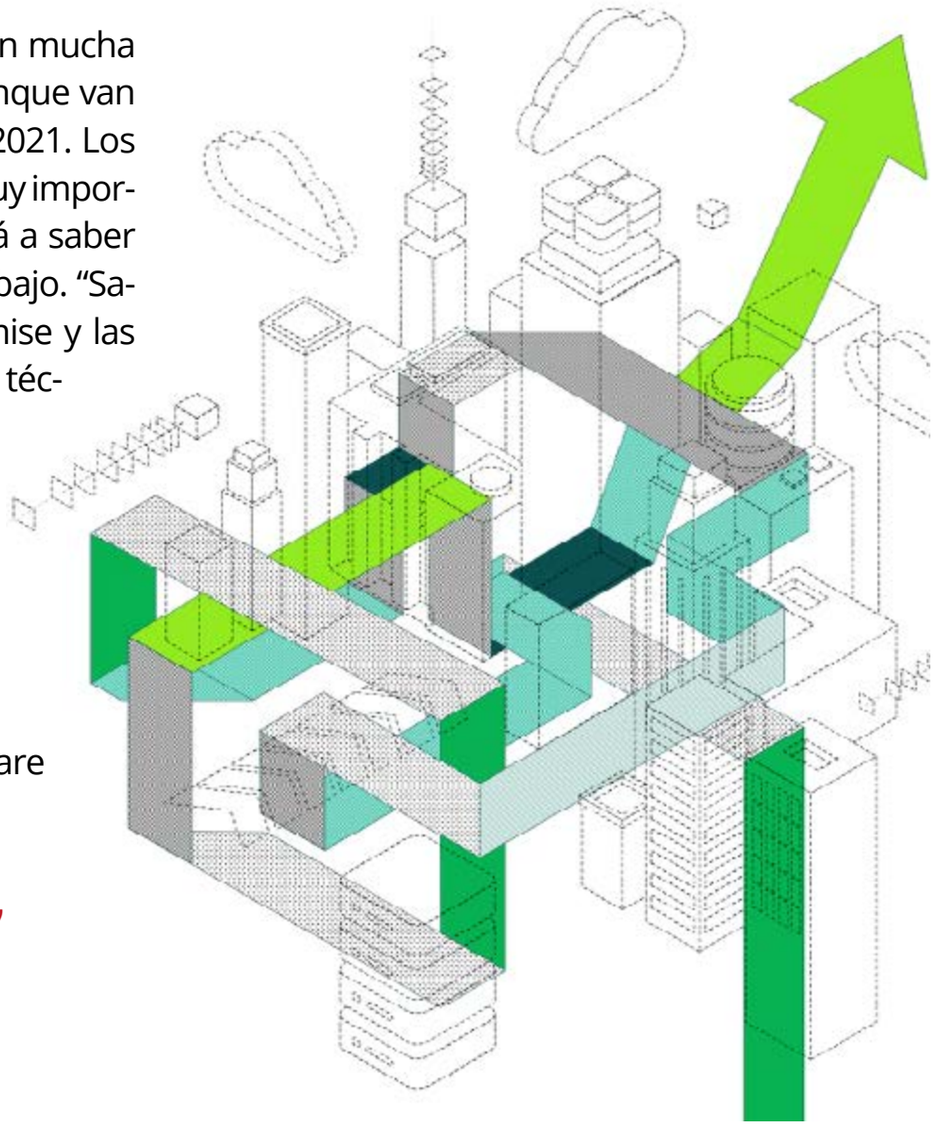
En opinión de este experto de Veeam, “cada vez se van a desplegar menos datos en la nube sin tener claro el plan de contingencia de todos los datos y el reto será añadir dinámicas de protección del dato a las cosas que te llevas a la cloud”.

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.

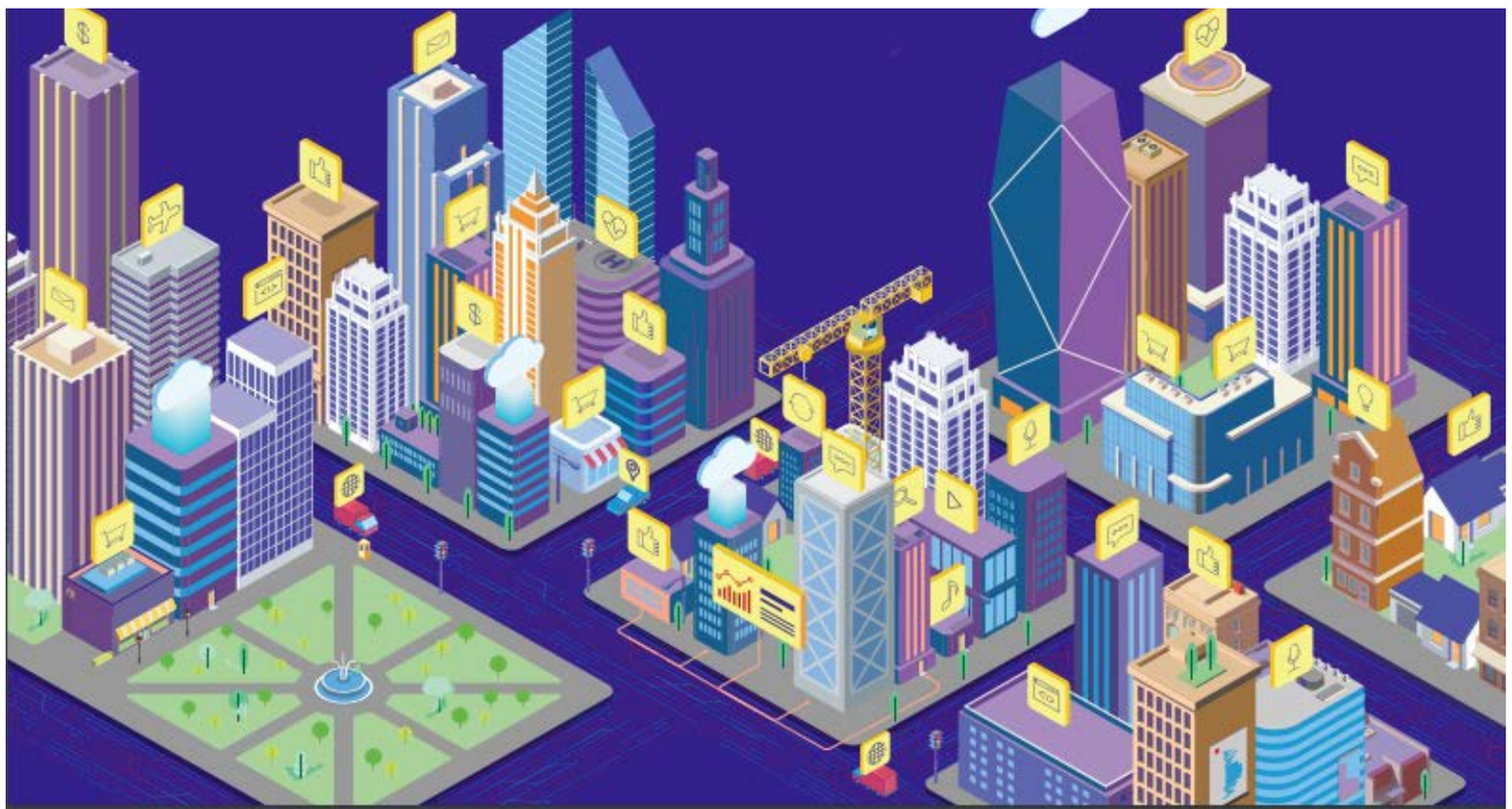
El directivo resaltó también que un 75% de las empresas que tienen medidas avanzadas de autenticación y ciberseguridad seguirán

JUAN RODRÍGUEZ, DIRECTOR GENERAL, F5 NETWORKS

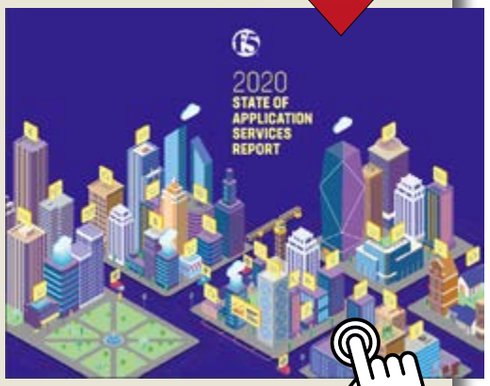
“Va a haber una gran inversión en empresas que den valor de extremo a extremo”

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.

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

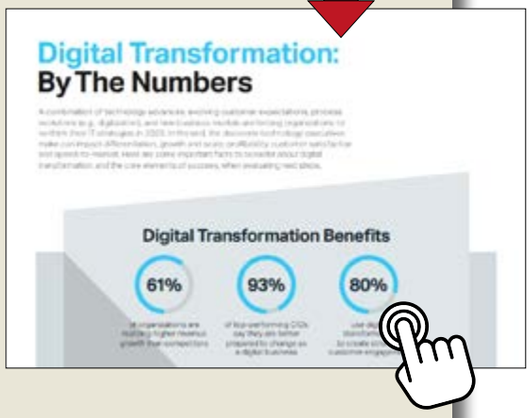
LUIS COLINO, DIRECTOR PREVENTA, MICRO FOCUS

“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.

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”. ■

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”. ■

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

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". ■

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.

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

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-

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. ■

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. ■

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

it TRENDS

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

Adrien Pujol,
Product Marketing Manager de Fastly EMEA

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 heredadas 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

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 heredadas no pueden almacenar en caché las

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

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 heredadas) 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 cloud edge soporta microservicios permitiendo a las empresas definir decisiones de enrutamiento basándose en el contenido, a la vez que proporciona una convergencia y una recuperación por error 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 flash.

