it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Octubre 2020 - nº 34

Phishing, la amenaza eterna

“Los CISO somos ciberresilientes desde hace mucho tiempo”

¿Cómo mantener la seguridad en un mundo inundado por las cookies?

Planteando la base digital para el negocio en un mundo cambiante

Hacia un nuevo orden digital inteligente y seguro

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

IT Digital Security

Directora Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez Bárbara Becares
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

Phishing, la amenaza eterna

Hace décadas que el phishing se instaló en nuestro día a día, y lejos de irse reduciendo, no ha hecho sino crecer sin freno y hacerse más sofisticado. Iniciándose en el correo electrónico y asociado en sus primeros tiempos al ordenador, el phishing ha revolucionado hacia el móvil y los SMS en nuevas formas que tienen el mismo objetivo: engañar al usuario para que pinche donde no debe, ceda sus credenciales, se descargue la amenaza que desatará el terror.

Cuando hablamos de phishing el usuario, el empleado, es quien está en primera línea de batalla. La evolución de unos mensajes generales, con faltas de ortografía y poco creíbles hacia otros con todo tipo de detalles recogidos en la información que desperdigamos en redes sociales sin darnos cuenta, está haciendo que el phishing sea cada vez más difícil de detectar y que los programas de formación y concienciación se hayan generalizado en las empresas. Y junto con ello, soluciones de seguridad de nueva generación, tecnologías de sandboxing avanzadas que permitan detectar una amenaza que parece eterna.

En este número de IT Digital Security hablamos también de seguridad multicloud, temática de un desayuno que reunió a Thales Data Protection, Trend Micro, S21sec y SonicWall, hablamos de Cookies, de Human Augmentation o de cómo la comunicación sigue siendo la asignatura pendiente de los responsables de seguridad.

En el apartado de entrevistas los protagonistas son Javier Sánchez Salas, CISO de Haya Real Estate; Marco Blanco, nombrado recientemente responsable de Splunk en la región de Iberia y Neil Thacker, CISO de Netskope para la región de EMEA.

La actualidad se completa con una revista digital centrada en las nuevas soluciones B2B de Kaspersky así como otro documento que recoge todo lo acontecido en el VMworld 2020, el evento anual de VMware.

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

itds

Sumario

En Portada

Phishing, la amenazas eterna

Actualidad

Mejorar la comunicación sigue siendo la asignatura pendiente de los responsables de seguridad

El círculo se cierra.

Pulse Secure lleva su servicio de acceso seguro al cloud

Human Augmentation, nuestros cuerpos al alcance de los ciberdelincuentes

Reportaje

¿Cómo mantener la seguridad en un mundo inundado por las cookies?

Desayunos

La seguridad en entornos multicloud

Entrevistas

“Los CISO somos ciberresilientes desde hace mucho tiempo”

Javier Sánchez, HAYA Real Estate

“Los fabricantes de IoT han dado marcha atrás en sus posturas de seguridad”

Neil Thacker, Netskope

“El machine learning es lo que nos hace diferentes”

Marco Blanco, Splunk

Revistas Digitales

Planteando la base digital para el negocio en un mundo cambiante

Hacia un nuevo orden digital inteligente y seguro

No solo IT

El Poder Legislativo en la Nueva Sociedad Digital: ¿Evoluciona o no?

La demanda de digitalización impulsa la recuperación económica en EEUU

Índice de anunciantes

Sophos Managed Threat Response

¿Aún no conoce todo el potencial de nuestro servicio MTR?

Nuestro equipo de expertos ofrece un servicio con funciones de búsqueda,
detección y respuesta ante amenazas las 24 hora

Conocer qué ha ocurrido en el pasado y qué está ocurriendo ahora es imprescindible

Descubra todos los detalles en este webinar

Viernes 9 de Octubre | 10:30 [CEST]

SOPHOS

El círculo se cierra.

Pulse Secure lleva su servicio de acceso seguro al cloud

El 2 de octubre de 2014 Juniper Networks vende Junos Pulse, su negocio de VPN y secure Gateway, a Siris Capital, quien crea una nueva compañía que bautiza como Pulse Secure con la misión de potenciar la productividad empresarial mediante una movilidad segura y sin problemas. Recién creada la compañía, se anuncia la compra de MobileSpaces, una empresa de seguridad de aplicaciones móviles y empieza a hablar de acceso seguro, un término al que años después se aferraría toda la industria.

Desde entonces Pulse Secure no ha cambiado ni su estrategia ni su misión, reforzada en 2017 con la compra del negocio de Virtual Application Delivery Controller (vADC) a Brocade Communications Systems, lo que permitió a la compañía expandir su portfolio de acceso seguro a servicios y aplicaciones.

El acceso seguro que Pulse lleva promoviendo desde sus inicios se ha convertido en realidad en el nuevo perímetro, un perímetro amorfo que cambia dependiendo de dónde esté la persona, qué dispositivos esté utilizando, desde dónde y a qué quiere acceder. “Lo que necesitamos es ir a un modelo Zero Trust”, Dice Luis Miguel García, el director general de Pulse Secure en la región de Iberia; un modelo Zero Trust que, asegura “ya vimos en su día”.

Afirma también el directivo que la evolución de la empresa no ha sido sencilla; “cogimos la plataforma Junos Pulse, la transformamos digitalmente y llevamos estos seis años ayudando al mercado a que lo que nosotros llamamos Secure Access Journey, o pasar de un modelo tradicional a un modelo Zero Trust, sea lo más sencillo posible”. La visión, que está en el mismo ADN de la compañía, que forma parte de la misión inicial, ha sido reconocida por algunas grandes consultoras o grupos, como Gartner o la Cloud Security Alliance, que han potenciado el concepto Zero Trust, “una filosofía para la cual se fundó nuestra empresa hace seis años y por la que este año hemos tenido un crecimiento muy exponencial”.

Seamless Acces

“Nuestro elemento completamente diferenciador es que venimos atacando tanto los productos tradicionales como los proyectos ZTNA (Zero Trust Network Access), o toda la parte de SASE (Secure Accesss Service Edge) que ahora está muy de moda,

"Se necesita el mismo control de acceso cuando estoy en mi casa, cuando estoy en un aeropuerto o en movilidad"

"NO BUSCAMOS IMPLEMENTAR UN PRODUCTO, SINO UNA METODOLOGÍA DE ACCESO SEGURO" (PULSE SECURE)

CLICAR PARA VER EL VÍDEO

con lo que nosotros denominamos Seamless Access", asegura Luis Miguel García. Explica que esta aproximación consiste en poder ofrecer la misma experiencia en una plataforma SaaS, IaaS o PaaS, en el centro de datos o con aplicaciones móviles, fácil de usar, desde cualquier dispositivo, e independientemente de si están en la LAN corporativa o se conectan de forma remota a través de Internet.

Añade el máximo responsable de Pulse Secure en España que su compañía proporciona una gran experiencia de usuario que cumple con los requisitos clave de cumplimiento y seguridad "centrándonos en el control de acceso granular y avanzado (o posture management como otros denominan), unificando la autenticación de usuarios (SSO), el cumplimiento de dispositivos y la autorización basada en roles. Por ejemplo, nuestro Single Sign On para aplicaciones de nube y centro de datos está vinculado al cumplimiento de dispositivos y posture check, así como a la autenticación de usuarios basada en roles".

Sobre los clientes a los que va dirigida la oferta de Pulse Secure, dice Luis Miguel García que la compañía tiene una propuesta bastante flexible; "nuestra idea es ayudar tanto a clientes que siguen invirtiendo en modelos de infraestructura de red, del tipo: VPN, accesos remotos, NAC, SSO, MDM... Que son modelos más tradicionales", así como a los que están metidos de lleno en procesos de transformación digital.

En todo caso, algunos elementos clave que la compañía se está encontrando en la demanda de sus soluciones son, por un lado, los que buscan entender cómo sus políticas de seguridad actuales pueden evolucionar para cubrir a los usuarios, los dispositivos, las aplicaciones, las redes y la infraestructura en lo que son iniciativas Zero Trust.

Atributos de una solución de Zero Trust Access

Desde Pulse Secure aseguran que en una evolución hacia las soluciones de Zero Trust Access se deben combinar 4 atributos:

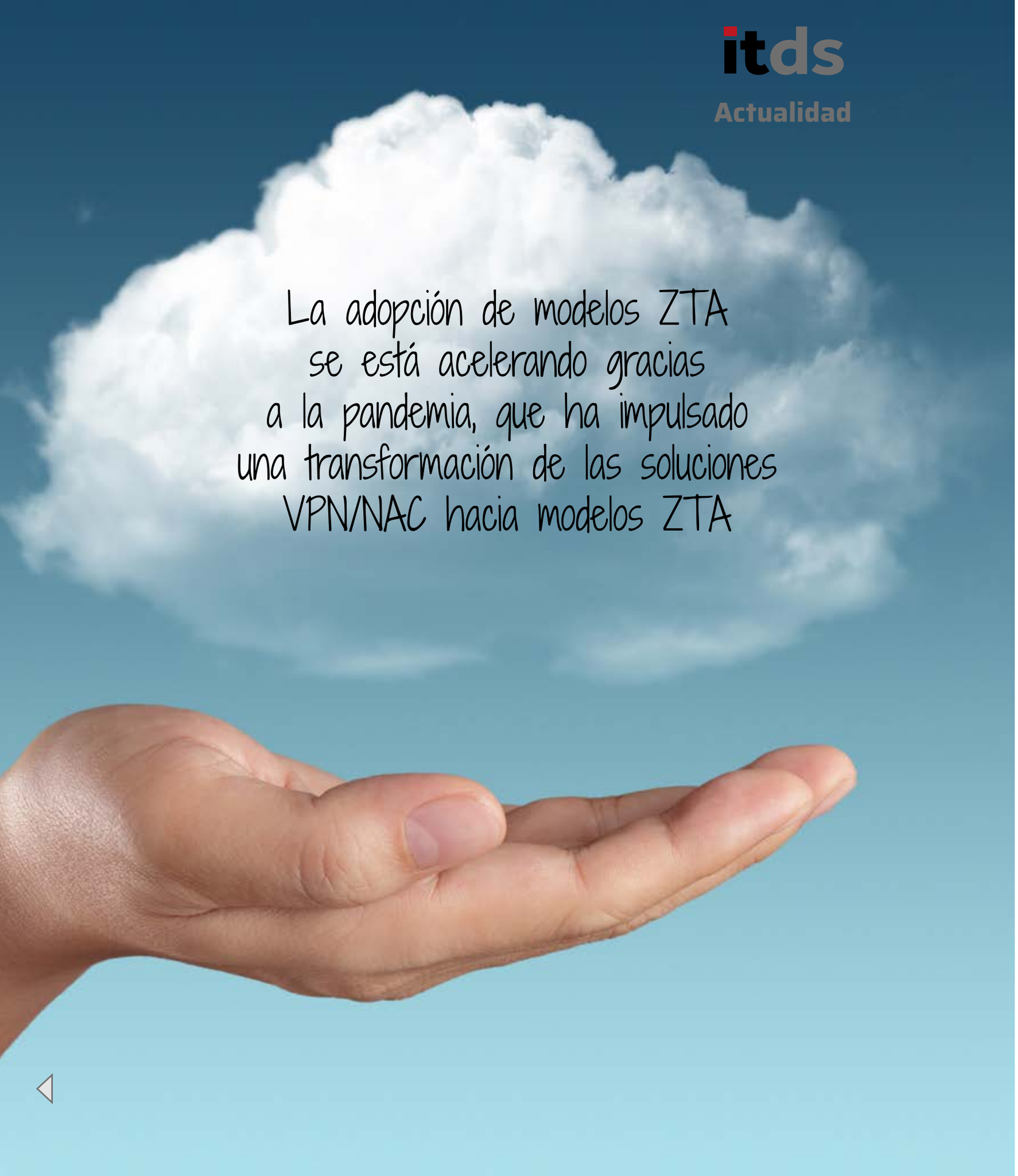
- La experiencia de los usuarios debe ser sencilla y estéticamente agradable de extremo a extremo, incluyendo aspectos como la Interfaz de Usuario (UX) para un único inicio de sesión seguro en las aplicaciones a través de dispositivos, sistemas operativos e infraestructuras de aplicaciones heterogéneas.
- Se espera que haya movilidad y las empresas quieren aprovechar los dispositivos móviles y, al mismo tiempo, garantizar automáticamente el cumplimiento y la salud de los dispositivos y aislar las aplicaciones de trabajo de las aplicaciones privadas, incluso en los dispositivos no gestionados por BYOD.
- La nube híbrida es una opción de despliegue necesaria y las soluciones deben aprovechar el beneficio de la computación en nube y las arquitecturas tradicionales de los centros de datos, al tiempo que se ocupan del cumplimiento y los requisitos de seguridad. Por ejemplo, combina SSO con controles de cumplimiento de dispositivos y autorización de acceso basada en roles en todas las aplicaciones, ya sea que estén alojadas en nubes privadas o en nubes públicas IaaS o se entreguen como SaaS.
- La seguridad de los dispositivos es crítica, tanto para los dispositivos internos como para los externos, para el acceso de los BYOD y los Huéspedes a las redes internas. Las redes internas deben ser protegidas de una nueva generación de dispositivos de IO que pueden proporcionar puertas traseras a los hackers.

de los ciberataques. Ante el aumento de los ciberartaques y la pérdida de perímetro, las empresas necesitan considerar la seguridad de manera holística y abarcar el acceso interno y remoto, el acceso a la nube y la TI híbrida de forma global. Finalmente, hay clientes que buscan satisfacer las necesidades de una nueva generación de trabajadores que se ha acostumbrado a aprovechar las aplicaciones web y móviles junto con las aplicaciones empresariales tradicionales y esperan utilizar sus propios dispositivos móviles para acceder a todas las aplicaciones de trabajo, tanto en remoto como en la LAN corporativa.

SaaS llega a la oferta de Pulse

¿Cómo está siendo la evolución hacia un modelo as-a-service? ¿Cómo lo ha aceptado el canal de distribución? “El mercado está aceptando muy bien nuestro cambio”. A día de hoy todo va encaminado

También está el caso que busca soluciones que permitan a sus empleados y administradores de TI utilizar y desplegar recursos en entornos híbridos como un único conjunto integrado con capacidades. La explosión del Internet de las Cosas también impulsa la demanda de soluciones Pulse Secure, que ayudan a que esas soluciones de IoT que requieren que las cosas (es decir, los microdispositivos) puedan acceder a las aplicaciones “que deben” consumir esos dispositivos IoT en tiempo real mientras mantienen estas infraestructuras clave protegidas



a un modelo de suscripción y no tanto a un modelo de licencias perpetuas o inversión en la construcción de arquitecturas. Donde antes las organizaciones apostaban por un modelo de CaPex, ahora están apostando más por el modelo OpEx y reducir el TCO, "por lo tanto teníamos que ofrecer a nuestro canal ese modelo de solución SaaS como Pulse Zero Trust Access (PZTA) que va dirigido a los clientes que quieren un modelo de usar y suscribir", explica Luis Miguel García cuando le preguntamos cómo ha evolucionado la compañía hacia el modelo as-a-service.

El impacto de esta nueva oferta de Pulse Secure ha sido muy importante también para el canal de distribución de la compañía. Dice el directivo que Pulse Zero Trust Access (PZTA) basada en un modelo suscripcional ha sido visto por el canal como un "cerrar el círculo dentro de nuestro portfolio" y "nos permite pasar a un modelo SASE y tener un framework de seguridad y redes que establece una serie de tecnologías a cubrir de una forma más elástica y distribuida. Nuestra propuesta con PZTA se enmarca en la parte de seguridad, para ofrecer una de las mejores soluciones del mercado de Zero Trust Access como servicio y siendo la única propuesta del mercado que separa el plano de control del plano de datos e implementa de manera nativa la aproximación CARTA sugerida por Gartner".