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 heredada, 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 heredadas 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 sist 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, se perciben ciertos sacrificios entre el rendimiento y la seguridad. Sin embargo, las modernas CDN a menudo protección avanzada WAF, API, bot y DDoS con una latencia mínima para una mejor experiencia de compra. Limitar la velocidad de transmisión también ayuda a proteger el coste y la resiliencia de las API. Además, con la mayoría de las CDN la seguridad se consigue enviando el tráfico a través de una red segura, a diferencia de las CDN heredadas, 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. ■

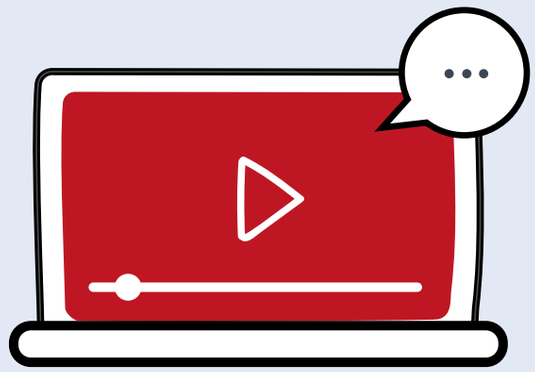
Aplicaciones,
¿cómo desarrollo y entrego mi mejor software?

Porque las aplicaciones son hoy -más que nunca- la cara del negocio y estamos en la era del DevSecOps... ¿cómo creo mi mejor software y lo pongo a disposición de mis usuarios? Únete a esta sesión online y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlas en producción. ¡Reserva ahora tu sitio!

REGISTRO

Ya vivo en la nube, ¿y ahora qué?
Mejores prácticas para desenvolverse en entornos híbridos

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



#ITWEBINARS

“Zero Trust y SASE ponen en valor las soluciones de gestión de identidades privilegiadas”

(Carlos Ferro, Thycotic)

Hace unas semanas lanzaba Verizon su informe anual sobre brechas de seguridad, el primero que incorpora una sección dedicada expresamente a la gestión de accesos privilegiados, o PAM (Privileged Access Management), con un dato que pone en evidencia la importancia de tener controlados estos perfiles: el 53% de todas las brechas de seguridad investigadas se produjeron por un uso indebido de las cuentas privilegiadas.

El negocio de PAM no es nuevo. Hace tiempo que varias empresas trabajan en un mercado que hasta hace poco no estaba maduro. Hay dos hitos que desencadenan esta madurez, explica Carlos Ferro, Vice President, SEEMEA & Asia de Thycotic. Por un lado, “se hace una anatomía de lo que son las brechas de seguridad y se identifica que las cuentas privilegiadas, o ciertas cuentas que son críticas en los entornos empresariales, aparecen prácticamente en todos los ataques”. Es cuando el mercado empieza a madurar “en el tipo de soluciones que busca para resolver esta problemática” y se empiezan a desplegar las soluciones PAM.

Pero no sólo maduran los clientes, sino los propios fabricantes. En 1996 aparece Thycotic, que en 2016, el mismo año que realiza su primera adquisición, decide expandirse internacionalmente. Hasta el día de hoy Thycotic ha sumado 6,2 millones de dólares de inversión en dos rondas de financiación y acumula tres adquisiciones: Arellia y Cyber Algorithms en febrero y noviembre de 2016 respectivamente, y Onion ID en junio de este año y con la que no sólo ha añadido tres nuevos productos a su oferta, sino reforzado su posicionamiento para proporcionar soluciones PAM para entornos IaaS, SaaS y bases de datos, un mercado actualmente desatendido por la mayoría de los proveedores de

Impacto de Zero Trust y SASE

¿Cómo impactan tendencias como Zero Trust y SASE en la propuesta de Thycotic?

“Ponen en valor las soluciones de gestión de identidades privilegiadas”, asegura Carlos Ferro, explicando que cuando uno empieza a pensar en Zero Trust y SASE y define su estrategia entendiendo estos dos modelos, “la realidad es que hace que muchas de las identidades que históricamente se trataban como identidades estándar pasan a ser identidades privilegiadas; no porque haya un privilegio, sino por una criticidad que ahora tiene esa cuenta”.

"El futuro de la compañía es seguir desarrollando nuevas opciones que nos permitan acompañar a los clientes en lo que es nuestra especialidad: las identidades privilegiadas"

PAM. En 2020 Thycotic es uno de los líderes del mercado, reconocida por consultoras como Gartner o Forrester.

Según Carlos Ferro, hay factores que están acelerando la adopción de este tipo de soluciones, como es la adopción del cloud, “que hace que muchos de los entornos que están muy controlados ahora pasan a controlarse de una forma diferente”. Haciendo referencia a las identidades que no están asociadas a las personas pero que gestionan información crítica, dice también el directivo que la relación entre las identidades y la información ha variado y que estas situaciones “han acelerado los procesos de madurez del mercado de PAM”. Si hace tres años se calculaba que el 70% de las empresas necesitaban una solución de gestión de accesos privilegiados, hoy un 60% requiere complementar la solución de PAM que tienen o adquirir una nueva, dice Ferro, añadiendo que para 2022 “el 75% tendrá ya una solución implantada, lo que significa que habrá un nivel de crecimiento, de adquisición y de despliegue de este tipo de soluciones aún mayor en el mercado”.

Mercado Español

Dice Carlos Ferro que el mercado español sigue un poco la tendencia del mercado europeo. Thycotic desembarca en nuestro país a finales de 2018 “y

"La ventaja principal de Thycotic es nuestra capacidad de integración y de poner a disposición de los clientes una cantidad de funcionalidades muy rápidamente"

COVID19 IMPULSA LA INVERSIÓN EN CIBERSEGURIDAD, PERO NO DE SOLUCIONES PIONERAS

CLICAR PARA VER EL VÍDEO

estamos duplicando nuestra facturación", con previsiones de crecer más de tres dígitos en 2020.

La pandemia, que como se ha dicho infinidad de veces, ha acelerado muchos procesos de transformación digital, también ha sido un disparador del mercado de gestión de identidades privilegiadas. El teletrabajo, apunta Carlos Ferro, ha disparado "la criticidad de asegurar la gestión de las identidades", pero a veces nos olvidamos de que el teletrabajo no sólo está asociado al empleado que trabaja desde casa, sino que "también impacta en los proveedores, los contratistas, las consultoras que están trabajando ahora en remoto y que también tienen acceso a la información". La gran mayoría de los responsables de ciberseguridad, tanto de España como de Europa, "habían pensado en ello en mayor o menor medida, pero la pandemia lo ha acelerado".

En España "se sigue trabajando con Ingecom", dice Carlos Ferro cuando le preguntamos por el canal mayorista. Se trabaja además con resellers, integradores de sistemas y proveedores de servicios "porque queremos llegar al mercado con las diferentes posibilidades que se requieren para poder cubrir los diferentes segmentos".

Gestión de identidades, ¿un mercado saturado?

El de gestión de identidades sin que éstas sean privilegiadas es un mercado en el que si bien no se puede hablar de saturación, hay ya unos cuantos fabricantes bien asentados. Es además un mercado que se ha ido consolidando y para el que los proveedores de cloud desarrollan herramientas específicas que permiten a sus clientes controlar quién accede a sus servicios casi sin coste. Lejos de inquietarle, Carlos Ferro ve la situación como algo que "ayuda a madurar el mercado".

Recuerda el directivo que alrededor de un concepto emergente suelen aparecer nuevas compañías y que hace dos años se produjeron movimien-

tos de consolidación en este mercado. Cierto, 2018 fue movidito en el mercado PAM: en septiembre de 2018 Bomgar compró BeyondTrust; en julio de 2018 Bomgar compró Avectro; en agosto de 2018 Thoma Bravo se convirtió en el mayor accionista de Centrify; en marzo de 2018 CyberArk adquirió Vaultive; en febrero de 2018 Bomgar compró Lieberman Software; y en enero de 2018 OneIdentity se hizo con Balabit.

Todos estos movimientos no hacen sino "hacer visible la problemática", dice el directivo, añadiendo: "No nos preocupa competir porque tenemos tecnología que es puntera en el mercado". Menciona Carlos Ferro que el valor de sus soluciones no sólo está en la herramienta per sé, sino "en la capacidad de integrar esta herramienta con el entorno del cliente para maximizar la inversión. Si le dices al cliente que compró una herramienta que no la puedes integrar o es compleja de integrar… esto termina siendo un stopper para esta evolución", dice Carlos ferro añadiendo que la ventaja principal de Thycotic "es nuestra capacidad de integración y de poner a disposición de los clientes una cantidad de funcionalidades muy rápidamente".

COVID-19 e inversiones en seguridad

En medio de las crecientes ciberamenazas y riesgos generados por la crisis de COVID19 Thycotic realizó una encuesta con el objetivo de saber cómo ha influido la pandemia, qué factores influyen más a la hora de tomar la decisión de invertir en medidas ciberseguridad o cuáles son los principales obstáculos a la hora de invertir en ciberseguridad. Entre otras cosas, el estudio "Cyber Security Team`s Guide to Technology Decision Making" desveló que el 58% de los encuestados considera que COVID19 provocará un aumento de su presupuesto en seguridad en el próximo años, porcentaje que en España llega al 70%; que el temor a las sanciones sigue siendo el principal motivo de inversión en ciberseguridad o que sólo un 36% de las empresas apuestas por soluciones pioneras.

En medio de las crecientes ciberamenazas y riesgos generados por la crisis de COVID19, los encuestados indican que las juntas directivas están tomando conciencia y aumentando el presupuesto para ciberseguridad, y la abrumadora mayoría, el 91%, está de acuerdo en que la junta los apoya adecuadamente con inversiones. Casi 3 de cada 5 creen que en el próximo año financiero tendrán más presupuesto de seguridad debido a COVID-19.

Evolución de producto

La evolución del producto está girando en dos áreas, explica Carlos Ferro. Por un lado la compañía trabaja para cubrir todos los segmentos del mercado, tanto en la gran cuenta como en la mediana y pequeña empresa, "porque la problemática es la misma: gente que tiene acceso a información crítica y queremos asegurarla", de forma que se han desarrollado soluciones que permiten apoyar a esas compañías con las necesidades que ellos tienen.

"La relación entre las identidades y la información ha variado y esto ha acelerado los procesos de madurez del mercado de PAM"

"A veces nos olvidamos de que el teletrabajo no sólo está asociado al empleado que trabaja desde casa, sino que también impacta en los proveedores, los contratistas, las consultoras que están trabajando ahora en remoto"

Por otro lado, "hemos desarrollado un producto puramente nativo cloud que apoya a todas las compañías que se están moviendo en este proceso de transformación digital", independientemente del momento en el que se encuentren. La idea, explica Carlos Ferro, es que puedan contar con una solución PAM en un modelo on-premise, o en un modelo híbrido.

"Y por último, una de las evoluciones que hemos desarrollado en los últimos dos años, y que se consolidó sobre todo en el 2020, son las soluciones de gobierno de estas identidades". Explica el directivo de Thycotic que hay un área dentro de las cuentas privilegiadas que son las identidades privilegiadas no asociadas a personas, los sistemas que interactúan entre sí. En Thycotic "hemos reforzado nuestro portfolio de gestión de identidades privilegiadas con soluciones de gobierno que nos permiten abarcar y gestionar el ciclo de vida completo". Añade Ferro que este año se han adquirido unas compañías "que también nos permiten reforzar los accesos remotos".

Además de reforzar los entornos privilegiados y los entornos de acceso remoto, hace poco la compañía también ha reforzado la integración de dos mundos que parecían complejos, "que es la integración del mundo Linux y Unix con el mundo Microsoft, unificando plataformas que históricamente se solían gestionar de forma separada".

El futuro de la compañía, asegura Carlos Ferro, es seguir desarrollando nuevas opciones que permitan acompañar a los clientes en lo que es nuestra especialidad: las identidades privilegiadas.

Las identidades no son sólo humanas. Las aplicaciones acceden a información y recursos empresariales; hay un mundo de identidades no humanas,

de Apis, del IoT, de procesos… ¿cómo está gestionando todo esto Thycotic? Responde Carlos Ferro que ya está contemplado, que se cuenta con soluciones específicas para DevOps, un área de crecimiento dentro de la compañía, así como soluciones para entornos de infraestructuras críticas, IoT y OT.

Respecto a DevOps la compañía acaba de lanzar la última versión de DevOps Secrets Vault, una solución que ayuda a proteger máquinas, aplicaciones y bases de datos en entornos de DevOps. Entre las ventajas de DevOps Secrets Vault pueden mencionarse nuevo soporte de credenciales privilegiadas dinámicas para bases de datos, la capacidad de proporcionar máquinas y aplicaciones recién creadas con acceso único a credenciales privilegiadas guardadas y una nueva integración con Azure DevOps.

Otra novedad en cuanto a lanzamientos tiene que ver con Secret Server, cuya última versión ayuda a controlar la superficie de ataque de la cuenta privilegiada con más facilidad gracias a una serie de nuevas capacidades que reducen el número de pasos para administrar todo tipo de privilegios, protegiendo al administrador, al servicio, a la aplicación y a las cuentas raíz del ciberataque.

De cara a 2021 el foco es “seguir acompañando a nuestros clientes en su movimiento a la cloud, que es una de las grandes tendencias; las cuentas de servicios, que son las cuentas no asociadas a personas, como DevOps y OT”.

Enlaces de interés…

- Accesos privilegiados, clave para asegurar las infraestructuras críticas
- Thycotic refuerza su oferta con la compra de Onion ID
- Thycotic creció un 25% en el segundo trimestre

Compartir en RRSS

it User
TECH & BUSINESS

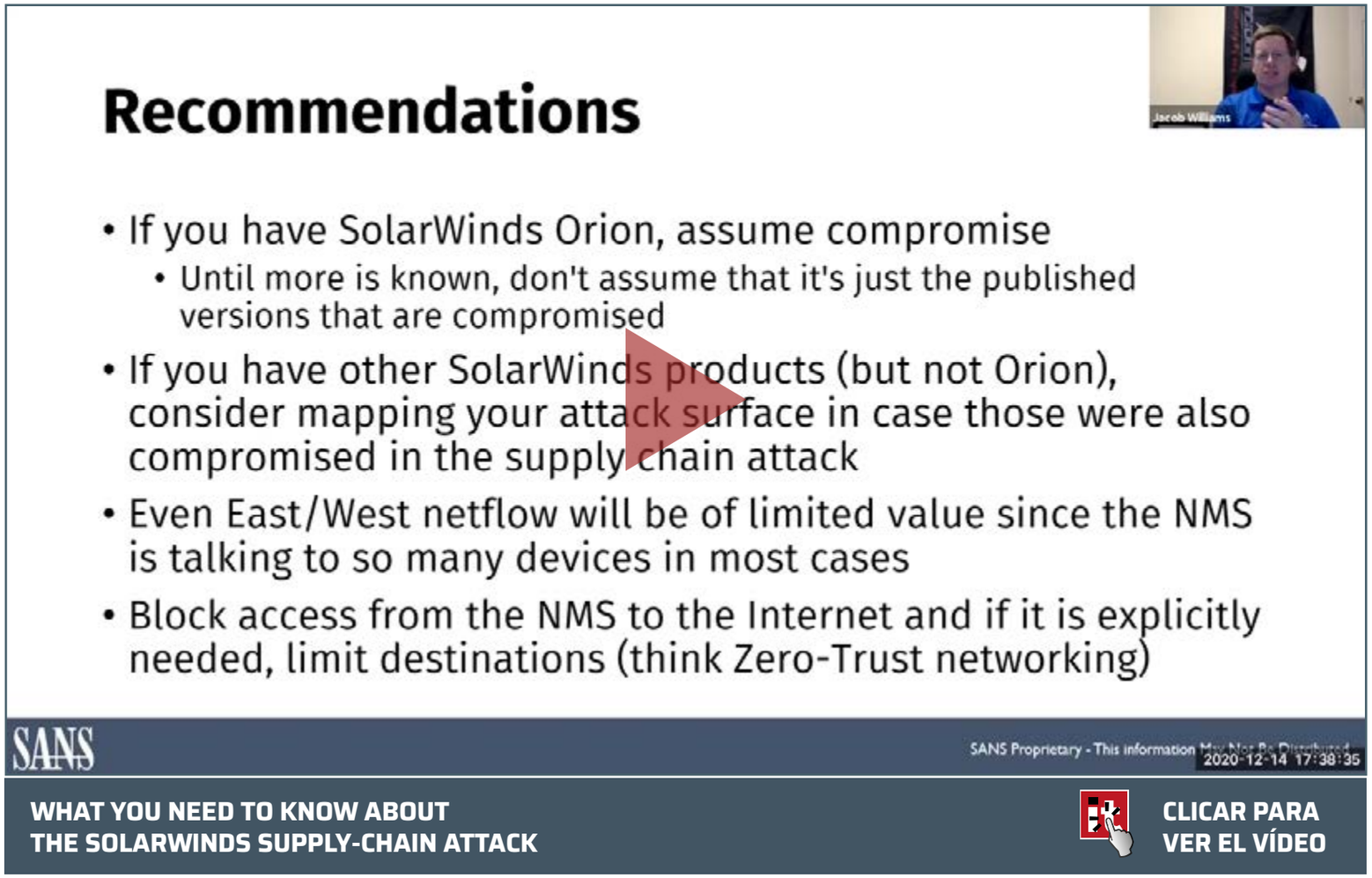
Cada mes en la revista, cada día en la web.

El ataque a SolarWinds pone en jaque a medio mundo

El ciberataque a SolarWinds, que algunos ya han bautizado como SunBurts Hack o Solorigate y sobre el que se dice que es el peor de la última década, el mayor perpetrado contra Estados Unidos, quedará en la memoria, en las páginas de la historia, incluso es de los que impulsan la conciencia de ciberseguridad, y las ventas. La historia comienza a hacerse pública a primeros de diciembre, cuando FireEye anuncia un ciberataque contra su red, pero en realidad comienza muchos meses atrás, comienza en noviembre de 2019, cuando se desarrolla un malware que acabará dentro de organismos gubernamentales y algunas de las empresas de TI más relevantes.

Un ataque a la cadena de suministro es el que ocurre cuando alguien se infiltra en tus sistemas a través de un socio comercial o un proveedor que tiene acceso a tus datos y sistemas. Y este es el tipo de ataque que ha impactado contra SolarWinds y muchos de sus clientes. Fue el pasado 8 de diciembre cuando FireEye revelaba que había sido víctima de un ciberataque, de un APT (amenaza persistente avanzada) llevada a cabo por un estado-nación estado cuyo resultado había sido el robo de herramientas utilizadas por el Red Team de la compañía y que se pueden utilizar para montar ciberataques por todo el mundo. Apenas unos días después se supo que SolarWinds, una empresa que desarrolla software que ayuda a administrar redes, sistemas e infraestructura TI, había sido hackeada y que uno de sus productos, la plataforma Orion, utilizada entre otros muchos por FireEye, podría ser el centro de una de las brechas de seguridad más importantes de la última década, no sólo por la cantidad de posibles víctimas, sino porque muchas son agencias gubernamentales estadounidenses, como la Agencia Nuclear de Estados Unidos.