ZTA vs VPN

Gartner predice que hasta el 60% de las VPN existentes en la actualidad serán reemplazadas por al-

gún tipo de tecnología ZTA para 2023, lo que situaría el valor de este mercado entre 20.000 y 24.000 millones de dólares para 2023.

Siendo uno de los principales proveedores de soluciones VPN, dice Luis Miguel García que “es evidente, las VPN existentes serán reemplazados por modelos ZTNA basados en on-premise o cloud”, y que Pulse Secure es “el único fabricante del mercado que puede ofrecer una propuesta

Según Gartner hasta el 60% de las VPN existentes en la actualidad serán reemplazadas por algún tipo de tecnología ZTA para 2023

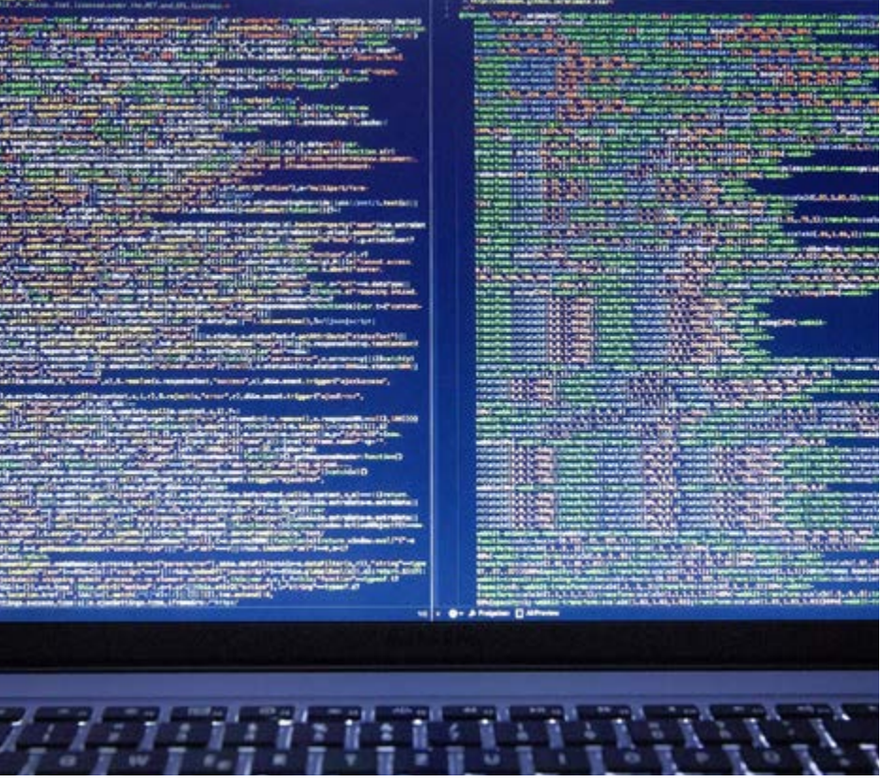
híbrida totalmente integrada”. Explica que por eso ha sido tan importante no sólo tener un modelo de seguridad de ZTA en modo on-premise como se tenía hasta ahora, “sino el reciente lanzamiento de ZTA en modelo cloud, en modelo consumo, para poder cubrir tanto un panorama on-premise, con un panorama Cloud o un hibrido, “con lo cual podemos ayudar a cualquier cliente de aquí hasta el 2023”, y añade que se sigue ofreciendo a los clientes de la compañía un offering mixto “de tal forma que cuando se quiera ir hacia un modelo de ZTA no haga falta hacerlo de manera radical”.

La adopción de modelos ZTA se está acelerando gracias a la pandemia, que ha impulsado una transformación de las soluciones VPN/NAC hacia modelos ZTA. Explica Luis Miguel García que una evolución hacia las soluciones de Zero Trust Access debe combinar 4 atributos: experiencia de usuario sencilla, movilidad, nube híbrida y seguridad de los dispositivos.

Sector Industrial

Recientemente se ha anunciado un acuerdo entre Nozomi y Pulse para el mercado de OT. El acuerdo pone sobre la mesa la solución Pulse Policy Secure, que permite un acceso remoto seguro y granular basado en la identidad y el rol del usuario (RBAC). ¿El industrial es el siguiente gran mercado en el que quiere estar presente Pulse? “Si, por supuesto. No hay que dejar de lado tanto las redes OT industriales, o los entornos productivos ya sean de banca, reatil, etc…”, asegura el directivo, añadiendo que Pulse Secure Policy Secure es una solución de control de acceso a la red (NAC) completa, fácil de implementar y lista para ser usada por BYOD, que aplica granularmente las políticas de seguridad. Se gestiona de forma centralizada con un motor de políticas que tiene en cuenta el contexto y proporciona granularidad de usuario, función, dispositivo, ubicación, hora, red y aplicación. Pulse Policy Secure ofrece una experiencia intuitiva para el usuario con el apoyo de un cliente multifuncional tanto para VPN, ZTA como para NAC.

Dice también el directivo de Pulse Secure que se necesita el mismo control de acceso cuando estoy en mi casa, cuando estoy en un aeropuerto o en movilidad, y que también es el mismo control de accesos cuando estoy pinchado a mi red corporativa, a la cual no sólo estamos conectadas personas, sino dispositivos. Al respecto de los dispositivos dice Luis Miguel García que su compañía está abordando proyectos de coche conectado, ambulancias conectadas, smart cities… porque todos



A día de hoy todo va encaminado a un modelo de suscripción y no tanto a un modelo de licencias perpetuas o inversión en la construcción de arquitecturas

estos dispositivos “son elementos corporativos que están fuera del perímetro de seguridad pero que necesitan inyectar información dentro las organizaciones y hay que protegerlo”.

Negocio

Hasta no hace mucho, la facturación de la compañía se dividía al 50/50 entre las soluciones de acceso remoto y NAC, pero “en 2020 hemos cambiado a un modelo 80/20 en el que el 80% son soluciones de acceso remoto y el 20% soluciones de NAC”. Por donde más crece la compañía es por las soluciones de Work from Home, Hybrid IT/Multi-Cloud y Data Center Access que “son una tendencia del mercado innegable porque los modelos de seguridad basados en el perímetro han dejado de tener validez y los usuarios y dispositivos corporativos acceden desde cualquier lugar y consumen aplicaciones y servicios que se encuentran alojadas también en cualquier lugar”.

El resto de la propuesta de la compañía, ese 20% se agrupa en la propuesta de Network and Cloud Visibility (que Gartner determina como SASE), Threat Protection , Business Continuity y Security Orchestration.

Sobre la parte de Threat Protection, dice Luis Miguel García que se cubre con la parte de CARTA, “un concepto fundamental en la propuesta de Pulse Secure hace mucho años” y que la compañía, como líder en soluciones de Acceso Seguro tiene como máxima: un usuario o dispositivo es peligroso antes de entrar pero lo es mucho más cuando ya está dentro. “Si solo nos preocupamos de securizar el acceso antes de que este se produzca, estaremos obviando anomalías en el comportamiento o uso inadecuado de los privilegios concedidos una vez hayan sido validados. Es por esto que en PZTA hacemos un análisis de comportamiento en tiempo real tanto del usuario, como del dispositivo, como de las aplicaciones así como de feeds de inteligencia que nos puedan venir de terceros. En el momento que se produzca un cambio en la política Zero Trust del usuario/dispositivo y/o se detecte una anomalía que comprometa la seguridad, eliminaremos los accesos en tiempo real a aquellas aplicaciones o servicios que pudieran verse afectados por dicho comportamiento eliminando así cualquier compromiso de seguridad que pudiera existir”.

Por último dice el directivo de Pulse Secure que la visibilidad, la prevención en tiempo real y la respuesta automatizada son fundamentales para que las tecnologías de la información puedan combatir las amenazas que son el resultado de la actividad interna, el uso indebido de privilegios, los dispositivos que no cumplen las normas establecidas y la pérdida de los dispositivos/robo. it

Enlaces de interés...

- Ivanti compra MobileIron y Pulse Secure
- Pulse Zero Trust Access (PZTA) simplifica la gestión y mitiga el riesgo
- Pulse Secure consolida los accesos con su nuevo Pulse Access Suite Plus

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

Human Augmentation, nuestros cuerpos al alcance de los ciberdelincuentes

Que la ficción se convierta en realidad es más habitual de lo que podría parecer. Que se lo digan a Julio Verne, o a Isaac Asimov. Empieza a ser común escuchar el término Human Augmentation, que aboga por incrementar las capacidades del ser humano gracias a la tecnología.

Kaspersky, que hace unos años hablaba de la ciberinmunidad, se centra ahora en esta tendencia que, utilizada correctamente, tiene el potencial de mejorar nuestra salud, entretenimiento, productividad y calidad de vida en general. Claro que para que sea un "aumento" debe integrarse tanto en la vida del usuario que se convierta en una extensión de él, por lo que abarca desde tecnologías ampliamente aceptadas y enormemente beneficiosas, como marcapasos

Gartner identificó el Aumento Humano como una tendencia que tendrá un "impacto transformador" y seguirá creciendo en popularidad durante los próximos cinco a diez años

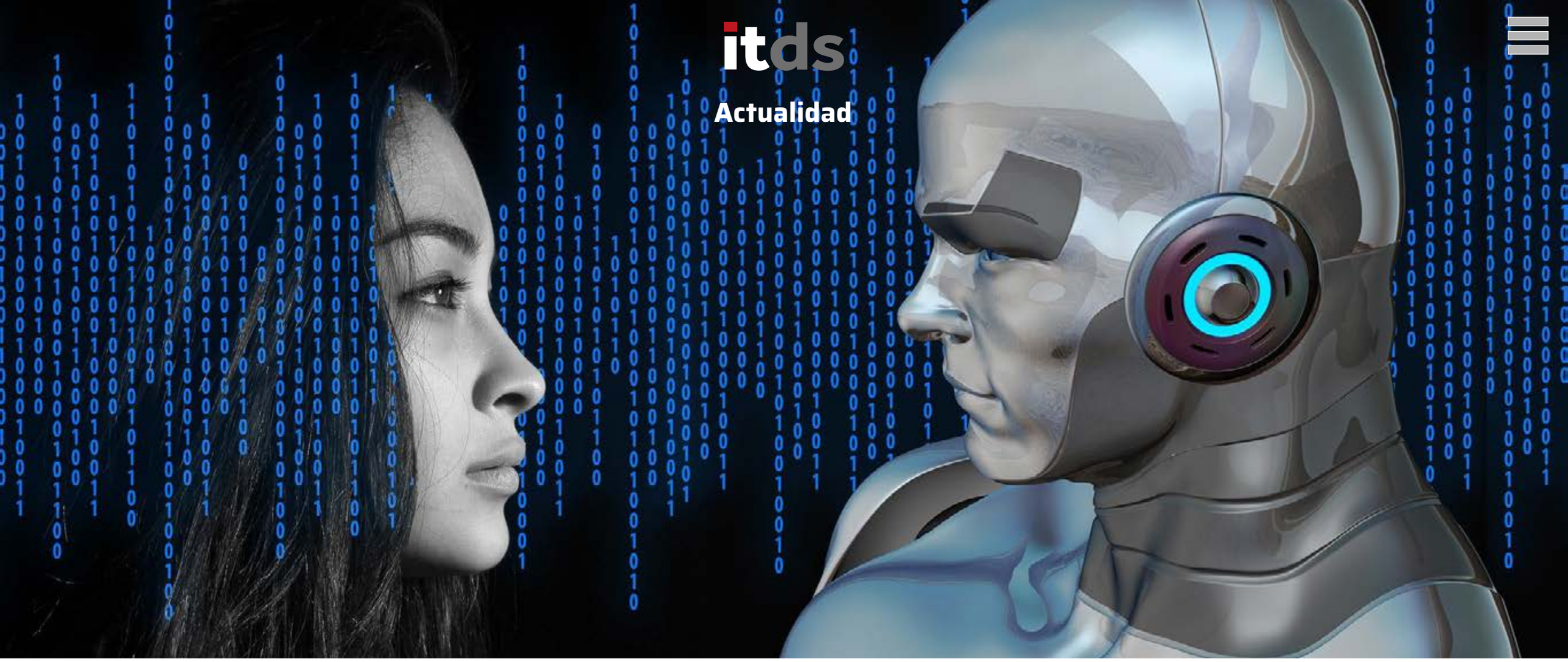
y audífonos, hasta aumentos más controvertidos, como modificaciones genéticas, implantes neurales y la creación de tejido artificial.

Recordemos que hace unas semanas Elon Musk, el carismático director general de Tesla y Space-X, presentó un "chip cerebral" que, con suerte, permitirá que personas con discapacidades puedan volver a hablar o caminar. En el momento de la presentación dijo: "Creo que os va a dejar boquiabiertos. Es como un Fitbit conectado a tu cráneo mediante unos cables diminutos". La ficción se está haciendo realidad.

El año pasado, la firma de investigación Gartner identificó el Aumento Humano como una tendencia que tendrá un "impacto transformador" y seguirá creciendo en popularidad durante los próximos cinco a diez años. Sin embargo, trae consigo varias consideraciones éticas y de seguridad. "El aumento humano es una de las tendencias tecnológicas más importantes en la actualidad", dijo Marco Preuss, director europeo de investigación y análisis global de Kaspersky, añadiendo que los amantes de este Aumento Humano ya están probando los límites de lo que es posible y que "se necesitan estándares comúnmente acordados para garantizar que el aumento alcance su máximo potencial y minimice los riesgos".

Kaspersky ha publicado un informe sobre esta Human Augmentation, examinando cómo se percibe la tecnología. Este informe, elaborado por la firma de investigación Opinium entrevistó a más de 14.000 personas en 16 países para comprender "qué mejorarían las personas, qué elementos deberían permitirse mejorar, la ética, la seguridad y la participación del gobierno en forma de regulación futura".

Entre otras cosas, la investigación encontró que el 63% de los encuestados consideraría aumentar sus cuerpos con tecnología para mejorarlos, ya sea de forma permanente o temporal, siendo una mejoría de la salud física el atributo más popular que los



"Se necesitan estándares comúnmente acordados para garantizar que el aumento alcance su máximo potencial y minimice los riesgos"

Marco Preuss, director europeo de investigación y análisis global, Kaspersky

encuestados querían mejorar. El mayor beneficio del aumento humano fue su potencial para mejorar la calidad de vida.

Según el estudio, la mayoría de los encuestados españoles desearía que esta tendencia se utilizara para el bien de la humanidad, y el 55% para mejorar la calidad de vida. Por otra parte, los encuestados españoles temen que el uso de este tipo de tecnologías solo llegue a estar al alcance de los ricos (57%), mientras que para nueve de cada 10 (91%) el principal miedo es que sus cuerpos puedan ser hackeados por ciberdelincuentes.

Los adultos del sur de Europa, incluyendo España, Portugal, Grecia e Italia, así como Marruecos, son los más predispuestos al "Human Augmentation", mientras que británicos y franceses parecen ser los más escépticos.

Recoge también el estudio que casi la mitad (47%) de los entrevistados cree que los gobiernos deberían regular el concepto "Human Augmentation". El Reino Unido es el país más a favor de la intervención del gobierno (77%) y Grecia es el más reticente (17%)

Human Augmentation en Kaspersky NEXT

Hace unas semanas, durante el evento Kaspersky NEXT, se planteó un debate en torno a las amenazas u oportunidades de la Human Augmentation.

Enlaces de interés...