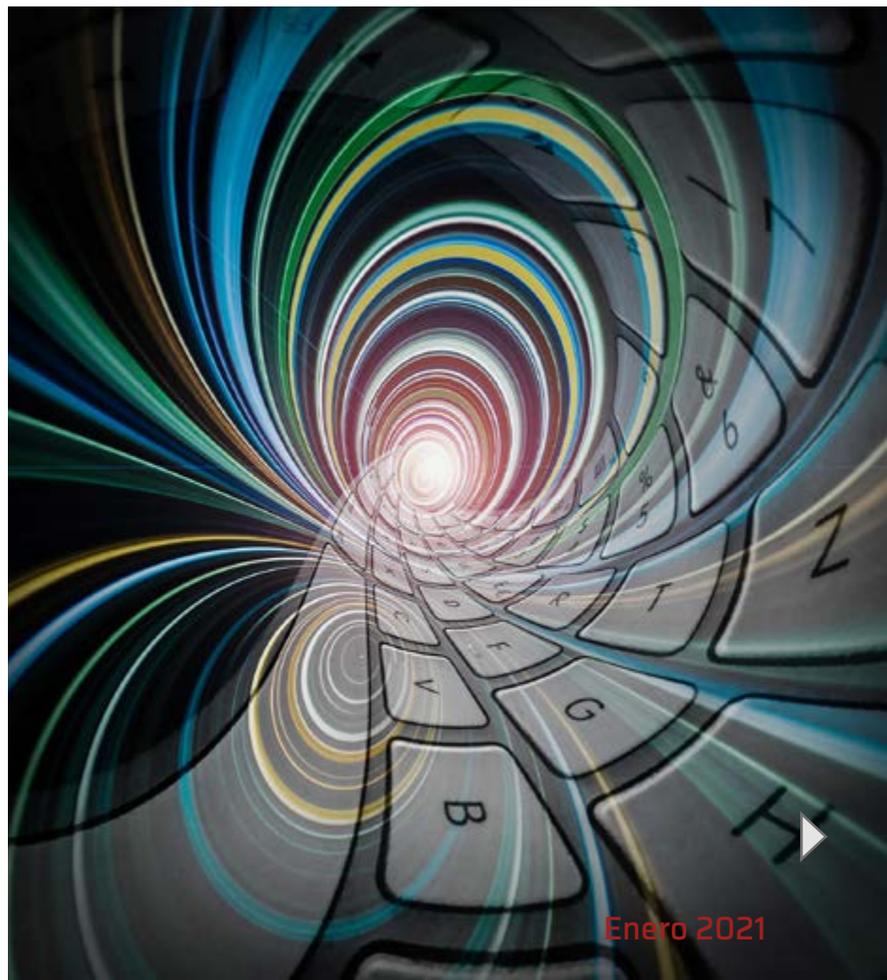
El producto más popular de SolarWinds es Orion, un sistema de gestión de redes (NMS – Network Management Systems) muy atractivo para los cibercriminales por varias razones. La primera es que este tipo de sistemas deben ser capaces de comunicarse con todos los dispositivos que gestionan y monitorizan; en segundo lugar, muchos de estos sistemas están configurados para monitorizar eventos y responder a ellos. Según explican desde el SANS Institute, “incluso cuando los NMS son de ‘solo monitorización’, las credenciales utilizadas siguen ofreciendo algún nivel de acceso al atacante”, que no sólo puede utilizarlas para monitorizar el sistema, sino para moverse lateralmente a los sistemas de destino.



SolarWinds tiene uno de los sistemas de gestión de red más utilizados del mercado. La compañía suma más de 300.000 clientes, incluidas 425 empresas de la lista Fortune 500 y parte del gobierno federal de Estados Unidos.

El malware se implementó como parte de una actualización de los propios servidores de SolarWinds y se firmó digitalmente mediante un certificado digital válido con su nombre. Y esto es precisamente uno de los aspectos a destacar de este ataque: la vulnerabilidad inicial no existía, sino que está en el proceso de creación de software para SolarWinds. Como parte del ataque, los ciberdelincuentes obtuvieron acceso al sistema de compilación SolarWinds Orion y agregaron una puerta trasera al archivo DLL legítimo de SolarWinds.Orion.Core.BusinessLayer.dll. Esta DLL luego se distribuyó a los clientes de SolarWinds a través de una plata-

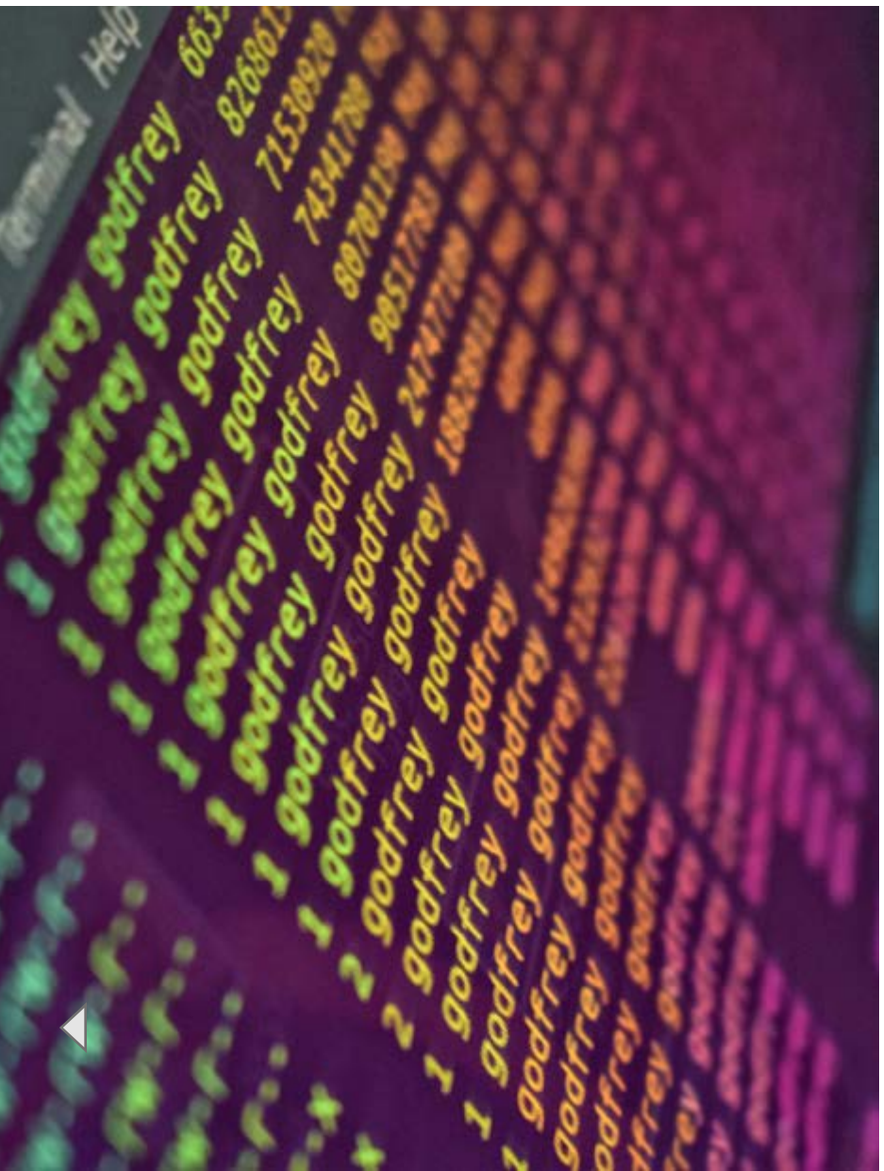
SolarWinds tiene uno de los sistemas de gestión de red más utilizados del mercado. La compañía suma más de 300.000 clientes, incluidas 425 empresas de la lista Fortune 500



Cronología

- **8 Diciembre.** FireEye informa que ha sufrido un ciberataque en su red procedente de un estado nación que ha resultado del robo de las herramientas de prueba de penetración Red Team de la empresa.
- **11 Diciembre.** Durante la investigación de su brecha de seguridad FireEye descubre que las actualizaciones de SolarWinds Orion habían sido corrompidas y utilizadas por los ciberdelincuentes.
- **12 Diciembre.** Desde FireEye se informa a Kevin Thompson, CEO de SolarWinds, de que Orion contiene una vulnerabilidad y está detrás del ciberataque sufrido.
- **13 Diciembre.** SolarWinds emite un aviso de seguridad que describe el ataque a la plataforma Orion y las medidas defensivas asociadas al tiempo que FireEye cuenta que un ciberatacante ha aprovechado la cadena de suministro de SolarWinds para comprometer a múltiples víctimas globales y la CISA (Cybersecurity and Infrastructure Security Agency) emite la directiva de emergencia 21-01, que ordena a las agencias federales apagar SolarWinds Orion debido a una importante amenaza de seguridad.
- **14 Diciembre.** SolarWinds informa de la brecha de seguridad a la SEC (Securities and Exchange Commission) mientras sus acciones caen 20 dólares.
- **15 Diciembre.** Conocido que entre las víctimas del ciberataque se encuentran el Departamento de Seguridad Nacional o el del Tesoro, varios senadores de Estados Unidos piden al FBI y a la CISA que investiguen el impacto del ciberataque a SolarWinds en las agencias gubernamentales
- **16 Diciembre.** Aunque se confirma que el software SolarWinds MSP no se ha visto afectado en el ataque se eliminan todos los certificados digitales y se pide a los clientes que reinicien sus sesiones. Mientras se cuestiona que Thoma Bravo y Silver Lake Partners, dos conocidas firmas de inversión, estén vendiendo algunas acciones de SolarWinds, el New York Time publica que “Es difícil exagerar la magnitud de esta violación de la seguridad nacional”.
- **17 Diciembre.** Microsoft informa que más de 40 de sus clientes se han visto afectados por el fallo de seguridad de SolarWinds. Se hace público que los ciberdelincuentes han accedido a la Agencia Nuclear de Estados Unidos.
- **19 Diciembre.** Aún sin pruebas, Mike Pompeo, Secretario de Estados de Estados Unidos, acusa a Rusia de estás detrás de la brecha de SolarWinds.
- **21 Diciembre.** The Wall Street Journal identifica al menos 24 empresas afectadas por el ciberataque a SolarWinds. Salen a relucir nombres como Intel, Nvidia, Deloitte, Cisco o la Universidad de Kent.
- **22 Diciembre.** Según publica Associated Press docenas de cuentas de correo electrónico del Departamento del Tesoro se vieron comprometidas debido a que los ciberdelincuentes irrumpieren en los sistemas utilizados por los funcionarios de más alto rango del departamento.
- **24 de Diciembre.** En respuesta al malware SUPERNOVA SolarWinds lanza nuevas actualizaciones para todas las versiones soportadas de la plataforma SolarWinds Orion, así como un parche para las versiones no soportadas.
- **30 Diciembre 2020.** CISA publica un comunicado por el que todas las agencias federales que operan versiones de SolarWinds Orion deben utilizar al menos la versión 2020.2.1HF2 de la plataforma.

Las versiones de actualización de Orion 2019.4 a 2020.2.1, lanzadas entre marzo de 2020 y junio de 2020, se contaminaron con malware



SOLARWINDS HACK: MICROSOFT'S SMITH

CLICAR PARA VER EL VÍDEO

forma automática que se utiliza para lanzar nuevas actualizaciones de software.

La empresa de software dijo que las versiones de actualización de Orion 2019.4 a 2020.2.1, lanzadas entre marzo de 2020 y junio de 2020, se contaminaron con malware. FireEye nombró a este malware SunBurst y publicó un informe técnico junto con las reglas de detección en GitHub. Microsoft nombró al malware Solorigate y agregó reglas de detección a su antivirus Defender.

El malware se carga mediante el programa SolarWinds.BusinessLayerHost.exe. Una vez cargado, se conectará al servidor de comando y control remoto para recibir instrucciones y ejecutar tareas en el equipo infectado. Las tareas pueden ser cualquier cosa, desde dar acceso remoto a los actores de la amenaza, a descargar e instalar más malware o robar datos.

Información publicada apunta a que los ciberdelincuentes ya habrían realizado pruebas del método

Los ciberdelincuentes ya habrían realizado pruebas del método de distribución del malware en octubre de 2019

de distribución en octubre de 2019, “cinco meses antes de que los archivos informados anteriormente se enviaran a las víctimas a través de los servidores de actualización de software de la empresa. Sin embargo, los archivos de octubre no tenían una puerta trasera incorporada”. Que primero probaran si funcionaba y sería detectado indica, según los expertos, que los creadores son disciplinados.

Cinco meses después del ensayo, los ciberdelincuentes agregaron nuevos archivos maliciosos a los servidores de actualización de SolarWinds que se distribuyeron e instalaron en las redes de las agencias del gobierno federal y otros clientes. Estos nuevos archivos instalaron una puerta trasera en las redes de las víctimas que permitieron a los ciberdelincuentes acceder directamente a ellos. Una vez dentro de una red infectada, los atacantes podrían haber utilizado el software SolarWinds para conocer la estructura de la red o alterar la configuración de los sistemas de red. Pero también habrían podido violar otros sistemas en la red o descargar nuevos archivos maliciosos directamente a esos sistemas.

Todos los expertos apuntan a que este ataque es “verdaderamente sofisticado”, y esto se refiere tanto al desarrollo como a los propios equipos operativos. Mientras que los equipos de desarrollo implementaron contramedidas anti-análisis, los equipos operativos parecen haber utilizado una infraestructura específica para cada víctima.

Sobre los actores de la amenaza, tanto SolarWinds como FireEye atribuyen el ataque a “actores de un estado-nación”, pero no han nombrado

SUPERNOVA, el segundo malware

Al analizar el ataque a la cadena de suministro de SolarWinds Orion, los investigadores de seguridad descubrieron otra puerta trasera, probablemente procedente de un actor de amenazas diferente. El malware, un webshell bautizado como SUPERNOVA es una variante troyana de una biblioteca .NET legítima (app_web_logoimagehandler.ashx.b6031896.dll) presente en SolarWinds Orion, modificado para permitirle eludir los mecanismos de defensa automatizados

No se cree que este malware esté relacionado con el ataque a la cadena de suministro SolarWinds.Orion.Core.BusinessLayer.dll. Sin embargo, sí indica que la plataforma SolarWinds Orion se usó en dos ataques diferentes, y posiblemente por grupos diferentes, para distribuir malware.

La semana pasada, SolarWinds publicó un aviso de actualización que aconseja a todos los clientes de Orion Platform actualizar a las últimas versiones para estar protegidos no solo de la vulnerabilidad SUNBURST sino también del malware SUPERNOVA.

un país directamente. A pesar de no tener pruebas, el secretario, Mike Pompeo, ha acusado a Rusia de estás detrás del ataque mientras que la embajada rusa en Estados Unidos emitía un comunicado a través de Facebook en el que se decía que “las actividades maliciosas en el espacio de la información contradicen los principios de la política exterior rusa, los intereses nacionales y nuestra comprensión de las relaciones interestatales”, añadiendo que “Rusia no realiza operaciones ofensivas en el ciber dominio”.

¿Por qué un estado nación? Habitualmente los ciberdelincuentes se centran en obtener beneficios económicos a corto plazo. Usan técnicas como ransomware para extorsionar a sus víctimas, robar información financiera y recolectar recursos informáticos para actividades como enviar correos

Se atribuye el ataque a un estado-nación, y aunque muchos apuntan a Rusia, esto último no se ha podido demostrar

electrónicos no deseados o extraer criptomonedas. Los ciberdelincuentes explotan vulnerabilidades de seguridad conocidas que, si las víctimas hubieran sido más exhaustivas en su seguridad, podrían haberse evitado.

Por otra parte, los ciberdelincuentes asociados a gobiernos nacionales tienen motivos completa-

mente diferentes. Buscan acceso a largo plazo a la infraestructura crítica, recopilan inteligencia y desarrollan los medios para inhabilitar ciertas industrias. También roban propiedad intelectual, especialmente propiedad intelectual que es costosa de desarrollar en campos como alta tecnología, medicina, defensa y agricultura.

La gran cantidad de esfuerzo para infiltrarse en una de las empresas víctimas de SunBurst también es una señal reveladora de que no se trataba de un simple ataque criminal. Por ejemplo, una empresa como FireEye es un objetivo inherentemente malo para un atacante criminal; tiene menos de 4.000 empleados, pero su seguridad informática está a la altura de las principales empresas financieras y de defensa del mundo.

UNC2452, Dark Halo o CozyBear

Mientras FireEye atribuye este ataque a un actor de amenazas desconocido que rastrea bajo el nombre de UNC2452, la firma Volexity apunta a Dark Halo, a quien sigue desde hace unos años y que habría estado involucrado en tres incidentes separados. En el primero Volexity encontró múltiples herramientas, puertas traseras e implantes de malware que habrían permitido al atacante pasar desapercibido durante varios años. Dark Halo regresó por segunda vez explotando una vulnerabilidad en el Panel de control de Microsoft Exchange de la organización; cerca del final de este incidente, Volexity observó al actor de amenazas utilizando una técnica novedosa para evitar la autenticación multifactor (MFA) de Duo para acceder al buzón de un usuario a través del servicio Outlook Web App (OWA) de la organización. El tercer incidente identificado por Volexity relacionado con Dark Halo es el relacionado con SolarWinds Orion este año.

Explica FireEye que las principales motivaciones de UNC2452 son probablemente el espionaje mediante la filtración de datos. Asegura la compañía que por el momento el actor no ha descubierto ningún indicador de extorsión o delito financiero, y añade que la campaña descubierta parece haber comenzado en la primavera de 2020 y actualmente está en curso. “La campaña es obra de un actor altamente calificado y la operación se llevó a cabo con una seguridad operativa significativa”, dice la firma de seguridad, añadiendo que los ataques que se han llevado a cabo como parte de esta campaña comparten ciertos elementos comunes: Uso de actualizaciones maliciosas de SolarWinds: inserción de código malicioso en actualizaciones de software legítimas para el software Orion que permiten al atacante acceder de forma remota al entorno de la víctima; Huella de malware ligera: uso de malware limitado para cumplir la misión y evitar la detección; Priorización del sigilo: hacer todo lo posible para observar y combinar con la actividad normal de la red; Alto OPSEC: Realización de reconocimientos con paciencia, cubriendo constantemente sus pistas y utilizando herramientas difíciles de atribuir.

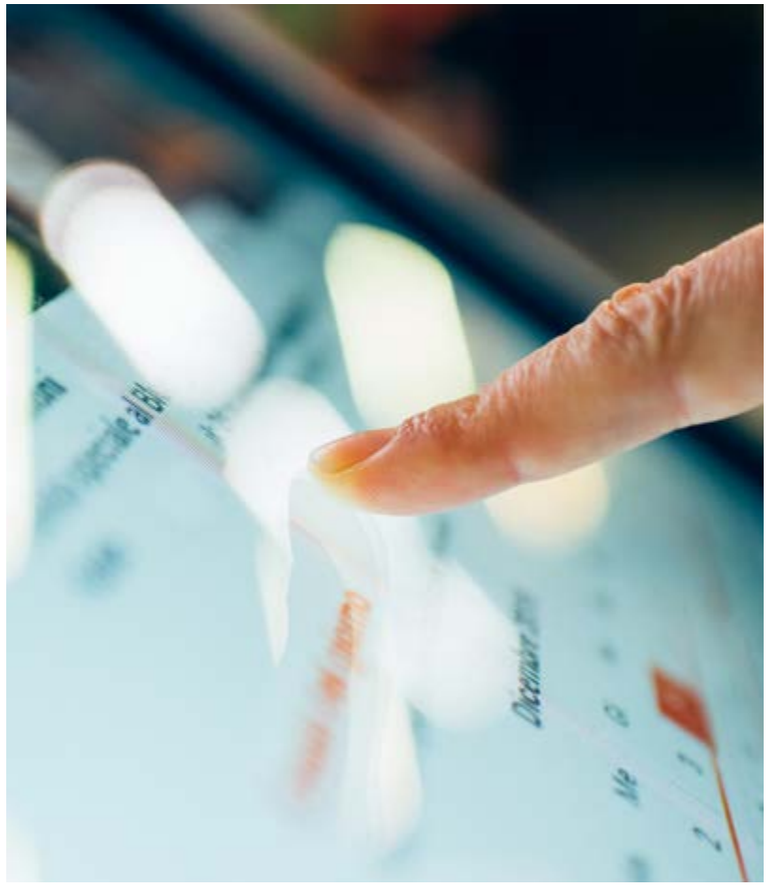
Otros apuntan al grupo APT29, o CozyBear, como el responsable de atacar los Departamentos de Comercio y Finanzas de Estados Unidos gracias al malware distribuido dentro del software Orion de SolarWinds. Se trata de un grupo que anteriormente ha sido acusado de atacar los sistemas de correo electrónico en el Departamento de Estado y la Casa Blanca durante la administración del presidente Barack Obama. También fue nombrado por las agencias de inteligencia de Estados Unidos como uno de los grupos que se infiltró en los sistemas de correo electrónico del Comité Nacional Demócrata en 2015.