- Kaspersky forma a las empresas en ciberseguridad con Adaptive Online Training
- El código completo del malware bancario Cerberus, disponible gratis en los foros clandestinos
- Kaspersky dota a los analistas de seguridad de más recursos para detectar y analizar amenazas
- El 35% de los españoles compartiría datos privados a cambio de ofertas y descuentos

Para nueve de cada 10 usuarios el principal miedo del Human Augmentation es que sus cuerpos puedan ser hackeados por ciberdelincuentes

La discusión se inició con David Jacoby y Marco Preuss de Kaspersky, analizando las amenazas y los temores de la tecnología, especialmente en torno a la piratería, los implantes y la identidad, así como los temores en torno a una "brecha de acceso" entre ricos y pobres. Sin embargo, el transhumanista estadounidense Zoltan Istvan y el filósofo australiano Julian Savulescu tendieron a virar hacia una perspectiva más brillante, y ambos dijeron que sería mejor para la humanidad a largo plazo si nos sumamos al aumento; ambos también señalaron que, históricamente, frenar o paralizar la tecnología por miedo siempre ha terminado mal, por lo que debemos mirar hacia adelante.

Sin embargo, aunque hubo diferencias de opinión sobre cómo podría ser el futuro y si el aumento es una amenaza, todos los invitados acordaron unánimemente que el aumento para personas con discapacidades es un cambio de juego y solo puede ser algo bueno.

Es inevitable el avance de esta Human Augmentation, así como las trabas y obstáculos éticos y de seguridad que le acompañen. Quizá porque por el momento su uso no está muy extendido los ciberdelincuentes no han explorado aún sus opciones. ¿O sí?

Compartir en RRSS

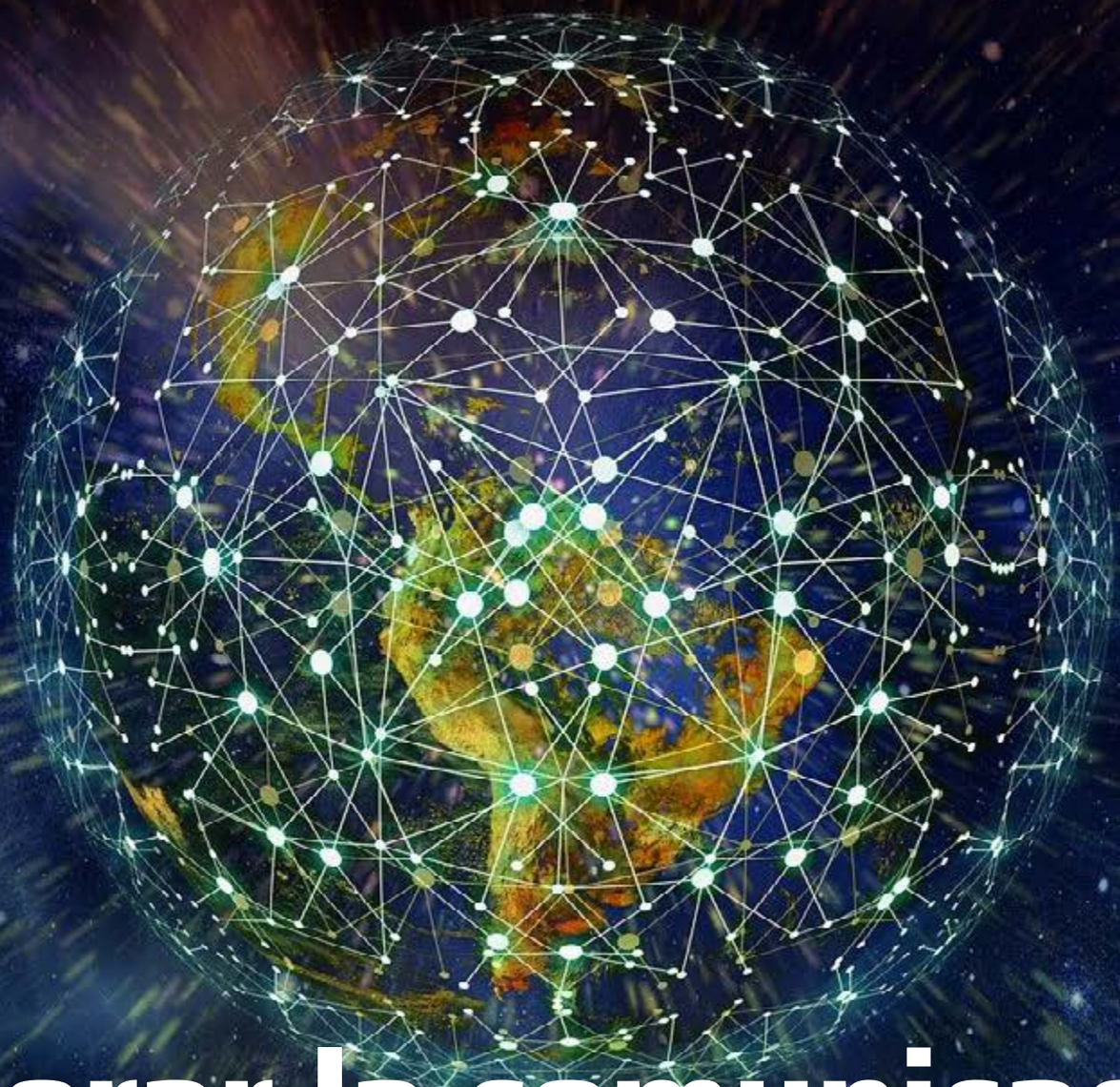
ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES



Mejorar la comunicación sigue siendo la asignatura pendiente de los responsables de seguridad

Un reciente estudio de Bitdefender pone de manifiesto que un 63% de responsables de ciberseguridad creen que la ciberguerra es una amenaza para sus organizaciones; un 57% cree que los ataques de ransomware van a seguir creciendo durante los próximos meses, o que el déficit de talento en el sector de la seguridad es una realidad y la solución pasa por enriquecer los equipos con una mayor diversidad de habilidades.

El 68% de los responsables de seguridad españoles cree que la ciberguerra es una amenaza inminente para sus organizaciones, una cifra que se acerca mucho al 63% a nivel global. Además, un 49% cree que los ataques relacionados con la ciberguerra tendrá un perjuicio real para la economía en el próximo año. A pesar de ello, un 30% no tiene o no sabe si su empresa tiene una estrategia para hacer frente a ese riesgo.

El estudio, bautizado como 10 in 10, analiza los resultados de una encuesta realizada a 6.724 profesionales y responsables de seguridad de la información de diez países, de los que 526 son españoles, que trabajan en todo tipo de compañías -desde pequeñas empresas a partir de cien empleados, hasta grandes corporaciones que cotizan en bolsa y cuentan con plantillas superiores a las 10.000 personas-, de un amplio espectro de sectores, como Tecnología, Finanzas, Salud y Administración Pública.

Sobre la ciberguerra dice Liviu Arsene, Senior Threat Analyst de Bitdefender, que es muy eficaz “debido a la diversidad de vectores de ataque y cargas útiles que se utilizan”, añadiendo que en el último año, se ha detectado un aumento del malware sin archivos y exploits descubiertos re-

Liviu Arsene, Senior Threat Analyst, Bitdefender

BITDEFENDER 10 IN 10, 2020

El Estudio 10 in 10 es una investigación independiente que analiza qué factores afectarán más el éxito de la seguridad en la próxima década. La investigación ha explorado las expectativas específicas que tienen las organizaciones en lo que respecta a la seguridad y lo que los equipos de seguridad querrían hacer si tuvieran más tiempo, más dinero y culturas empresariales que acogieran y apoyaran la ciberseguridad.

cientemente contra sistemas operativos o software de terceros.

Uno de los asuntos tratados en el estudio es el ransomware. Un 44% de los responsables de seguridad españoles dice que está observando un incremento de los ataques de ransomware y un 57% (63% a nivel global) espera que durante los próximos meses este tipo de ataques siga creciendo. Lo que es más preocupante, un 47% de los encuestados españoles (42% a nivel global) piensa que es posible que un ataque de ransomware pueda acabar con su negocio en los próximos 12 a 18 meses si no se incrementa la inversión en seguridad para evitarlo.

Lo que está claro es que “el ransomware está aquí para quedarse durante al menos varios años más”, dice Liviu Arsene, y eso es porque esta amenaza sigue siendo muy rentable, tanto como para que los ciberdelincuentes estén adoptando nuevas tácticas para ejercer una presión adicional sobre las víctimas. Recuerda el analista de Bitdefender que el ransomware ya ha agregado capacidades de exfiltración de datos y que ahora los cibercriminales amenazan con filtrar esta información robada si las empresas afectadas deciden no pagar el rescate. En todo caso, poco tienen que perder, por el 47% de los encuestados españoles (50% a nivel global) está convencido de que su

Para afrontar la nueva realidad con éxito es necesario que este sector comience a comunicar de una forma más accesible, en la que todo el mundo entienda lo que se está diciendo

empresa pagaría el rescate para evitar la publicación de sus datos.

Falta de comunicación

Lo que resulta curioso es que el 53% de los profesionales de seguridad de la información españoles (51% a nivel global) cree que para conseguir aumentar la inversión que se destina a sus proyectos es necesario dar un giro drástico a su comunicación. Este porcentaje aumenta hasta el 55% entre los CISO y CIO a nivel global, profesionales que cuentan, en gran medida, con presencia en los consejos de dirección de sus organizaciones.

No es algo nuevo. Hace mucho que los departamentos técnicos de las empresas vieron la necesidad de hablar el lenguaje de los negocios.

En opinión de Liviu Arsene la tarea no es fácil por varias cosas. Por un lado “la ciberseguridad es una especialidad compleja donde los desarrollos ocurren a diario, lo que obliga a los gerentes de ciberseguridad a mantenerse actualizados con los últimos desarrollos, por lo que tienen poco tiempo para cualquier otra cosa”. La aparición, constante, de siglas acuñadas por expertos o consultores (CASB, SASE, CARTA…) que a menudo sólo responden a iniciativas de marketing, “crea confusión en la industria y dificulta aún más a los gerentes de TI comprender para qué serviría la tecnología respectiva”.

Entre los cambios que deberían realizarse, un 41% de los encuestados españoles piensa que es fundamental mejorar la comunicación con la alta

Existe una clara disparidad entre el mayor uso de dispositivos conectados y la falta de seguridad que se implementa

dirección de sus compañías para lograr que comprenda mejor los riesgos a los que está expuesto el negocio. Un 37% (41% a nivel global) cree que es importante hacer hincapié en la comunicación a empleados y clientes. Finalmente, un 36% afirma que es necesario emplear un lenguaje menos técnico si lo que se pretende es que todo el mundo entienda bien tanto los riesgos como las formas de estar protegido.

La importancia de la diversidad

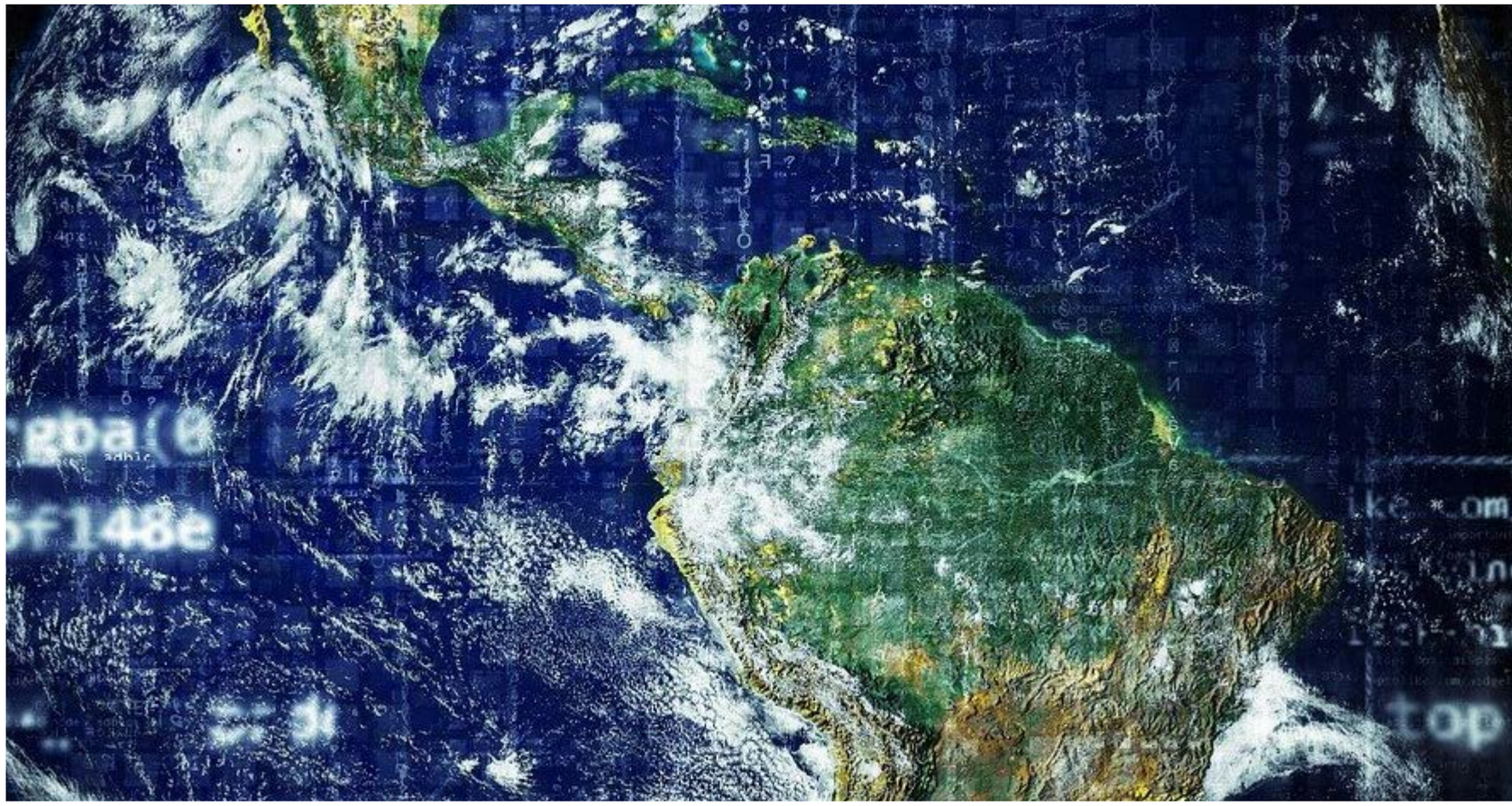
Uno de los mayores desafíos del sector es lidiar con el déficit de talento disponible, algo que se refleja en las opiniones de los profesionales encuestados. Así, un 39% de los españoles (43% a nivel global) considera que sus empresas se están viendo afectadas por la escasez de personal especializado.

En este sentido, un 10% de los responsables de seguridad españoles está convencido de que el avance en los desarrollos relacionados con la ciberseguridad va a seguir su curso, por lo que es muy probable que en un plazo de 12 a 18 meses se incremente aún más la brecha que ya existe con respecto a las habilidades de los profesionales. Hay que destacar que a nivel global mantienen esta opinión un 15% de los profesionales, y que hay países, como Francia, en el que la cifra de los que así piensan sube hasta el 17%.

El 28% de los CISO y CIO a nivel global consideran que si el déficit de talento continúa durante otros cinco años, es muy probable que acabe afectando a la supervivencia de las empresas. Igualmente, un 50% de los directores de IT y seguridad a nivel global piensan también que este es un problema que puede llegar a ser muy perjudicial para la evolución del negocio.

Parece, sin embargo, que solucionar el problema de la escasez de talento requiere algo más que la simple formación o contratación de personal cualificado en ciberseguridad. El 55% de los encuestados españoles (52% a nivel global) considera que en el sector de la ciberseguridad, aparte de talento, falta también diversidad, algo que supone una preocupación para ellos. En este sentido, un 36% de los profesionales españoles (40% a nivel global) coincide en afirmar que para ser eficaz, el sector de la ciberseguridad debería ser un reflejo de la sociedad a la que intenta proteger. Así, un 82% de los encuestados españoles (un 72% a nivel global) piensa que es necesario ampliar el conjunto de habilidades de los profesionales de la seguridad, para hacerlo más diverso.

En este sentido, el 41% de los profesionales de seguridad españoles (39% a nivel global) dice que añadir neurodiversidad servirá para fortalecer las defensas de ciberseguridad cibernética. Otro 38% (34% a nivel global) está convencido de que una fuerza laboral más neurodiversa servirá para nivelar el campo de juego en el que se lucha contra los malos. Todo lo anterior indica que la brecha de



habilidades es una realidad que ha llegado para quedarse, por lo que la solución pasa por buscar alternativas al talento tradicional.

La falta de talento se está afrontando con servicios gestionados o con automatización. Explica Liviu Arsene, Senior Threat Analyst de Bitdefender, que los servicios de Detección y Respuesta Gestionadas permiten a las empresas subcontratar por completo sus necesidades de seguridad de ciberseguridad, que a nivel tecnológico cada vez se descarga más automatización y toma de decisiones en las máquinas y que la inteligencia artificial

El 28% de los CISO y CIO a nivel global consideran que si el déficit de talento continúa durante otros cinco años, es muy probable que acabe afectando a la supervivencia de las empresas

y el análisis de riesgos humanos son solo algunas de las tecnologías que han sido extremadamente efectivas contra el malware.

IoT sin compromiso con la seguridad

Analiza también el estudio de Bitdender el uso de dispositivos IoT. Asegurando que va en aumento dice el informe que "existe una clara disparidad entre el mayor uso de dispositivos conectados y la falta de seguridad que se implementa, lo que deja a las empresas y los consumidores abiertos a una serie de amenazas potenciales".

Según los datos recogidos, el 45% de los CISO/CIO y 2 de cada 5 profesionales de seguridad de la información (40%) creen que es fácil para los ciberdelincuentes obtener el control de los dispositivos de IoT que utilizan los empleados desde casa con fines comerciales.

Afirma Liviu Arsene que a pesar de todas las increíbles características que la IoT trae a nuestras vidas, tanto desde el punto de vista comercial como industrial, "esta rama de la tecnología está plagada de problemas de seguridad, que van desde la falta de soporte de los fabricantes hasta vulnerabilidades que afectan a miles de millones de dispositivos a la vez.

Enlaces de interés...

- 'Creemos que la mayor diferencia de Bitdefender está en la tecnología' (Emilio Román)
- El cibercrimen tiene un nuevo 'modus operandi' y mejores habilidades a raíz del coronavirus
- El 55% de las empresas españolas carecía de un plan de contingencia de ciberseguridad para afrontar la crisis

Y añade que uno de los problemas más graves que a menudo se pasa por alto es que las personas no se dan cuenta de que poseen dispositivos de IoT.

Concluye el analista de Bitdefender que "2020 ha sido un año de cambios, para el mundo en general y para la industria de seguridad en particular", que "lo único que sabemos con certeza es que el panorama de la seguridad va a seguir evolucionando" y que "para afrontar la nueva realidad con éxito es necesario que este sector comience a comunicar de una forma más accesible, en la que todo el mundo entienda lo que se está diciendo".

El 47% de los encuestados españoles (50% a nivel global) está convencido de que su empresa pagaría el rescate para evitar la publicación de sus datos

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/

“Los CISO somos ciberresilientes desde hace mucho tiempo”

(Javier Sánchez Salas)

Indra y Ernst & Young han sido parte del rodaje de Javier Sánchez Salas hasta convertirse, hace más de tres años, en el CISO de HAYA Real Estate, servicer de referencia en España multicliente e independiente que gestiona la totalidad del ciclo inmobiliario, desde que se origina la deuda hasta la comercialización de los inmuebles. Tiene este directivo las ideas claras cuando asegura que la pandemia ha terminado por demostrar que el perímetro de seguridad no existe, que hay que hacerse fuerte contra el cloud, que la seguridad es una necesidad, que tenemos que ir a por DevSecOps con todas nuestras fuerzas y que hay que tener cifrado todo lo que se pueda.

Texto: Rosalía Arroyo
Fotos: Ania Lewandowska

Hace tiempo que los responsables de ciberseguridad han tomado más relevancia en sus empresas. Más ataques y más sofisticados, normativas con sanciones y falta de personal les colocan en primera línea de batalla y cada vez más cerca de la dirección. Dice Javier Sánchez Salas que la seguridad “está dejando de ser un lujo para ser una necesidad”, que aún falta tiempo para que se convierta en una prioridad dentro de las empresas, y que el salto no se producirá hasta que no se entienda la ciberseguridad y los medios de control “como algo que está ligado al beneficio del negocio o a la no pérdida”.

Dice también el responsable de ciberseguridad de HAYA Real Estate que hace tiempo que los CISOs

"Yo no dormiría tranquilo sin poder supervisar mi gestión de la ciberseguridad en el mundo cloud"

saben adaptarse a los riesgos que se les presentan y que la pandemia sanitaria les ha obligado a actuar de forma rápida para ofrecer la disponibilidad adecuada de todos los servicios; "somos ciberresilientes desde hace mucho tiempo", asegura. La pandemia no ha hecho sino demostrar, para aquellos que se hubieran empeñado en no creerlo, que el perímetro de seguridad de la empresa no es el perímetro de la oficina; "tenemos que ir pensando que los perímetros son más amplios o globales, y con el mundo cloud más".

En cuanto a los directores generales, la pandemia les ha servido… "para darse cuenta de esa transformación digital, organizativa; al final las oficinas ya no existen como tal, cualquier empleado puede trabajar en cualquier sitio y eso tiene su parte buena, porque al final somos más competitivos y tenemos más capacidad para trabajar, pero también tiene sus riesgos. Nada crítico, nada grave, solo hay que establecer una política de riesgos en función de estas nuevas formas de trabajar".

Esta nueva forma de trabajar, desde fuera de la oficina, ya se empezaba a hacer en HAYA Real Estate de forma gradual antes de la pandemia, "por lo tanto, el cambiar de modo oficina a modo teletrabajo para toda la compañía no ha sido un impacto grande, salvo el tener que duplicar temas de VPN para que tuviéramos más espectro, pero por lo demás, ha sido un caso de éxito", asegura Javier Sánchez Salas. Explica el directivo que "llevamos mucho tiempo formando a los empleados por temas de continuidad de negocio, por si hay un desastre" y que durante todo este tiempo no ha habido más

"En un proveedor de servicios busco que esté conmigo, que me acompañe. Eso es lo primero"

incidencias que las del día a día habitual; “no hemos tenido ninguna crisis reseñable”.

Sí que se han reforzado los mensajes de concienciación a los empleados, que en ocasiones y según algunos informes, han bajado la guardia con el teletrabajo. “El tema de la concienciación de la seguridad lo estábamos haciendo desde hace tiempo, pero no obstante mandamos un decálogo de medidas de seguridad al uso para recordarlo”.

La pérdida del perímetro de seguridad empezó con los portátiles, siguió con las tabletas y los móviles, y se aceleró con el cloud. ¿Cómo se aborda la adopción del cloud teniendo en cuenta la seguridad? “El cloud es algo que ya tenemos encima y lo que tenemos que hacer simplemente es establecer qué se puede hacer, qué no se puede, y controlarlo. Simplemente es eso. Hay que controlar”, asegura Javier Sánchez, explicando que igual que antes se establecían controles sobre el mundo no cloud, hay que adaptar esos controles para mitigar todo el riesgo que se tenga en el mundo cloud.

Dice también el CISO de HAYA Real Estate que “tenemos que hacernos fuertes contra el cloud. Es decir, que tenemos que apoyarnos sobre todo para que en este mundo cloud, que ya es una realidad presente, esté suficientemente controlado o con los controles necesarios para que cualquier empresa que se vaya a la nube tenga la garantía de seguridad, igual que la disponibilidad, que es lo que te ofrece cloud per sé”.

En el cloud, ¿se tiene en cuenta el modelo de responsabilidad compartido? “Cuando las empresas van a cloud están dando por hecho algunas cosas que no son realidad en materia de seguridad”, asegura Javier Sánchez Salas, añadiendo que le parece correcto ese modelo de seguridad compartido ya que

las empresas deben establecer sus propios controles para saber lo que está pasando en todo momento; “yo no dormiría tranquilo sin poder supervisar mi gestión de la ciberseguridad en el mundo cloud”.

Servicios, una apuesta segura

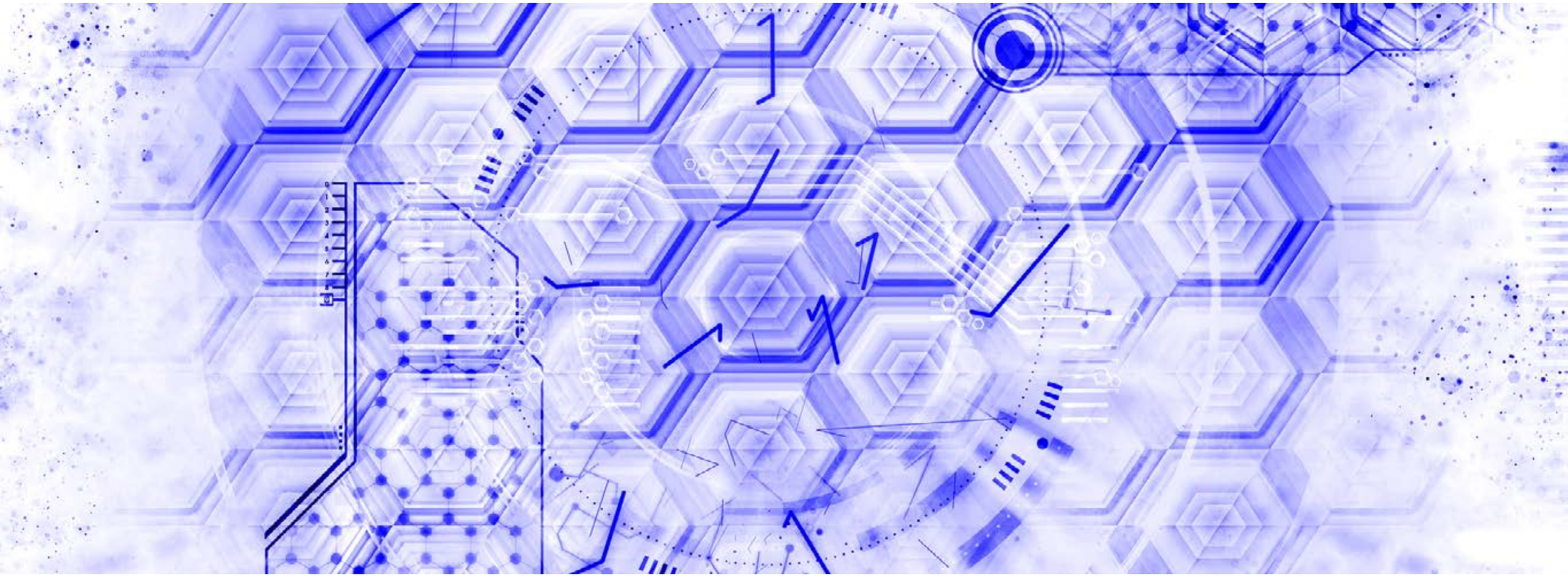
Decíamos que cada vez hay más ataques y que son más sofisticados, que las amenazas se multiplican, igual que los vectores de ataque. Añadimos que hay falta de profesionales de seguridad. Un cóctel explosivo que dejaría a las empresas desprotegidas si no fuera por los servicios de seguridad gestionados. ¿Os están salvando la vida? “Sí. Porque nos dan la ventaja de poder hacer ciertas acciones sin tener recursos físicos en la empresa. Si yo, por ejemplo, me meto en un proyecto de SIEM y tengo que dominarlo, gestionarlo, administrarlo, tengo que crear las reglas… no llego. Me tengo que apoyar en los servicios de seguridad gestionados”.

Asegura también Javier Sánchez Salas que no hay que olvidar que los servicios de seguridad gestionados son de expertos que no sólo ayudan, sino que dan el feedback de las tendencias del mercado, y añade que, lo mismo que ocurre con el cloud, no por externalizar una parte de la seguridad significa que tengas que olvidarte, “hay que estar encima para saber lo que hay”.

A la hora de escoger fabricantes hay un buen puñado de opciones, cuando hablamos de servicios también hay que saber elegir. ¿En qué se fija Javier Sánchez Salas? “Yo lo que busco es un servicio en el que no me traten como un número más. Al final intento ir a un servicio que esté conmigo, que me acompañe. Eso es lo primero”.

De los servicios gestionados de seguridad, un mercado que pasará de los 31.600 millones de dólares en 2020 a 46.400 millones en 2025, según datos de MarketsandMarkets, pasamos a hablar de normativas y cómo hacer frente a tanta regulación: “Con cuidado, intentando entenderlas muy bien, sobre todo las que tienen sanción”, dice el responsable de ciberseguridad de HAYA Real Estate. Añade

"La normativa no es una idea feliz del CISO. Está en el mercado y que hay que invertir, tanto desde el punto de vista económico como de esfuerzo, para adaptarse a ella"



que entre las labores del responsable de ciberseguridad está la de hacer entender a la parte de negocio que la normativa “no es una idea feliz del CISO”, sino que está en el mercado y que hay que invertir, tanto desde el punto de vista económico como de esfuerzo, para adaptarse a ella.

Para Javier Sánchez Salas, “las últimas normativas ayudan. GDPR nos ayudó en muchas cosas, a avanzar en muchos proyectos y las próximas espero que sean un refuerzo para el mundo de la seguridad”.

"El cloud es algo que ya tenemos encima y lo que tenemos que hacer simplemente es establecer qué se puede hacer, qué no se puede, y controlarlo"

Los imprescindibles de Javier Sánchez

“Tener cifrado todo lo que se pueda. Eso para empezar”, dice Javier Sánchez Salas cuando le preguntamos qué tecnologías de seguridad nombraría como imprescindibles. No menciona de manera explícita la seguridad perimetral (firewalls, IPS, IDS…) porque considera que es algo que se sobrentiende que se tiene que tener.

“Y algo a lo que creo que tenemos que ir todos, y los que no se hayan adaptado se tienen que adaptar, es el mundo del DevSecOps. Tenemos que ir a

Enlaces de interés...

- 'Está demostrado que cada vez que invier-tes 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 Sán-chez, Sanitas)

por DevSecOps con toda nuestra fuerza porque es adelantarnos a las vulnerabilidades antes de que salga el producto. Si tuviera que apostar por algo ahora sería DevSecOps; nos ahorraríamos mucho tiempo, mucho dinero y muchos esfuerzos", asegu-ra con rotundidad el responsable de ciberseguridad de Haya Real Estate.

Finalizamos la entrevista hablando de aquello que hay que mirar de cerca para protegerse de las ciberamenazas. Parece fácil: los riesgos. Pero no lo es tanto. Por eso, dice Javier Sánchez, en el mundo que nos movemos, donde cada vez hay más desa-rrollo, y los desarrollos van mucho más rápidos que hace diez años, que eran proyectos eternos, De-vSecOps es tan importante.

Si el objetivo de DevOps fue acelerar el lanza-miento del software sin afectar negativamente la calidad de los productos, con DevSecOps se aña-dió la seguridad a la ecuación. DevSecOps signi-fica que Desarrollo, Operaciones y Seguridad se convierten en una sola cosa y que la función de seguridad estará presente en una etapa temprana del proceso de desarrollo. De hecho, con la cre-ciente complejidad de los ciberataques y la rapidez con la que pueden comprometer todo un negocio con daños a menudo irreparables en términos de mala reputación, la necesidad actual no es solo tener un código de alta calidad, sino que también debe ser seguro y protegido por una arquitectura fuerte.

Con DevSecOps, asegura el CISO de HAYA Real Estate, consigues que los desarrolladores se preo-cupen de que toda la seguridad esté bien desde el inicio del proyecto. Con DevSecOps, "todos vamos a vivir mucho más felices y vamos a dormir mejor", concluye Javier Sánchez Salas.

Compartir en RRSS

La aniquilación del ransomware

No permitas que un ransomware paralice tu negocio.