Víctimas

Lo primero que hay que aclarar es que no todos los clientes de SolarWinds son vulnerables a SunBurst. Solo los usuarios de la plataforma de software Orion se ven afectados, y solo aquellos que cargaron la actualización de marzo. SolarWinds ha comunicado que el número de clientes que tienen esta actualización es de unos 18.000, muchos objetivos a piratear incluso para un gran grupo de estado-nación con muchos recursos.

Los expertos aseguran que lo más probable es que los ciberdelincuentes fueran primero tras los objetivos de alto valor, como las agencias del gobierno federal de Estados Unidos y las grandes empresas, y avanzarán en la lista. Aun así, se debe asumir que se es una víctima y tomar todas las medidas necesarias para limitar la exposición.

Las víctimas de SunBurst incluyen entidades gubernamentales, de consultoría, tecnología, salud, telecomunicaciones y petróleo y gas en América del Norte, Europa, Asia y Medio Oriente. Por el momento no está claro cuántas agencias están afectadas o qué información podría haberse robado. Según los expertos, el malware es extremadamente potente y permite un amplio alcance en los sistemas afectados.



La firma Volexity apunta a Dark Halo, a quien sigue desde hace unos años y que habría estado involucrado en tres incidentes separados, como el grupo autor del ataque contra SolarWinds

Según informes de Reuters, The Washington Post y The Wall Street Journal, el malware afectó a los departamentos de Seguridad Nacional, Estado, Comercio y Tesoro de Estados Unidos, así como a los Institutos Nacionales de Salud. El 17 de diciembre se informó además de que los programas nucleares administrados por el Departamento de Energía de Estados Unidos y la Administración Nacional de Seguridad Nuclear también fueron atacados.

CISA agregó gobiernos locales y estatales a la lista de víctimas. Según el sitio web de CISA, que ha agregado gobiernos locales y estatales a la lista de víctimas, la agencia está “rastreando un incidente cibernético significativo que afecta las redes empresariales en los gobiernos federal, estatal y local, así como en las entidades de infraestructura crítica y otras organizaciones del sector privado”.

Microsoft también ha identificado y notificado a más de 40 de sus clientes afectados por este ataque, pero no ha revelado sus nombres. Desde la compañía afirman que el 80% de las víctimas son estadounidenses y el 44% pertenecen al sector de las tecnologías de la información. Fuera de Estados Unidos se han identificado víctimas en siete países adicionales: “Canadá y México en América del

Norte; Bélgica, España y el Reino Unido en Europa; e Israel y los Emiratos Árabes Unidos en el Medio Oriente". Se advierte que el recuento de víctimas seguramente seguirá creciendo.

La firma de seguridad Kaspersky ha descubierto que alrededor de 100 de sus clientes descargaron la actualización del software Orion troyanizado, que luego contactó con los servidores de comando y control.

Además de FireEye, la compañía con la que se destapó esta crisis, VMWare y Microsoft son algunas de las que han confirmado que instalaron actualizaciones maliciosas de Orion en sus redes internas. Otras víctimas son Cisco, Intel, Nvidia, VMware o Belkin.

En todo caso, si su empresas de una posible víctima, debería activar su plan de respuesta a incidentes. Los primeros pasos: retirar el software y comenzar a buscar cualquier Indicación de Compromiso (IoC). En todo caso, quizá sea el momento de poner en práctica tareas de threat hunting, porque no hay que olvidarse de que se trata de hackers sofisticados que pueden ocultar muy bien los signos de un ataque y que podrían llevar meses dentro de todas estas organizaciones de alta seguridad sin ser descubiertos.

Incluso si su organización no está ejecutando SolarWinds, es posible que no esté fuera de peligro, ya que si un tercero o proveedor que utiliza su organización ejecuta este software, es posible que esté infectado. Y si tienen acceso a su red o sistemas, su organización podría ser atacada a través de esa conexión.

No todos los clientes de SolarWinds son vulnerables a SunBurst. Solo los usuarios de la plataforma Orion, y solo aquellos que cargaron la actualización de marzo

Cómo protegerse

Desde que se reveló el ciberataque, las empresas de seguridad han estado agregando los binarios maliciosos de puerta trasera Sunburst a sus detecciones. Si bien inicialmente Microsoft ya estaba detectando y alertando a los clientes sobre binarios de SolarWinds maliciosos, no los estaba poniendo en cuarentena por temor a que pudiera afectar los servicios de administración de red de una organización, pero a partir del 16 de diciembre Microsoft Defender comenzó a poner en cuarentena los binarios detectados incluso si el proceso se está ejecutando.

También se trabaja de forma común para crear un Kill Switch que detenga el proceso, de forma que cuando los binarios maliciosos intenten ponerse en

contacto con los servidores de comando y control, realizarán una resolución de DNS para obtener la dirección IP. Si esta dirección IP es parte de ciertos rangos de IP, incluidos los que son propiedad de Microsoft, la puerta trasera terminará e impedirá que se ejecute nuevamente.

En todo caso, si bien este Kill Switch desactivará las implementaciones de puertas traseras de Sunburst que conectan los servidores de comando y control, FireEye ha declarado que los actores de amenazas pueden haber implementado otras puertas traseras.

Por cierto que cuando una organización está investigando, monitorizando y auditando a sus proveedores de manera adecuada, tendrá muchas más posibilidades de detener o detectar ataques provenientes de terceros. Si aún no lo ha hecho, debe implementar un programa de gestión de riesgos de terceros que cubra el acceso de proveedores de cualquier tipo. Incluso si su organización tiene un programa, es un buen momento para una revisión y mejora.

Alcance

"A moment of reckoning: the need for a strong and global cybersecurity response", con este título fir-

Fuente. FireEeye

maba Brad Smith, presidente de Microsoft, un post en el que asegura, entre otras muchas cosas, que se necesitan medidas más contundentes “para responsabilizar a los estados-nación por los ciberataques”. Explica el directivo cómo en los últimos años empresas como Microsoft, Google, Facebook y Twitter han actuado y hablado directa y públicamente al responder a los ciberataques de los estados nacionales y cómo una coalición de más de 145 empresas de tecnología global se han adherido al Acuerdo Tecnológico de Ciberseguridad, que promueve un comportamiento responsable para promover la paz y la seguridad online, incluida la oposición a los ciberataques contra civiles y empresas inocentes.

Asegurando que los próximos meses presentarán una prueba crítica y que esta tipo de ataques reflejan “no solo la última tecnología aplicada al espionaje tradicional, sino también un riesgo imprudente y generalizado de la cadena de suministro digital y de nuestras instituciones económicas, cívicas y políticas más importantes”, planteaba Brad Smith que durante cuatro siglos, los pueblos del mundo han confiado en los gobiernos para protegerlos de las amenazas extranjeras, “pero la tecnología digital ha creado un mundo en el que los gobiernos no pueden actuar de forma eficaz por sí solos. La defensa de la democracia requiere que los gobiernos y las empresas de tecnología trabajen juntos de formas nuevas e importantes: compartir información, fortalecer las defensas y responder a los ataques. Al dejar atrás 2020, el nuevo año brinda una nueva oportunidad para avanzar en todos estos frentes”.

Quizá sea el momento de poner en práctica tareas de threat hunting, porque no hay que olvidar que los ciberdelincuentes podrían llevar meses dentro de sus víctimas sin ser descubiertos

Hay que tener en cuenta que el verdadero impacto de este evento puede tardar años en descubrirse y es posible que algunas cosas nunca se descubran. Por otra parte, los ataques a la cadena de suministro continuarán, entre otras cosas porque son extremadamente difíciles de proteger, lo que destaca la necesidad de que la seguridad se considere parte del proceso de selección de proveedores.

Enlaces de interés...

- SolarWinds Security Advisory
- Talos. SolarWinds supply chain attack
- SUNBURST Backdoor

Compartir en RRSS

it Reseller
TECH&CONSULTING

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

SANTIAGO MORAL RUBIO

EXPERTO EN CIBERSEGURIDAD

Actualmente es el VP de Innovación y Ciberseguridad de OpenSpring y codirector y uno de los fundadores del Instituto DCNC Sciences de la Universidad Rey Juan Carlos, así como Presidente de la Asociación HITEC en España y miembro de su sede norteamericana. Moral Rubio, quien ocupó el cargo de CISO del Grupo BBVA entre 2000 y 2018, también ha participado en la creación del Grupo de Ciberseguridad del Laboratorio de Informática e Inteligencia Artificial (CSAIL) del MIT.