Splunk, más allá del SIEM

“El machine learning es lo que nos hace diferentes”

(Marco Blanco)

Splunk proporciona software de inteligencia operativa que supervisa, informa y analiza los datos de la máquina en tiempo real. La definición es de Crunchbase y es muy similar a la de Owler: Splunk es una plataforma de software como servicio para buscar, monitorizar y analizar macrodatos generados por máquinas a través de una interfaz de estilo web. Añade también esta web que la sede de la compañía está en San Francisco, que genera más de 500 dólares por empleado, ha recaudado casi 270 millones de dólares en fondos y su adquisición más reciente fue la de Omnition en septiembre de 2019.

Rosalía Arroyo

Splunk no es una compañía de seguridad, aunque “es verdad que aquí en España el reconocimiento de la compañía en el mercado de seguridad es más claro que en otros países”, dice Marco Blanco, AVP & Country Manager para España y Portugal, desde el pasado mes de julio. Añade que

"Splunk no es una compañía de seguridad, aunque es verdad que aquí en España el reconocimiento de la compañía en este mercado es más claro que en otros países"

"si bien en seguridad se están haciendo muchas cosas, también se están haciendo otras en otros mercados".

Y es que, al menos en España, hablar de Splunk es hablar de SIEM, que en su sentido más simple lo que ofrece es una herramienta de gestión de datos desestructurados. Explica Marco Blanco que la misión original de la compañía era escuchar a las máquinas para sacar valor del machine data, de la información que generan las máquinas; "podemos ingerirla, inyectarla y analizarla, y gracias al machine learning y la inteligencia artificial, encontrar el valor que hay en los datos que se generan". El hecho de que "las máquinas que hablan de manera más vehemente, las máquinas más charlatanas son precisamente los dispositivos de seguridad" ha convertido el mundo SIEM en el uso perfecto de la tecnología de Splunk.

La capacidad de ingesta de la plataforma de Splunk en el análisis de la información en tiempo real permite que el caso de uso SIEM sea muchísimo más avanzado "y más teniendo en cuenta que los SIEM tradicionales requerían de muchísima más intervención manual, más configuración". El hecho de que los ciberataques sean muchísimo más cambiantes y más dinámicos hace que contar con una herramienta de machine learning que ayude con la parte de correlación de elementos de seguridad hace que sea absolutamente diferente.

Y sobre la seguridad, explica el directivo, se han ido incorporando una serie de ofertas premium que permiten complementar qué es lo que hace la compañía, como por ejemplo la orquestación de la remediación una vez que tenemos eventos de seguridad.

Cloud

Según Gartner, se espera que el gasto global en la nube pública aumente un 6% a partir de 2019 para alcanzar unos 258.000 millones de dólares, y luego vuelva a aumentos porcentuales de dos dígitos en 2021 y 2022, momento en el que la consultora prevé que el gasto global en la nube supere los 364.000 millones de dólares.

Las empresas migran al cloud y eso conlleva algunos desafíos importantes, algunos en torno a la gestión de sus aplicaciones, "por eso hemos complementado nuestra plataforma de gestión de datos con capacidades de observability". Esta observabilidad va más allá de la monitorización

it whitepapers

¿ESTÁS PREPARADO
PARA LA ERA DE LOS DATOS?

Aproximadamente un cuarto de siglo de transformación digital nos ha traído hasta la era de los datos. Este informe se centra en los desafíos y oportunidades ante los que las organizaciones deben prepararse para tener éxito en la era de los datos.

tradicional porque es capaz de dar sentido al comportamiento impredecible de los sistemas modernos y resolver los problemas más rápido.

Esas capacidades de Observability a las que hace referencia Marco Blanco "permite gestionar la calidad del servicio de las aplicaciones críticas desplegadas en la nube en tiempo real, algo que siempre ha sido un desafío para aquellas aplicaciones. ¿Por qué ha sido un desafío? Porque las aplicaciones, sobre todo las nativas cloud, están basadas en micro servicios, con múltiples dependencias entre ellos y el nivel de complejidad es increíble, por lo cual las herramientas de monitorización tradicional se quedan cortas".

Lo que nos está diciendo el directivo es que Splunk va mucho más allá del SIEM. No sólo menciona los eventos de seguridad, sino los de disponibilidad y también la gestión del rendimiento. "La misma inteligencia artificial que estamos utilizando para la gestión de eventos de seguridad, la estamos aplicando para la gestión de eventos de disponibilidad de las aplicaciones y eso da un tiempo

"La aguja en el pajar que encuentra, Splunk la encuentra de manera automática"

Splunk, algunos datos

Fundada en 2003 por Michael Baum, Erik Swan y Rob Das, el nombre “Splunk” proviene del término inglés que hace referencia a la exploración de cuevas, la espeleología (en inglés, spelunking), ya que se asemeja a lo que hace Splunk: espeleología en los datos del usuario.
Desde su fundación, la compañía ha recaudado 40millones de dólares en cinco rondas de financiación y cotiza en Bolsa desde septiembre de 2019.
Hasta la fecha ha realizado un buen puñado adquisiciones

- **2013 – Septiembre. BugSense**
- **2013 – Diciembre. Cloudmeter**
- **2015 – Junio. Metafor Software**
- **2015 – Julio. Caspida**
- **2017 – Octubre. SignalSense**
- **2017 – Octubre. Rocana**
- **2017 – Mayo. Drastin**
- **2018 – Febrero. Phantom**
- **2018 – Junio. VictorOps**
- **2018 – Agosto. KryptonCloud**
- **2019 – Septiembre. Omnition**
- **2019 – Octubre. SignalFx**
- **2019 – Noviembre. Streamlio**

de recuperación muchísimo más rápido, incluso una reducción de incidentes, tanto de seguridad como de disponibilidad”, explica Marco Blanco asegurando que la oferta es muy completa y que “nuestro desafío ahora es explicarlo adecuadamente a aquellos clientes que ya nos conocen por lo diferenciales que somos en la parte de seguridad. Hablarles también de la parte de observabilidad y gestión de servicios IT”.

Clientes

Sobre los clientes, no se limita Splunk a las grandes cuentas. “En realidad el caso de uso de la inteligencia artificial y Machine Learning lo que permite es que cualquier tipo de cuenta pueda aprovechar el valor de sus datos. Es lo que convierte de manera más diferencial la eficiencia que se puede tener a la hora de proteger de seguridad o a la hora de gestionar adecuadamente los datos de disponibilidad de los servicios o incluso hacer Big Data o Business Insight para saber cuáles son los servicios de negocio que funcionan mejor”.

Añade que hay ciertas soluciones de seguridad que parece que solamente están disponibles para grandes empresas que tienen grandes departamentos de IT o de seguridad para poder explotar esa tecnología más avanzada, “cuando en realidad nosotros precisamente ese es el problema que estamos resolviendo; cuanta más escala pues más visibilidad o más riesgos. Pero por otro lado, empresas de tamaño medio pueden aprovechar

> "En realidad el caso de uso de la inteligencia artificial y Machine Learning lo que permite es que cualquier tipo de cuenta pueda aprovechar el valor de sus datos"

o pueden tener la misma calidad de seguridad o el misma nivel de seguridad, o el mismo nivel de gestión de servicios, o incluso el mismo nivel de analítica de datos para prestar mejores servicios gracias a que la plataforma de Splunk permite hacer eso de manera eficiente". ¿Y cómo hace esto de manera eficiente? "Pues básicamente porque funciona de manera automática. La aguja en el pajar que encuentra, la encuentra de manera automática".

El concepto Data to Everything de la compañía se aplica a una plataforma capaz de ingerir "cualquier tipo de datos, de cualquier estructura en cualquier escala temporal, ya sea en breves segundos porque está ocurriendo algo muy específico, como podría ser un ataque de seguridad, o bien analizado a lo largo del tiempo para ser tendencias de negocio de los últimos meses o incluso de los últimos años".

> "Las máquinas que hablan de manera más vehemente, las máquinas más charlatanas son precisamente los dispositivos de seguridad"

Además del Data to Everything, la compañía tiene a gala hablar de 'Put your data into doing', o pon tus datos a trabajar. Explica Blanco que las empresas tienen un montón de datos disponibles pero no son capaces de sacarles valor, de ponerlos a trabajar para el negocio o para la seguridad "porque no tienen la capacidad de procesarlos debido a que son demasiado complejos o no tienen los suficientes recursos a nivel de personal. Por eso esta solución es perfecta no solamente para empresas tremendamente grandes, sino yo

diría justo lo contrario, para empresas que quieren acceder a esa capacidad de servicio pero que no tienen departamentos de IT".

Diferencial

Cuando Splunk arranca escuchando a las máquinas hace diez años se desarrollan una serie de patentes y una plataforma unificada de categoría empresarial que "proporciona la plataforma de datos para todo (IT, seguridad, DevOps y procesos de negocio) que permite monitorizar, investigar, analizar y actuar sobre datos de cualquier estructura, origen y escala temporal", dice el directivo. Según datos de la compañía, algunos de los clientes de Splunk han reducido un 90% el tiempo de detección y respuesta frente a incidentes, con una reducción de riesgo del 70% de fugas de datos, propiedad intelectual o fraude.

En definitiva, "al final el valor diferencial que tenemos desde Splunk es que nosotros permitimos a cualquier organización de cualquier tipo y de cualquier escala, ya sean grandes o pequeñas, movilizar sus datos de una manera tremendamente sencilla y obtener el valor de esos datos de manera muy rápida", dice Marco Blanco.

Ecosistema de canal

Splunk cuenta actualmente con un mayorista en España, Arrow, "que nos ayuda con la distribución de nuestra solución dentro de nuestro mercado".

Explica el directivo de Splunk que el programa de canal está basado en la especialización que permite posicionar la tecnología adecuadamente. Pero también quieren un canal experto en el cliente, "que entiendan cuáles son las dificultades que están pasando ahora mismo las organizaciones y que puedan hacer una conexión entre esas dificultades y la propuesta que tenemos".

Data Report

Encontramos una serie de desafíos más importantes que tienen los siguientes y luego, por otro lado, hacemos también una serie de recomendaciones, son cinco recomendaciones: Poner todos los datos a funcionar, Construir una estrategia de datos basada en la estrategia de negocios; Convertir la seguridad en un principio fundamental; no trabajar exclusivamente en parcelita pequeñita; y convertir a todo el mundo en un científico de datos. Es decir, en el mundo actual con el tema del machine learning inteligencia artificial al final resulta que necesitas un ejército de personas súper bien formadas para sacar partido a los datos, y eso se ve clarísimamente en el caso de uso de seguridad: puedes tener las mejores herramientas, pero si no tienes al listo detrás, sufres. Sin embargo, con la parte de machine learning, realmente eso es a lo que ayudamos, a que cualquiera pueda convertirse en un científico de datos o puede hacer este tipo de gestión. Y eso es lo que publicamos en este reporte.

Enlaces de interés...

- Siete tendencias de SIEM que tener en cuenta 2020
- Splunk compra SignalFx para mejorar la monitorización del cloud

Compartir en RRSS

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

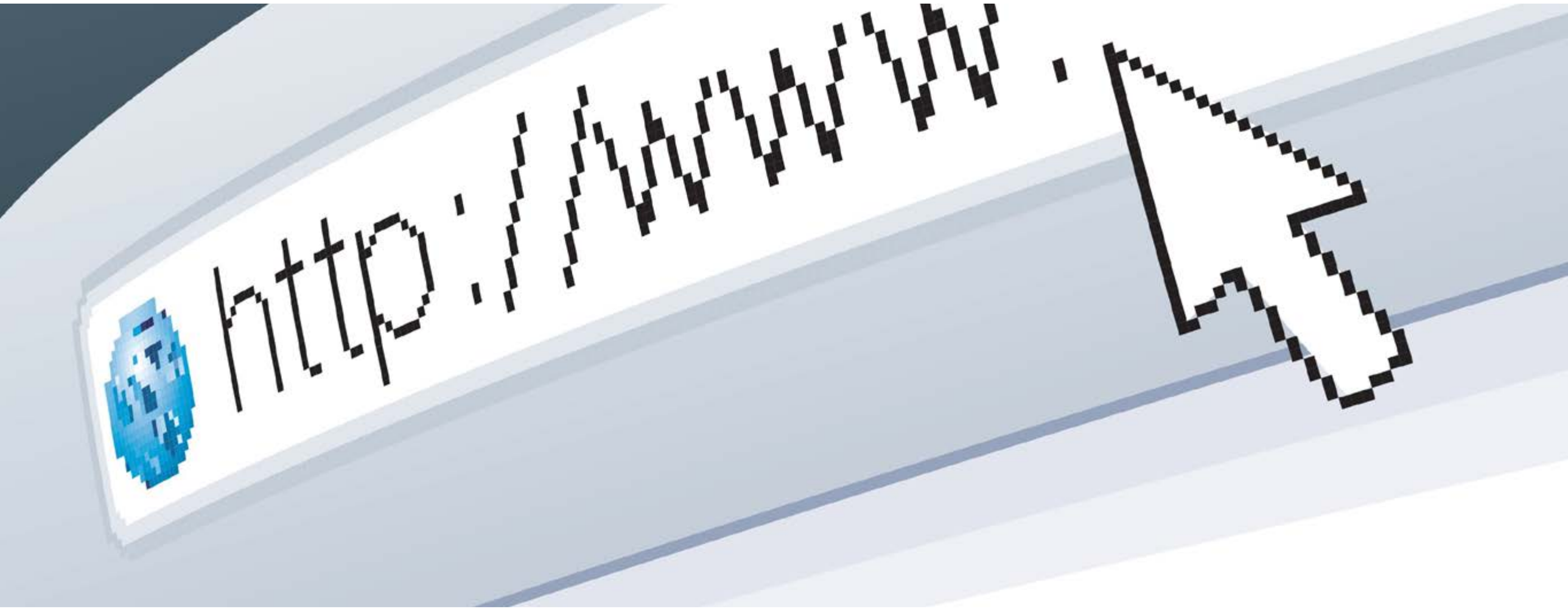
La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

¿Cómo mantener la seguridad en un mundo inundado por las cookies?



Las cookies son la información que las páginas de Internet recopilan de sus usuarios para conocerlos mejor y poder así ofrecer publicidad dirigida. Los CISO tienen que saber proteger esa información para no enfrentar multas. Pero hay empresas que quieren alternativas a las cookies.

Bárbara Bécares

Octubre 2020

Cada vez que accedes a cualquier web, te encuentras con ese famoso recuadro que te recuerda que se van a almacenar tus cookies y debes aceptarlo. Puedes no hacerlo, pero en ese caso, si no se aceptan las cookies, en algunas páginas es probable que no puedas navegar con total normalidad o acceder a cierta información. Para las empresas, almacenar esta información es esencial para conocer mejor el perfil de sus lectores o clientes potenciales.

Pero mantener esos datos seguros es un tema crucial, más ahora que hay nuevos criterios al respecto dictados por el Comité Europeo de Protección de Datos en mayo de este año y que tendrán que estar implementados antes del próximo 31 de octubre. En este artículo se ofrece una guía para conocer mejor para qué sirven las cookies y cómo proteger esta inmensa información.

Si una empresa sufre un robo de estas informaciones o recoge cookies sin el procedimiento adecuado, según la normativa, puede enfrentarse a multas. De hecho, firmas como Vueling se han enfrentado a multas. No son realmente altas estas sanciones, si hablamos de empresas grandes y multinacionales, pero para una pequeña empresa una multa de varios miles de euros puede suponer un gran problema. Además, como siempre pasa cuando hablamos de seguridad informática y de empresas, un problema de este tipo afecta a la reputación de la marca.

"Toda persona tiene derecho a la protección de los datos de carácter personal" y que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada"

Carta de Derechos Fundamentales de la Unión Europea

¿Qué son las cookies y para qué sirven?

Como explican desde el navegador Mozilla de Firefox, una cookie es un archivo creado por un sitio de Internet para almacenar información en el equipo. Por ejemplo, las preferencias de las personas que están visitando ese sitio. Las cookies a menudo guardan la configuración de los sitios web de la persona que está visitando la página, como el idioma preferido o la ubicación. Cuando un usuario accede de nuevo a esa web, el navegador envía de nuevo

las cookies que le pertenecen, lo que le permite que el internauta acceda a información personalizada en función de sus necesidades.

Las cookies también pueden guardar información que identifica a cada usuario personalmente como puede ser el nombre, correo electrónico, domicilio, domicilio de tu puesto de trabajo o número de teléfono. Sin embargo, un sitio web solo tiene acceso a la información personal que tú le proporcionas.

Como explica Javier Megias, emprendedor, “su utilidad es que la web sea capaz de recordar su visita cuando vuelva a navegar por esa página. Las cookies suelen almacenar información de carácter técnico, preferencias personales, personalización de contenidos, estadísticas de uso, enlaces a redes sociales, acceso a cuentas de usuario, etc. El objetivo de la cookie es adaptar el contenido de la web a su perfil y necesidades”.

Todo esto se traduce a que las empresas manejan grandes cantidades de datos de personas que visitan sus páginas de Internet y tienen que guardarlos con cuidado por respeto a la privacidad de las personas y para ahorrarse problemas con la ley.

Para una empresa, la recopilación de estos datos es muy importante. A la hora de ofrecer anuncios, si estos son personalizados de acuerdo a la información obtenida previamente gracias a las cookies, hay más probabilidad de acertar con el producto o servicio que se ofrece. Y más probabilidades de que ese usuario quiera consumir lo que se le anuncia.

Aunque no todas estas informaciones son tan necesarias, de acuerdo con expertos. Sergio Maldonado, CEO de PrivacyCloud explica que “nuestra recomendación es la eliminación completa de cookies “de terceros” (aquellas que no hemos creado nosotros mismos). Con ella desaparecerá la necesidad de recabar un consentimiento que no llega nunca a serlo de verdad (puesto que nadie entiende la pregunta, para empezar) y que molesta innecesariamente al usuario”. Maldonado recuerda que los usuarios se cansan de estos pop-up que aparecen al acceder a cada página y eso lleva a que “el consentimiento no es realmente informado o inequívoco (como exige la ley) porque la gente solo se busca quitarlo de en medio. Y porque en ocasiones no

se sabe siquiera qué empresas recibirán los datos en el momento de aceptarse la cesión (caso de los medios digitales)".

Cabe decir que esta firma aboga por eliminar las cookies no exentas para facilitar el uso de Internet, tanto para usuarios, como para empresas que recogen los datos.

Nuevos criterios europeos que un CISO no puede perder de vista

Los directivos que se encargan de la seguridad de la información de empresas y organismos no pueden perder de vista las cookies y la regulación que rodea su gestión. Por ello es importante recordar que la Agencia Española de Protección de Datos, o AEPD, lanzó una nueva versión de su guía sobre manejo de cookies, para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos. El hecho de no cumplir estas normas puede llevar a altas multas.

Por su parte Marcos Gómez, del Instituto Nacional de Ciberseguridad (INCIBE), explica que los CISO son expertos en ciberseguridad que desempeñan un rol crítico dentro de las compañías y "son los que se encargan del mayor activo de la organización, que es la información". Por ello, para un CISO es importante conocer el mundo cookie.

Este documento permite entender mejor qué son y qué tipos de cookies existen según diferentes variables. Un cambio fundamental que hay que tener en cuenta es que el Comité Europeo de Protección de Datos considera que la opción de "seguir navegando" no constituye una forma válida de prestar el consentimiento, en la medida en que tales acciones pueden ser difíciles de distinguir de otras actividades o interacciones del usuario, por lo que no sería posible entender que el consentimiento es inequívoco, tal y como ya publicó IT Digital Security.

Estas normas persiguen el objetivo de crear un marco legal para dar algo de protección al usuario;

"El consentimiento no es realmente informado o inequívoco (como exige la ley) porque la gente solo busca quitarlo de en medio. Y porque en ocasiones no se sabe siquiera qué empresas recibirán los datos en el momento de aceptarse la cesión (caso de los medios digitales)"

Sergio Maldonado, CEO, PrivacyCloud

La Agencia Española de Protección de Datos, o AEPD, lanzó una nueva versión de su guía sobre manejo de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos. El hecho de no cumplir estas normas puede llevar a altas multas.

"toda persona tiene derecho a la protección de los datos de carácter personal" y que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada", tal y como dice el texto de la Carta de Derechos Fundamentales de la Unión Europea.

De acuerdo con la empresa Cookiebot, "la ley europea de cookies no sólo tiene que ver con las cookies, sino también con cómo se puede fortalecer la privacidad del usuario a gran escala en la red. Un ejemplo de lo anterior es la prohibición de utilizar las direcciones de correo para propósitos de marketing sin el consentimiento previo".

¿Qué pasos debería una empresa o emprendedor llevar a cabo a la hora de crear una página web en la que vaya a recoger las cookies de los usuarios?

Recuerda el directivo de PrivacyCloud, Sergio Maldonado que, para aquellas empresas o emprendedores que creen una web en la que vayan a recopilar las cookies, existe la Guía de la Agencia Española de Protección de Datos (Guía de Cookies, actualizada en 2020) que "es un buen comienzo" para comprender cómo actuar. Uno de los asuntos clave que cualquier empresa o emprendedor debe tener en cuenta desde ahora es que seguir haciendo un uso ordinario de un sitio web, es decir, continuar navegando, no es una conducta de la que se pueda servir para asumir el usuario acepta el uso de 'cookies', por lo que "no es una forma lícita de obtener el consentimiento", como ya publicó IT Digital Security.

Además, el documento centra su atención en dos novedades relevantes que atañen a la libertad del consentimiento y a su manifestación inequívoca. Son las "cookie walls" y el 'scroll'. Las "cookie walls" o el 'muro de cookies' (la ventana que bloquea el contenido hasta que el usuario no acepta las cookies cuando no acepta las cookies) son ilegales.

Enlaces de interés...

- Cambios en el uso de las 'cookies' que hay que implementar antes del 31 de octubre
- Novedades en las formas de obtención de consentimiento mediante las 'cookies'
- Cookiethief, el troyano que roba cookies de navegadores y redes sociales

En este punto, el CEPD explica que, para que el consentimiento sea una manifestación de voluntad libre, el acceso a los servicios y funcionalidades no puede estar condicionado a aceptación de las cookies a través de una "cookie wall" de forma que se obligue al usuario a aceptarlas para acceder a los servicios, funcionalidades o contenidos.

Hay que recordar que hay ataques dirigidos a estas cookies. En el mes de marzo, especialistas de la firma de seguridad Kaspersky alertaban sobre dos nuevas variantes de malware para Android que, al combinarse, pueden robar las cookies recogidas por el navegador y las aplicaciones de redes sociales más populares. El peligro residía en que los ciberdelincuentes controlaban la cuenta de la víctima de forma discreta y pueden enviar contenido malicioso.

¿Hay alternativas a las cookies?

Para la empresa PrivacyCloud, las cookies podrían ser reemplazadas por otros sistemas más eficientes de marketing. Explica Sergio Maldonado que la AEPD da un plazo de cortesía hasta el 31 de octubre para adecuar las web y sistemas a la nueva normativa de cookies. Pero el directivo se pregunta si no será mejor "empezar a explorar alternativas de monetización que no dependan de un mercado tan intermediado, fraudulento, opaco y alejado de todos los principios de Privacidad desde el diseño, transparencia, control y centralidad en el cliente".

Muchas son las empresas que piensan similar a PrivacyCloud. Por ejemplo, a principios de este año 2020 Google anunció el fin de los cookies de terceros en su navegador Chrome y planteó una alternativa, llamada los tokens de confianza. Estos pueden autenticar a un usuario sin desvelar su identidad, lo que les permite ofrecer publicidad ajustada.

Por su parte, Jordan Mitchell, vicepresidente sénior de operaciones de IAB Tech Lab, opina que "se avecina una tormenta perfecta de problemas de privacidad. Estamos experimentando la proliferación de dispositivos personales conectados que generan una gran cantidad de datos personales, con un potencial creciente de mal uso. El status quo, compuesto por cientos de cookies, identificadores y rastreadores fragmentados, sin controles de privacidad del consumidor estandarizados, es insostenible". Esta firma también apuesta por esos tokens que mejoran el reconocimiento del usuario y la personalización mientras contribuye a proteger su privacidad.

Compartir en RRSS

Secure&IT by LKS
www.secureit.es

CIBERSEGURIDAD EN LA DESESCALADA DE LA COVID-19

& Promoción especial
Auditorías y seguridad gestionada

& Privacidad vs. COVID-19
¿Qué medidas de contención pueden implementar las empresas?

& Adecuación a la normativa e-commerce
¿Cómo adaptar una web para vender de forma online?

+ INFO

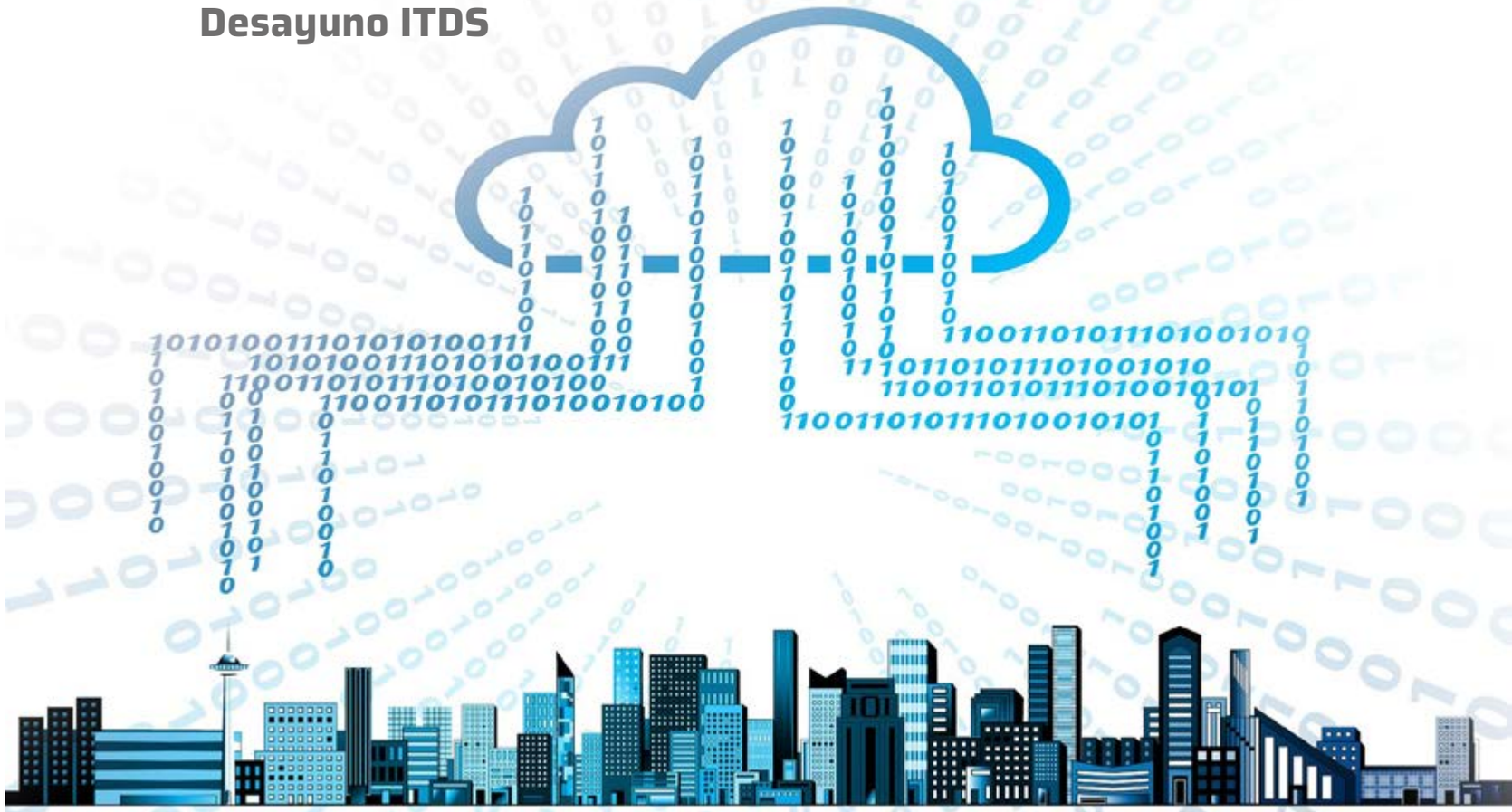
Ayúdanos a conocer la realidad digital

COVID-19,
¿cuánto y cómo ha influido en las estrategias de TI?

¡PARTICIPA!

en nuestra Encuesta

Se calcula que el 84% de las empresas ejecuta una estrategia multicloud, una tendencia que se ha consolidado en los últimos años y cuyo mayor atractivo es la flexibilidad. Las empresas implementan cargas de trabajo en diferentes plataformas cloud en función de las necesidades de costos y aplicaciones y además protegen las operaciones comerciales al reducir el tiempo de inactividad y mejorar la capacidad de recuperación en caso de interrupción o incumplimiento de la carga de trabajo (como un ataque DDoS).



La seguridad de los entornos multicloud

Sin embargo, la mayor complejidad de un entorno multicloud aumenta exponencialmente la superficie de ataque y el nivel de riesgo de una organización. De ello hablaremos en uno de nuestros #DesayunosITDS con Alfonso Martínez, Country Manager de Thales Data Protection; Santiago Urbano, Product Marketing Manager de S21sec; Sergio Martínez, Iberia Regional Manager de SonicWall y José de la Cruz, Director Técnico de Trend Micro Iberia

Arrancamos el debate planteando cuáles son las ventajas que ofrece el adoptar una estrategia multicloud. Asegura Alfonso Martínez que ya no hay

Compartir en RRSS

"Una de las piedras angulares de la seguridad en entornos híbridos es la visibilidad y el control"

Sergio Martínez, Iberia Regional Manager, SonicWall

tamaño ni vertical idóneo para la nube y que lo más importante de una estrategia híbrida es "el reducir la vulnerabilidad", al tener todo en un mismo proveedor. Para Sergio Martínez gracias a los entornos cloud "hemos podido mantener el nivel de trabajo". La realidad es que tenemos todos nuestros datos y aplicaciones distribuidos en múltiples cloud y hay que adecuarse a ello.

La diversificación es, para José de la Cruz, la gran ventaja de una estrategia multicloud. Asegura que además de multicloud se mantienen los entornos on-premise y por tanto hay que hablar de modelos híbridos pero que existe un pequeño porcentaje, sobretodo en empresas de reciente creación que han adoptado sobretodo el modelo DevOps directamente y que están trabajando ya puramente en nube.

El aumento de la superficie de exposición es uno de los grandes riesgos cuando adoptamos estrategias multicloud, asegura durante el debate Santiago Urbano. El responsable de marketing de producto de S21sec menciona como ventaja de una estrategia multicloud el que cada proveedor tiene sus propias herramientas de seguridad y eso permite "aprovechar distintas capacidades de seguridad de los distintos proveedores de Cloud".

Retos de adoptar una estrategia multicloud

"Los retos a los que se enfrentan las empresas con esta distribución de las cargas son muy variados", asegura el director general de SonicWall en España y Portugal. Menciona el phishing targueteado porque el email sigue siendo el vector número uno de

infección “y hay que protegerlo de forma adecuada”; habla también del robo de credenciales, que son “la joya de la corona”; el tercer reto es la seguridad de los datos, a los que hay que dar una protección adecuada. “A todo esto hay que sumar el malware, los ataques de ingeniería social y las fugas de información”, añade el directivo.