Ransomware... Zero Trust, Mitre ATT&CK y CIS

La industria del Ransomware: **discreción, mucha paciencia y buenos sistemas de información. Puro oportunismo.**

¿Cómo se aproximan NIST, Mitre y CIS a las estrategias de defensa contra el Ransomware?
Dentro de la serie de artículos dedicados a Zero Trust (NIST), Mitre ATT&CK y CIS Community Defense Model, os traemos en esta ocasión una reflexión sobre las estrategias de defensa contra el Ransomware y el Principio #2 de Zero Trust (NIST 800-207).

Para empezar es fundamental entender cómo funciona la Industria del Ransomware. Es un modelo industrial puramente oportunista.

Describamos un ejemplo real. En el Centro de Operaciones de un grupo de delincuencia tecnológica organizada tienen motores de búsqueda lanzados en Internet. Permanentemente están buscando puertos RDPs abiertos con usuario y contraseña y VPNs públicas también con usuario y contraseña.

Cuando los atacantes encuentran un RDP activo en el perímetro de una empresa, que no usa doble factor de autenticación, suele tratarse de una actividad no autorizada que ha montado alguien del personal técnico de la empresa. Esto lo hacen los técnicos y programadores para poder realizar labores de administración (habitualmente nocturnas o de fin de semana) desde su domicilio sin tener que ir a la empresa. Es fácil identificar que es una entrada no autorizada porque se encuentran activos en puertos muy altos no habituales del RDP.

Lo normal es que estos RDPs no tengan políticas de bloqueo por intentos reiterados de contraseñas incorrectas. El ataque es trivial. Se prueban contraseñas hasta que se encuentra la buena. Es cuestión de paciencia y de no ser muy intenso en la pruebas.

La instantaneidad del Ransomware hace que la posibilidad de evitarlo a base de detección temprana es prácticamente nula

En el caso de las VPNs el procedimiento es distinto. Cuando se encuentran VPNs públicas con usuario y contraseña (sin doble factor), lo normal es que sean “legales” dentro de la empresa y que tengan política de bloqueo por contraseñas erróneas repetidas. En este caso ¿qué hace la delincuencia organizada?

- **Se compran las claves en la DarkWeb**

Un volumen muy alto de nuestras contraseñas está disponible en la DarkWeb. Si alguien no se lo cree, puede contratar a algunas de las magníficas

Hay semanas (o meses) en el que los PCs y los Servidores de cada compañía están vulnerables porque es imposible técnicamente tenerlos siempre a la última versión

empresas españolas que hay en este ámbito un servicio para que les “busquen” las contraseñas de su empresa. Las caras de los que por primera vez descubren lo que se vende en la DarkWeb es un poema difícil de olvidar.

La probabilidad de encontrar en la DarkWeb el usuario y la contraseña de alguno de los cientos o miles de usuarios activos en cada una de las VPNs que tienen las empresas es altísima. Insisto para los descreídos en que lo prueben.

▪ Ya están dentro…

Una vez que el grupo organizado atacante ya tiene el usuario y la contraseña del RDP o de la VPN sólo les queda entrar y observar.

Lo hacen con mucha discreción y en los husos horarios de la empresa atacada.

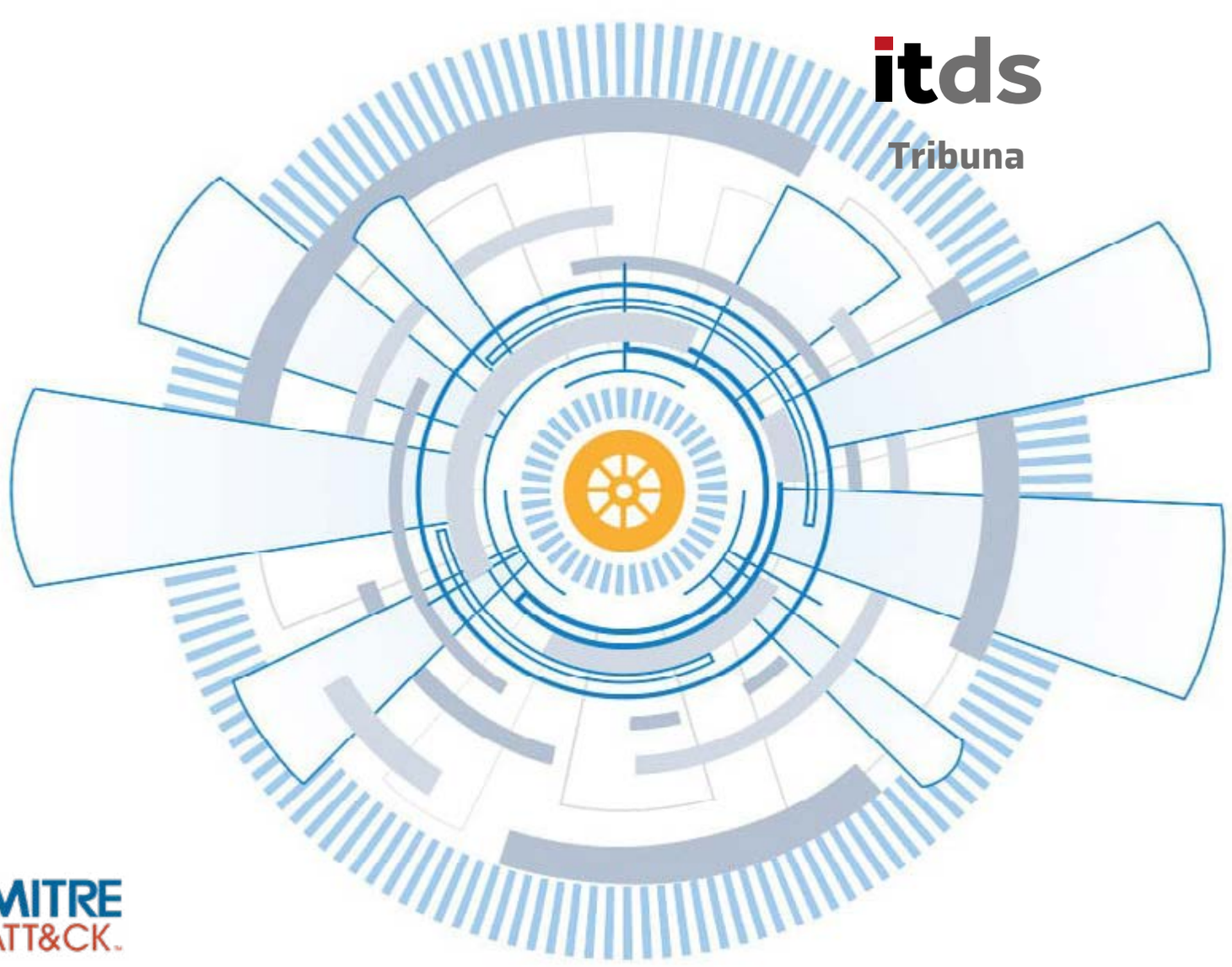
¿Ahora se dedicarán a saltar de máquina en máquina? No. Se lo pondrían muy fácil a los SIEM y los SOC.

Observan la propia máquina a la que han llegado (en el caso del RPD), ven si tiene antivirus, EDR, observan la frecuencia de parcheo de cada producto que tiene instalado el PC. Navegan por Internet (en el caso de VPN) para ver la secuencia de salto de direccionamiento IP.

Observan durante semanas para identificar las mejores condiciones para lanzar el cifrado de todos los PCs y servidores de la red. Son capaces de saber, observando la cadencia de parcheo interno, cuál es el mejor momento para lanzar el cifrado masivo de toda la instalación y qué herramientas específicas deben utilizar. Llegado este punto los atacantes no tienen ninguna duda en que van a poder cifrar TODA la instalación. Sólo deben esperar el momento adecuado. Es un negocio donde la paciencia tiene una recompensa altísima.

▪ Los SIEM y los SOC sirven de muy poco

Todos estos pasos los hacen de manera que las probabilidades de ser descubierto por un SIEM y el SOC que lo opera sean mínimas. Estos delin-



Si impides la visibilidad en "plano" entre las máquinas de la empresa, le pones bastante más difícil al atacante organizar un Ransomware dentro de tu empresa

cuentes son profesionales cuyo valor y experiencia radica en no ser descubiertos.
Una vez que ya saben cuándo y cómo hacer el ataque para maximizar el número de PCs y Servidores afectados (y así maximizar su beneficio), lo lanzan de manera fulminante. No hay forma de pararlo una vez iniciado. Lo han hecho justo cuando las medidas de seguridad y los parches están desactualizados.
Es muy difícil explicar a los Comités de Dirección que las inversiones más importantes que se han hecho los últimos años, en sistemas carísimos de SIEM y contratos multianuales suculentos en los SOCs, no valen para nada (para muy poco) para evitar el Ransomware.
La instantaneidad del Ransomware hace que la posibilidad de evitarlo a base de detección temprana es prácticamente nula.
Si en ese momento tu estrategia de copia de seguridad está basada en modelos activo-activo, y no tienes una tercera copia fría off-line… estás en mitad de la tormenta perfecta!!!
¿Qué dice Mitre ATT&CK y el CIS Community Defense Model al respecto?

Que lo fundamental es que no entren…
- … y si consiguen entrar, que no infecten al paciente cero…
- … y si infectan al paciente cero, que este no pueda infectar a los demás…
- … y que si todos se infectan, que tengas copia de seguridad fría …
- … y si no tenías copias de seguridad fría, que tuvieras una copia de tu curriculum en tu casa… (esto último no lo dice Mitre… es de mi cosecha)

Con las estrategias actuales todos estos puntos están “porosos” en algún momento. Zero Trust propugna que al menos uno de estos “… y si…” no puedan darse nunca. Hay que romper la cadena de ataque al menos en un punto. Y que esta rotura sea estable. No esté ligada a ciclos de actualización de sistemas y mecanismos de protección.
Es decir, hay semanas (o meses) en el que los PCs y los Servidores de cada compañía están vulnerables porque es imposible técnicamente

tenerlos siempre a la última versión. Los atacantes lo saben. Ese es el segundo elemento de éxito con el que cuentan. Una vez que han entrado por el RDP o la VPN sólo les queda esperar a esos días del mes en el que seguro que los sistemas son vulnerables, y actuar entonces.