En Trend Micro se identifican tres retos, dice su director técnico. “En primer lugar hablaríamos de la visibilidad”, asegura, porque cuando trabajas en un entorno híbrido y tan heterogéneo, pues al final pierdes el foco o pierdes la visibilidad de lo que está ocurriendo. En segundo lugar habla de cumplimiento normativo, “fundamental en cualquier organización y más importante cuando estamos hablando en un entorno cloud multi”. El último factor, “que también es muy, muy importante, es la responsabilidad”, que en el mundo de la nube es compartida entre los clientes y los proveedores.

Incide Santiago Urbano en que entender ese modelo de seguridad compartida “es clave”. Dice que la mayoría de los problemas de seguridad de los clientes en el cloud están relacionados con problemas de configuración y que en un entorno multicloud no hay que configurar un entorno, sino varios. “Hay herramientas que nos permiten unificar la visibilidad de varios entornos en el cloud y que para nosotros son prácticamente nuestro día a día de trabajo”, asegura.

“Primero hay que analizar si realmente van a empezar desde cero o van a migrar como hacen la mayoría”, apunta Alfonso Ramírez, añadiendo que en esto de la seguridad compartida el responsable

DESAYUNOS ITDS.
LA SEGURIDAD DE LOS ENTORNOS MULTICLOUD

CLICAR PARA VER EL VÍDEO

último de los datos es el cliente: “Al final del día, si pasa alguna cosa, el responsable de los datos eres tú y sólo tú, señor cliente”. El cifrado de los datos sensibles poniendo foco en la custodia de las claves criptográficas es, en opinión del directivo, la mejor forma de subirse a la nube.

Papel de los proveedores en la orquestación de la seguridad cloud

En ocasiones los proveedores de cloud ofrecen sus propias herramientas de seguridad. No suelen ser herramientas específicas y eso puede desarticular un poco la estrategia de seguridad, o no… Para José de la Cruz son un complemento e insiste en que lo más importante de una solución de seguridad multi cloud es la visibilidad y el control “esos componentes tan necesarios hoy en día en seguridad”.

Asegura en su intervención Santiago Urbano que al final lo que quieren los clientes es una gestión unificada del riesgo y que en este sentido las herramientas propias de cada entorno

pueden ser más adecuadas para distintos tipos de carga de trabajo. Para Alfonso Martínez las soluciones nativas de seguridad en la nube lo que generan son nuevos silos, “con lo cual al final te crea problemas diferentes”. La clave, asegura, es la gestión.

Para Sergio Martínez, es obvio que a todos los fabricantes nos gusta que se utilicen nuestras herramientas de gestión. En todo caso, sea un partner, un MSP, un prestador de soluciones que gestionan la seguridad del cliente como que sea el propio cliente que se gestiona, “es bueno simplificar y tener más visibilidad y control. Una consola que simplifique esta gestión y sea capaz de analizar, detectar y responder en tiempo real a muchas amenazas”.

Mejores prácticas

Establecidos los retos que plantea una estrategia multicloud desde el punto de vista de seguridad, se plantea durante el debate cuáles son las mejores prácticas de seguridad para hacer frente a la seguridad en esos entornos multicloud.

Asegura el portavoz de S21sec que la gestión de identidades es uno de los pilares básicos en los que nos tenemos que basar cuando abordamos la seguridad de un entorno cloud. Añade como buena praxis la automatización de la respuesta así como la visibilidad y monitorización continua.

La gestión de los roles y que la información sensible esté protegida son buenas prácticas para hacer frente a la seguridad de un entorno multicloud, dice el responsable de Thales Data Security. En

"El cumplimiento normativo es fundamental en cualquier organización y más importante cuando estamos hablando en un entorno multi cloud"

José de la Cruz, Director Técnico, Trend Micro Iberia

"Las soluciones nativas de seguridad en la nube lo que generan son nuevos silos, por lo que la clave es la gestión"

Alfonso Martínez, Country Manager, Thales Data Protection

primer lugar hay que saber definir e identificar los roles, que quien accede a ser dato sea quien dice ser, y en segundo lugar mantener la información a salvo mediante una buena propuesta de cifrado que asegure tanto los datos como las claves de cifrado

Hablando de las mejores prácticas de ciberseguridad Sergio Martínez hace un amplio recorrido, empezando por el nivel de red, "donde es obvio que tenemos que tener elementos de protección y detección de malware, y para eso es conveniente desplegar estrategias basadas en firewalls virtuales" que permitan establecer una monitorización continua para controlar y detectar y responder en tiempo real a todo lo que sucede". En un siguiente nivel sería conveniente un control de sesión o incluso de aplicaciones para evitar el robo de credenciales, que se han convertido en el nuevo perímetro.

"Hablamos de que uno de los riesgos era la visibilidad. Por lo tanto, una buena práctica sería implementar mecanismos o sistemas que nos aportarse en esa visibilidad", asegura José de la Cruz, añadiendo que deben implementarse mecanismos o herramientas que sean capaces de gestionar todo el entorno, independientemente de dónde se esté, añadiendo una capa de automatización que nos ayude a implementar unas medidas básicas de seguridad, entre las que destaca el hacer frente a las vulnerabilidades para reducir la superficie de ataque y, como consecuencia una correcta gestión de parches.

Falta de profesionales

Se habla mucho de la falta de profesionales en general en el mundo de la ciberseguridad, y cuando hablamos de la seguridad del cloud, ¿se necesita ser experto en seguridad y además ser experto en cloud? ¿Cómo se hace frente a esta situación? "Yo nunca he creído en el hombre orquesta", dice Alfonso Martínez, y habla de una buena separación de roles dentro de las empresas porque, de esta forma, "tendrás un único punto de fallo"; habla de profesionales dedicados para cada ámbito y que, por supuesto, haya una coordinación".

"Yo también pienso que con Leonardo da Vinci se acabó lo del hombre orquesta", dice Sergio Martínez, añadiendo que es verdad que el enfoque de ciberseguridad tiene que ser integral. Es decir, que el responsable de ciberseguridad de una compañía tiene que tener herramientas que permitan monitorizar y dar visibilidad, y tener control sobre todo lo que sucede en la red y todo tipo de aplicaciones.

Para José de la Cruz la falta de profesionales es algo evidente y que sufren todas las empresas.

A grandes retos, grandes soluciones

Para finalizar el debate pedimos a los expertos en seguridad que hagan sus propuestas para ayudar a las empresas a hacer frente a la seguridad en entornos multicloud.

Trend Micro. La propuesta de Trend Micro para este entorno híbrido se llama Cloud One, una suite de varios productos que pretende dar respuesta completa desde una única consola y desde un único punto de gestión a todas las necesidades de nuestros clientes. Los productos que interactúan y trabajan de manera orquestada empiezan por Workload Security, que nos permite proteger las cargas de trabajo y cualquier tipo de entorno, sea físico o virtual, incluso containers, en tiempo real. Se añade a la suite Container Security, junto con Application Security, que permite proteger, desde el punto de vista de la aplicación, cualquier interacción de esa aplicación con el mundo exterior; File Storage, que ayuda a proteger cualquier interacción de ficheros con sistemas almacenamiento en nube; Cloud One Conformity es la propuesta de Cloud Security Posture Management y Networks Security la parte de la red.

S21sec. Como empresa de servicios, S21sec no tiene productos concretos. Se ofrecen servicios de migración al cloud, aplicando controles de seguridad dentro de las cargas de trabajo que se están migrando en el Cloud, para lo que se cuenta con equipos internos de servicios profesionales certificados en muchas tecnologías de terceros y en los mayores proveedores de nube pública. La compañía cuenta con un equipo de auditoría para revisar la seguridad de la nube haciendo proyectos de pentesting, detección de brechas, etc. El equipo de consultoría ayuda a los clientes en toda la parte de cumplimiento normativo. Los servicios de seguridad gestionada de S21sec se apoyan en un SOC 24/7 multi región y ofrecen una gestión unificada con todos los entornos para poder tener esta visibilidad y esta trazabilidad completa de los distintos sectores de ataque que están afectando a las compañías.

Thales Data Protection. La propuesta de Thales Data Protección para la securización de los entornos multicloud pasa por un Smart Single Sign On para que, dependiendo de quién seas, donde vayas, en qué momento o desde dónde se te pidan un tipo de credenciales u otras más más fuertes. El cifrado es parte también fundamental porque es la primera línea de defensa del propio dato. En este sentido se puede aplicar un Bring Your Own Encryption, un Bring Your Own Key, que nos permite tener un control sobre las claves criptográficas. Insiste la compañía en que hay que poner foco en la custodia de las claves criptográficas, en el ciclo de vida, en el rotado, en saber cuándo son generadas, etcétera.

SonicWall. Empresa veterana en el mundo de la seguridad, conocida en el mundo pyme y con presencia creciente en el mundo Enterprise, SonicWall cuenta con más de tres millones de firewalls distribuidos por todo el mundo que les permite saber lo que está sucediendo en gran parte de las redes de todo el mundo. La protección de los entornos multicloud empieza por los firewalls de la compañía como pieza angular en este mundo sin perímetro, se extiende hacia la seguridad del email, donde se originan más del 90%. Se cuenta también con un CASB que controla todo tipo de aplicaciones en la nube, así como control de credenciales, de fugas de información y de compliance. Destaca una línea de acceso remoto a las redes de una forma inteligente.

Tampoco cree en el concepto del hombre orquesta y menciona el Cloud Center of Excellece, un departamento específicamente diseñado para gestionar el nuevo modelo devopd, el nuevo modelo de cloud, “un departamento multidisciplinar donde está el experto en seguridad, otros son expertos en redes, otros en cloud y que trabajan de manera coordinada para proporcionar la excelencia dentro de ese modelo cloud”. ¿Qué es lo que necesita este grupo? Necesita un único punto de vista que les ayude a simplificar su tarea, incluso que les ayuda a coordinar cómo interactúan los distintos

"La gestión de identidades es uno de los pilares básicos en los que nos tenemos que basar cuando abordamos la seguridad de un entorno cloud"

Santiago Urbano, Product Marketing Manager, S21sec

departamentos y a identificar posibles riesgos relacionados.

Menciona Santiago Urbano la fuga de talento como otro problema asociado al de la falta de profesionales y el coste, tanto económico como de tiempo, que supone para las empresas formar a empleados que son fichados.

SOAR

A lo largo del debate queda claro que se hace necesario sincronizar políticas entre diferentes entornos, saber escoger las herramientas más adecuadas, mantener la visibilidad, el compliance… ¿Es aquí cuando las herramientas de automatización/orquestación son imprescindibles?

"Ya hemos comentado que obviamente una de las piedras angulares de la seguridad en entornos híbridos de este tipo es la visibilidad y el control. Entonces es obvio que si disponemos de múltiples entornos, pues vamos a tener que ir a este tipo de herramientas de automatización y orquestación", dice el responsable de SonicWall para el mercado de Iberia.

Añade José de la Cruz un concepto que cobra cada vez más fuerza: Cloud Security Posture Management que "lo que permite es garantizar que la postura de seguridad de la organización a nivel de cloud se está cumpliendo". Esta postura, explica el director técnico de Trend Micro, se analiza desde tres puntos de vista: cumplimiento normativo, cumplimiento normativo interno y mejores prácticas.

Enlaces de interés...

- Claves para mejorar la seguridad en entornos multicloud
- Los planes de gestión del riesgo en la era multicloud
- Factores a tener en cuenta para blindar los entornos multicloud

Dice el portavoz de S21sec que orquestación y automatización son imprescindibles y que es lo que está haciendo su empresas; "hacemos una automatización a la respuesta y una orquestación completa tanto de los entornos cloud como de los entornos on premise como de los entornos de cloud privada para de esta manera poder dar una detección y una respuesta unificada"

"Obviamente va a ser muy complicado que un único fabricante, un único proveedor, le dé al cliente una única solución para su seguridad en le nube", dice el responsable de Thales Data Protectionen, y menciona que una de las cosas que sí que se pueden hacer es que todos los fabricantes aproximen posturas adoptando, por ejemplo, soluciones de single sign-on adaptativo o que cuando se levante una máquina vaya cifrada por defecto. En todo caso, asegura, "todo lo que sea automatizar la seguridad es imprescindible".

21
OCTUBRE
11:00 CET

REGISTRO

El dato: piedra angular de una experiencia customer-centric

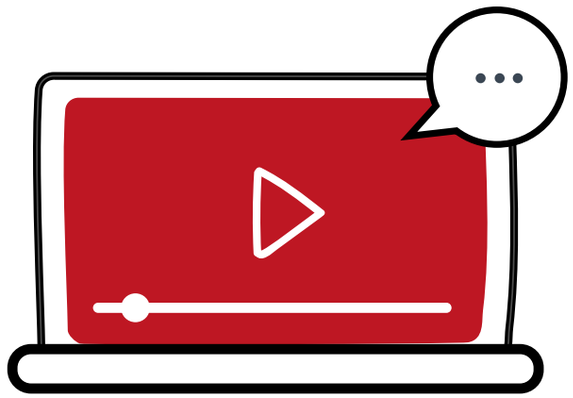
Para crear una experiencia de cliente satisfactoria, se necesita una buena gestión de la información. Los datos generan ingresos, pero no siempre se sabe cómo manejarlos de una manera óptima -en todo su ciclo de vida- y obtener así un resultado exitoso para la empresa.
La tecnología posibilita ofrecer experiencias para crear clientes fieles a nuestros productos. En este webinar reunimos a expertos que te presentarán **5 estrategias y casos prácticos para gestionar los datos de tus usuarios y ofrecerles una experiencia que les deslumbre.**

Trabajo seguro desde cualquier lugar:
Adaptándonos a la “nueva normalidad”

22
OCTUBRE
11:00 CET

REGISTRO

Conforme las empresas planifican distintos escenarios de regreso a la oficina, han de tener en cuenta las nuevas expectativas de los empleados. Muchas compañías están considerando la posibilidad de adoptar una política proactiva de “trabajo seguro en cualquier lugar”. En este #ITWebinars destacaremos qué aspectos del teletrabajo seguro ya se habían aplicado con éxito antes de la cuarentena, y cómo se puede apoyar y potenciar la productividad teniendo en cuenta la salud mental y física de los empleados, así como la privacidad en el entorno personal de los trabajadores mediante soluciones y tecnologías innovadoras.



#ITWEBINARS

Aplicaciones, ¿cómo desarrollo y entrego mi mejor software?

Las aplicaciones necesitan recopilar información de los usuarios (y responderles según su comportamiento), de la empresa, de las cosas que se conectan a Internet...; deben manejar datos de diversa naturaleza, que se alojan en diferentes ubicaciones y plataformas; y están, así mismo, cada vez más automatizadas, exigen un desarrollo continuo, ser seguras, estar monitorizadas y ofrecer un óptimo rendimiento, adaptarse a cualquier tipo de plataforma...

29
OCTUBRE
11:00 CET

REGISTRO

vmworld®
2020

Planteando la base digital para el negocio en un mundo cambiante

vmware®

Planteando la base digital

para el negocio en un mundo cambiante

Pat Gelsinger, Chief Executive Officer de VMware, fue el encargado de dar el pistoletazo de salida de la primera edición virtual de VMworld que se desarrolló del 30 de septiembre hasta el 1 de octubre para mostrar la visión estratégica de la compañía, así como múltiples ejemplos de éxito de sus clientes en un año, este 2020, que el propio Gelsinger definía como extraordinario y retador. Y esta estrategia pasa por proponer la base digital para responder a las necesidades de un mundo impredecible.

PLANTEANDO LA BASE DIGITAL PARA EL NEGOCIO EN UN MUNDO CAMBIANTE

La celebración virtual de VMworld 2020 ha permitido, tal y como explicaba Pat Gelsinger en su mensaje de bienvenida, "estar conectados con más de vosotros". De hecho, las cifras de registrados que manejaba ayer la compañía se situaban por encima de las 120.000 personas, con unas 2.700 desde España. Pero la edición de este año es especial, porque la situación que hemos vivido "está cambiando cualquier tipo de interacción en nuestras vidas", una realidad que exige un profundo cambio que coloca en el centro la innovación digital "donde convergen elementos como aplicaciones, nube y dispositivos, y donde nuestra estrategia pasa por permitir trabajar con cualquier app, en cualquier nube y con cualquier dispositivo", recordaba Pat Gelsinger.