▪ Principio # 2 de Zero Trust Architecture (NIST 800-207)

"All communication is secured regardless of network location… Network location alone does not imply trust"

Ninguna máquina debe poder "observar" a otra por el hecho de estar en la misma red.
El Principio #2 de NIST persigue que no pueda haber una propagación masiva de un Ransomware, simplemente porque no haya visibilidad entre los PCs dentro de las redes. Y que cada comunicación entre un PC y un Servidor esté expresamente autenticada y autorizada. Que el hecho de que un atacante se haga con un servidor no le permita tener a su disposición TODOS los PCs de las todas las redes con las que tiene conexión.
Si impides la visibilidad en "plano" entre las máquinas de la empresa, le pones bastante más difícil al atacante organizar un Ransomware dentro de tu empresa.

▪ ¿Es aplicable a otro tipo de incidentes?

Esto no es sólo aplicable a Ransomware. Si observas Mitre ATT&CK, las columnas centrales son las dedicadas a los pasos de "Discovery" y "Lateral Movement". Si haces un esfuerzo muy grande en conseguir anular todas las debilidades de estas dos columnas, reduces muchísimo la posibilidad de que los ataques progresen dentro de tu empresa. No sólo los de Ransomware. También habrás conseguido aproximarte bastante a la anulación, entre otros, de los demás ataques de malware y de los ataques dirigidos (Targeted Attack).

Enlaces de interés...

- El ransomware será la principal amenaza para la seguridad en 2021
- Para 2021 las mayores amenazas serán el ransomware y el malware fileless
- El ransomware PLEASE_READ_ME compromete al menos a 85.000 servidores

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos it User

Almacenamiento it

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

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

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

Un cuento de Navidad... o sueñan los androides con ovejas eléctricas

En una fresca mañana de la primera semana del siglo XXII, John Bowne III, ciudadano digital nacido a finales la primera mitad del siglo XXI en la zona conocida por el área Tijuana-San Angeles de California, utiliza el dispositivo digital que le mantiene unido al resto de los 4.500 millones de conciudadanos que conviven en la tierra al comenzar este nuevo siglo.

Le dedica los habituales 15 minutos de revisión de los indicadores de FELICIDAD en su Barrio, área urbana, área regional, zona continental americana y Global para comprobar que siguen todos por encima del 99%, como ha sido en los últimos 5 años, y cumplir con su deber de aportar su calificación diaria y si hubiera lugar aquellas cosas que le han interesado en las últimas 24 horas.

Esta aportación ciudadana diaria es el combustible que hace funcionar el denominado Poder Ejecutivo Digital Global, que, por motivos nostálgicos, es como se denomina al Sistema Colaborativo apoyado por Inteligencia Artificial que, a principios de la década de los 70, empezó a sustituir a los cada vez más decadentes poderes ejecutivos humanos encarnados por individuos con grandes y deformes egos y narcisismo extremo que pretendían situarse por encima de los nuevos Ciudadanos Digitales que ya no querían ser gobernados por ególatras sino más bien gobernarse ellos mismos con sistemas colaborativos digitales apoyados por sistemas de Inteligencia Artificial.

Como se estudia en la Historia del siglo XXI, estos procesos de Evolución Tecnológica fueron más lentos por trabas que fueron poniendo aquellos que se beneficiaban de haberse apropiado del antiguo poder ejecutivo olvidando que apareció como servicio público.

Los Derechos Humanos Digitales, que han evolucionado desde la mítica Declaración de los Derechos Humanos del siglo XX, han conseguido hacer evolucionar la sociedad de manera global y son el regalo que las generaciones del siglo XXI les hacen a las nuevas generaciones del siglo XXII

Ya en 2070, el Poder Ejecutivo Digital Global superó en eficacia a cualquier poder ejecutivo local, regional, nacional o global dirigido por un ser humano

Se estudia, por otra parte, como la pandemia de la tercera década del siglo, primera pandemia en la Era Digital de la Humanidad, aceleró el desarrollo tecnológico y, en mayor medida, la disrupción digital y la implantación de sistemas de Inteligencia Artificial, en un Circulo Virtuoso donde fueron acelerándose mutuamente para llegar en décadas a avances que se suponían que llevarían siglos.

La Disrupción Digital del Poder Ejecutivo trasladando la capacidad de control a sistemas colaborativos apoyados por sistemas de Inteligencia Artificial que permiten la participación continua de los Ciudadanos Digitales, dejó obsoleta la necesidad de representantes nombrados cada cuatro o seis años y con una cada vez mayor desconexión de los nuevos ciudadanos digitales del siglo XXI. La incapacidad del Poder Legislativo de realizar una gestión adecuada para mantener y evolucionar las leyes a la velocidad de la evolución digital y tecnológica, hizo que fuera sustituido por un sistema colaborativo apoyado por Inteligencia Artificial que en menos de una década realizó el trabajo pendiente de casi siglo y medio.

El grado de satisfacción de los ciudadanos digitales con el Poder Legislativo Global, denominado así por motivos nostálgicos, fue rápidamente subiendo hasta situarse por encima del 99%, aportando solidez a los índices de FELICIDAD e incrementando la participación ciudadana diaria que, por fin, puede participar activamente la democracia digital sin filtros ni cortapisas.

John Bowne III y su pareja Eva Chiang, nacida a mediados del siglo XXI en la isla de Taiwán, comunicaron a través de interfaz digital universal al Poder Ejecutivo Global que el último de sus dos hijos había dado por concluido su período de formación en fa-

milia y, por tanto, ellos daban también por concluido su derecho a la dedicación exclusiva para la educación y se ponían a disposición de la comunidad para asumir nuevas responsabilidades relacionadas con su formación y deseos de desarrollo personal.

Claro que el Poder Ejecutivo Digital Global se ocupa del funcionamiento del planeta siguiendo a través del sistema colaborativo la opinión diaria de los 4.500 millones de ciudadanos digitales, faltaría más, pero, a diferencia de todo lo conocido anteriormente por la humanidad, tiene la capacidad y la usa para ocuparse de cada uno de los ciudadanos individualmente y, lo que es más importante, es capaz de proporcionar las mejores soluciones para el bien común y el bien individual al mismo tiempo.

Ya en 2070, el Poder Ejecutivo Digital Global superó en eficacia a cualquier poder ejecutivo local, regional, nacional o global dirigido por un ser humano o grupo de seres humanos, aunque llevó aún una generación completa de ciudadanos digitales y 25 años eliminar a los candidatos narcisistas y ególatras que pretendían dirigir a sus conciudadanos digitales a sabiendas que el poder Ejecutivo Digital Global los había hecho obsoletos, porque los ciudadanos digitales de 2075 empezaron a dirigir sus destinos a través de un sistema colaborativo apoyado por un sistema de Inteligencia Artificial que analiza y procesa esos datos para dar la mejor solución a nivel global, regional e incluso individual.

Volviendo a John Bowne III y Eva Chiang, en un plazo de 7 días se les han propuesto diferentes nuevas responsabilidades. A John en el área de Cibergenética, Ciberseguridad y Cuidado Emocional de menores de 10 años; y a Eva en el área de Matemáticas Fundamentales, Elaboración de Algoritmos Cuánticos Multidimensionales y Cuidado emocional de menores de 10 años; donde la experiencia de cada uno es un valor a considerar, pero también se les ofrece la posibilidad de iniciar una

nueva y completamente diferente carrera profesional mediante un período de formación y asesoramiento profesional.

Siendo John y Eva adultos jóvenes menores de 60 años, han recibido el ofrecimiento de emigración espacial a las colonias espaciales en el sistema solar e, incluso, poder optar a las primeras emigraciones espaciales de larga duración a sistemas estelares cercanos y exploración del espacio profundo.

El mayor de los hijos de John y Eva ha solicitado formación en Cuidado Emocional de Menores de 10 años, con el ánimo de cumplir con su derecho de reproducirse y cuidar del desarrollo de un nuevo ciudadano digital y, en paralelo, Análisis y Monitorización de sistemas de Inteligencia Artificial; la menor ha solicitado formación musical y desarrollo de sistemas de entretenimiento digital con soporte de Inteligencia Artificial para elaborar arte digital al nivel requerido por las nuevas generaciones de ciudadanos digitales, y ha manifestado en la actualidad su desinterés por su derecho a reproducirse al menos hasta al menos conseguir sus objetivos artísticos .

Estos 4 ciudadanos digitales son un mínimo ejemplo más individualizado de los intereses que manifiestan el resto de los 4.500 millones de ciudadanos digitales del siglo XII, que podría ser el inicio de un nuevo salto evolutivo de la especie humana, pero esto es objeto de un sueño aún más avanzado.

Por lo que se puede intuir, los Derechos Humanos Digitales, que han evolucionado desde la mítica Declaración de los Derechos Humanos del siglo XX, han conseguido hacer evolucionar la sociedad de manera global y son el regalo que las generaciones del siglo XXI les hacen a las nuevas generaciones del siglo XXII.

Así pues, Feliz Navidad y Prospero 2101, desde un sueño del optimismo de 2020.

Este cuento navideño no incluye una consideración de la evolución del poder judicial por no tener tiempo ni espacio en este pequeño sueño navideño, y la gran dependencia de la evolución de los otros dos poderes, que pueden haber reducido en gran manera el aparato judicial necesario por haberse reducido la violación de las leyes por parte de los nuevos ciudadanos digitales. Será objeto de un sueño adicional.

Enlaces de interés...

- Teoría de la separación de Poderes