Sobre esta base, Gelsinger ha señalado que VMware quiere seguir siendo "el elemento más innovador de vuestra infraestructura, pero si vemos la VMware de hoy, va más allá de la infraestructura, estamos definiendo las prioridades digitales en todas las áreas del negocio. Nuestra estrategia consiste en proporcionar la base digital para un mundo impredecible".

Para el CEO de VMware, "el core de nuestra estrategia son vuestros negocios, vuestras aplicaciones y vuestros datos", y es que reconocía que en estos meses "he hablado con muchos CEO y CIO y en todos detecté la urgencia de buscar nuevas formas de interactuar con sus clientes para mantener el negocio. La clave para ello es la innovación en el software".

CINCO PIEZAS ESENCIALES PARA LA ESTRATEGIA DE VMWARE

El objetivo de VMware es potenciar el negocio de los clientes, y para ello ha diseñado una estrategia con cinco piezas esenciales: Modernización de las Aplicaciones, Multi-Cloud, Espacio de Trabajo Digital, Virtual Cloud Networking y Seguridad Intrínseca.

Comenzando por la Modernización de las Aplicaciones, hace un año VMware presentaba Tanzu, para crear, ejecutar y modernizar las aplicaciones en cualquier nube mediante con-

¿Quieres descubrir todas las novedades de VMworld 2020?

Accede a los contenidos bajo demanda en este enlace

VMWORLD 2020: SESIÓN GENERAL

tenedores. Ahora, explicaba Gelsinger, "hemos rediseñado vSphere para que Kubernetes sea el componente principal". El que hasta la fecha era el Proyecto Pacific, "ya está disponible, con lo que vSphere es a día de hoy la mejor plataforma para ejecutar apps virtualizadas y en contenedores".

ACUERDO CON NVIDIA: PROYECTO MONTEREY

Pensando en el futuro de las apps, éste está en los datos, y la mejor forma de extraerlos y explotarlos pasa por la Inteligencia Artificial. Son muchos los casos de uso, pero la IA sigue sin estar disponible para todas las empresas, y su adopción empresarial no pasa del 10-15%, de ahí que VMware haya anunciado en esta edición de VMworld una alianza estratégica con Nvidia para llevar la IA a cualquier empresa. La que será la próxima re-arquitectura de vSphere, el Proyecto Monterey, pasa por transferir el sistema operativo del centro de datos a SmartNIC aislando las apps del plano de datos y de control, acelerando el procesamiento de datos y la seguridad del procesamiento, incrementando con ello el rendimiento en el centro de datos.

UNA REALIDAD MULTI-CLOUD

La segunda de las áreas, el entorno multi-cloud, es la plataforma estratégica para desarrollar el negocio, porque permite la innovación aprovechando las fortalezas de los distintos servicios cloud. Pero "es imprescindible que no se creen nuevos silos entre las diferentes nubes y, para ello, VMware Cloud permite ejecutar cualquier app en cualquier nube.

En este terreno, presume VMware de sus alianzas, entre las que destacan la que tiene con AWS, cuyo número de máquinas virtuales se triplica anualmente y Azure, ya disponible en Norteamérica, Europa y Asia, si bien VMware Cloud alcanza ya los principales hiperescaladores, incluyendo IBM, Alibaba, Google y Oracle, además de instalaciones on-premise con VMware Cloud on Dell. Con esto y los más de 200 partners de VMware Cloud, "somos el elemento integrador en este mundo de nubes múltiples", recalcaba Gelsinger, que adelantaba el anuncio de VMware Telco Cloud para el desarrollo de 5G, "poniendo a disposición de los principales jugadores un entorno abierto y definido por software en la nube". Asimismo, añadía que están trabajando con Dish en el desarrollo de la primera RAN (Radio Area Network) nativa de la nube y definida por software, que llegará primero a Estados Unidos antes de desplegarse en otras zonas geográficas.

NETWORKING DEFINIDO POR SOFTWARE

La tercera pieza de la estrategia de VMware es Virtual Cloud Networking, con un elemento central, NSX, que ya supera los 17.000 clientes a nivel mundial, incluidas 91 empresas de la lista Fortune100. NSX proporciona la flexibilidad de una solución definida por software en cuatro segmentos:

Novedades VMWorld 2020: Modernización de Aplicaciones

Recordaba Gelsinger que cuando Java llegó al mercado, lo hizo con la promesa de desarrollar una vez y ejecutar en cualquier plataforma. Ahora es necesaria una propuesta similar en el mundo actual, un mundo multi-cloud e híbrido, y ésta es Kubernetes, la herramienta ideal para automatizar la creación y ejecución de aplicaciones en contenedores.

Tanzu permite a los desarrolladores llevar las apps a producción más rápido y entregar el código en cualquier nube. Con el nuevo rediseño de vSphere, VMware convierte esta plataforma "en la mejor para ejecutar aplicaciones virtualizadas y contenedorizadas".

VMware Tanzu

❖ Extender las apps modernas en varias nubes de forma automática con equilibrio de carga avanzado.

❖ Seguridad intrínseca en las apps en cualquier lugar con firewalls definidos por servicio, que ahora se integra con la detección de amenazas de LastLine.

❖ Extender la red al Edge y sucursales con VeloCloud.

❖ Extender los servicios de seguridad al Edge.

Ahora, VMware anuncia significativas mejoras en seguridad en SD-WAN con Secure Access Service Edge (SASE), que incluye acceso Zero Trust con Workspace ONE junto con el firewall para NSX y controles web avanzados con Secure Web Gateway. Además, la compañía ha anunciado un alianza de la suite SASE con Zscaler.

SEGURIDAD INTRÍNSECA

Y es que la seguridad es un elemento esencial en toda la estrategia de VMware, una seguridad basada en una propuesta coherente independientemente de la app, la nube o el dispositivo. Catorce meses después de la combinación con Carbon Black, ofrecen servicios a más de 200.000 clientes de seguridad, un negocio que representa más de 1.000 millones de dólares para la compañía.

Ahora se anuncia VMware Carbon Black Cloud Workload, una herramienta para configurar y administrar cargas de trabajo virtuales, que integra, de forma navita, vSphere para simplificad las operaciones. Aprovechando su anuncio,

Novedades VMworld 2020: Alianza con Nvidia

VMware y Nvidia han anunciado durante el VMworld 2020 un acuerdo para ofrecer una plataforma empresarial de extremo a extremo para Inteligencia Artificial, una nueva arquitectura para los centros de datos, la nube y el perímetro que utiliza unidades de procesamiento de datos (DPU) de NVIDIA para apoyar a las aplicaciones existentes y de próxima generación.

A través de esta colaboración, el conjunto de soluciones de IA de Nvidia se integrará en VMware vSphere, VMware Cloud Foundation y VMware Tanzu, con el objetivo de acelerar la adopción de la IA, al permitir a las empresas ampliar la infraestructura existente para IA, gestionar todas las aplicaciones con un único conjunto de operaciones, e implementar una infraestructura preparada para IA donde residan los datos, ya sea en el centro de datos, la nube o el perímetro.

Como parte del Proyecto Monterey, ambas compañías trabajarán para ofrecer una arquitectura para la nube híbrida basada en la tecnología SmartNIC, incluido Nvidia BlueField-2. La combinación de VMware Cloud Foundation y Nvidia BlueField-2 ofrecerá una infraestructura de próxima generación diseñada específicamente para las demandas de la IA, machine learning, alto rendimiento y aplicaciones centradas en datos. También ofrecerá una aceleración de aplicaciones ampliada más allá de la inteligencia artificial para todas las cargas de trabajo empresariales y proporcionará una capa adicional de seguridad a través de una nueva arquitectura que descarga los servicios críticos del centro de datos de la CPU a las SmartNIC y las DPU programables. Preguntado por este proyecto por IT User, Pat Gelsinger señalaba que se trata de un proyecto "a largo plazo. Se trata de un proyecto muy significativo del que esperamos ver resultados en los próximos años. No se trata de buscar resultados a corto plazo, porque es un cambio muy profundo".

NOVEDADES VMWORLD 2020:

Seguridad Intrínseca

La estrategia de seguridad de VMware pasa por una propuesta única y coherente sin que importe de qué aplicación se trata, en qué nube se ejecuta o con que dispositivo. Esta propuesta de seguridad se vio reforzada hace poco más de un año con la combinación de la tecnología de la compañía con Carbon Black, y ahora se mejora con la posibilidad de configurar y administrar máquinas virtuales.

Virtual Cloud Networking

VMware anuncia significativas mejoras en seguridad en SD-WAN con Secure Access Service Edge (SASE), que incluye acceso Zero Trust con Workspace ONE junto con el firewall para NSX y controles web avanzados con Secure Web Gateway. Además, la compañía ha anunciado un alianza de la suite SASE con Zscaler.

Espacio de trabajo digital

En un momento en que el trabajo en remoto ha adquirido un protagonismo inusitado, VMware ha anunciado una solución que potencia las capacidades de su plataforma en este segmento: Workspace ONE. Así, para potenciar a esta fuerza laboral remota, anuncia Workspace Solution, que incluye: Workspace ONE, VMware SD-WAN by VeloCloud y VMware Carbon Black EndPoint. Unidas estas tres herramientas, se ofrece una solución Zero Trust para que los trabajadores tengan la libertad para trabajar desde cualquier lugar y con cualquier dispositivo.

VMware ofrece una prueba gratuita para sus clientes durante los próximos 6 meses, con un número ilimitado de máquinas virtuales.

ESPACIO DE TRABAJO DIGITAL

La última pieza de la estrategia es el Espacio de Trabajo Digital, en un momento en que "vivimos la mayor evolución del teletrabajo en la historia". De ahí que VMware quiera potenciar a esta fuerza laboral remota y anuncie Workspace Solution, que incluye "lo mejor de tres áreas", Workspace ONE, VMware SD-WAN by VeloCloud y VMware Carbon Black EndPoint, que, combinados, "constituyen una solución Zero Trust que ofrece a los trabajadores la libertad para trabajar desde cualquier lugar y con cualquier dispositivo". ■

MÁS INFORMACIÓN

Todos los contenidos de VMworld

CYTOMIC

De la hipótesis a la caza

Threat Hunting: Zero Trust y Analítica de comportamiento

Nuestros servicios de **Threat Hunting e investigación** estudiarán y clasificarán todos los comportamientos de aplicaciones, máquinas y usuarios para erradicar las ciberamenazas avanzadas en tu entorno corporativo.

“Los fabricantes de IoT han dado marcha atrás en sus posturas de seguridad

CISO de Netskope para la región de EMEA, Neil Thacker es, además, cofundador de la Security Advisor Alliance, miembro de los consejos asesores de la Cloud Security Alliance o la Security Advisor Alliance; y participante del ENISA Threat Landscape Stakeholder Group (TLSG).

Hablamos con el directivo de cómo se está gestionando la seguridad de los dispositivos IoT, el cloud, la importancia y papel de ENISE en la Unión Europea, el impacto de la Inteligencia Artificial o las inversiones en seguridad de las empresas europeas.

En general, ¿cree que Europa como grupo se ocupa adecuadamente de la seguridad? ¿Hay mucha diferencia entre la madurez de algunos países y la de otros?

Europa está considerada como una de las regiones líderes en materia de ciberseguridad. En los últimos cinco años, la mayoría de las naciones europeas han lanzado o revisado sus estrategias de ciberseguridad para hacer frente a las nuevas y emergentes amenazas a la economía digital. Para apoyar aún más estas iniciativas, Europa también cuenta con organizaciones de talla mundial como CERT-EU, EC3 y ENISA que proporcionan apoyo a empresas y personas en la lucha contra la ciberdelincuencia.

A nivel mundial, la ciberseguridad se ha convertido en un requisito fundamental y los países de todo el mundo están comprendiendo la importancia de invertir en el sector para su propia seguridad, protección y crecimiento económico.

En lo que respecta a la madurez de los distintos territorios, aclarar que, aunque Europa puede tener una ventaja y estar respaldada por organizaciones

"Es necesario que exista un gran proveedor de nubes europeo para que Europa tenga soberanía digital, protección de datos europea, y que ofrezca confianza y transparencia"

establecidas y recursos financiados, ciertamente hay algunos países de la región que se están poniendo al día para seguir las tendencias que imperan en la actualidad. En este sentido espero que, en todo el mundo, estas iniciativas puedan integrarse mejor con un mejor intercambio de información y colaboración.

¿Cuál es el papel y la importancia de ENISA?
ENISA (Agencia de la Unión Europea para la Ciberseguridad) trabaja con los Estados miembros de la UE para ofrecer asesoramiento y soluciones con el objetivo general de mejorar las capacidades en materia de ciberseguridad. ENISA está integrada por expertos en muchos dominios diferentes de la ciberseguridad con muchos partidarios y partes interesadas que ofrecen su propio tiempo y recursos para apoyar mejor a la agencia.

Como ejemplo, he estado personalmente involucrado con el grupo Threat Landscape de ENISA durante los últimos cinco años para discutir y presentar las últimas investigaciones sobre amenazas, técnicas de mitigación de amenazas y especializarme en la importancia de la seguridad en la nube y la innovación en el análisis de amenazas.

El grupo se reúne regularmente y organiza eventos y talleres para discutir las últimas tendencias. Además, el informe de ENISA sobre el panorama de las amenazas se publica cada año como un documento de orientación para que las organizaciones y los consumidores comprendan y respondan a los últimos cambios en el panorama de las amenazas.

El manifiesto de la presidencia alemana de la UE pide una cooperación más estrecha entre los países de la UE en materia de ciberseguridad, especialmente para la protección de las infraestructuras nacionales críticas. ¿Qué opina usted? ¿Está Europa preparada para ese nivel de cooperación?
Ciertamente, la colaboración es fundamental para las Infraestructuras Nacionales Críticas (CNI, por sus siglas en inglés). Hoy en día, los equipos del

"La Inteligencia Artificial (IA) no es nueva, sin embargo, a medida que se produce la transformación digital, el papel de la IA se hace cada vez más importante"

CERT, CSIRT e ISAC de toda Europa cooperan juntos. El mandato de la presidencia de la UE de Alemania no hará más que apoyar esta iniciativa clave y, aunque la cooperación no es obligatoria, lo cierto es que para proteger las Infraestructuras Nacionales Críticas es fundamental considerar que la seguridad de las CNI es única y requiere un área de especialización. El enfoque clave debería ser el cambiante panorama que rodea a las CNI y la dependencia de estas en IoT y la nube. En los últimos años, las Infraestructuras Nacionales Críticas han integrado muchas capacidades digitales y, siguiendo el mismo enfoque que muchas organizaciones han adoptado con la transformación digital, los proveedores de CNI también han optado por la nube para el consumo de software, servicios e infraestructura. Sin embargo, con este cambio viene la necesidad de modificar sus capacidades de seguridad, que deben incluir la protección de los servicios esenciales de la nube.

Entre otras cosas, Alemania quiere establecer una seguridad mínima para la IoT, como ya ha hecho Australia. ¿Es tarde para esta medida?

El espacio IoT está evolucionando y madurando y, en este sentido, desde hace varios años se está abordando la necesidad de dotarlo de un mínimo de seguridad. No obstante, y a pesar de que se han emitido diferentes directrices -con ENISA adoptando un papel clave en esta iniciativa- los fabricantes de IoT han dado marcha atrás en sus posturas de seguridad, al entender que estas afectarían tanto al coste como a la implementación de IoT. A medida que el espacio de IoT madura, no es demasiado tarde para establecer un mínimo de seguridad, sin embargo, no se sabe qué ocurrirá con los dispositivos de IoT ya existentes que no cumplen con este mínimo. La orientación tanto de la presidencia de Alemania como de las agencias de la UE será clave aquí.

RGPD fue una regulación avanzada en términos de la obligación de proteger los datos de los usuarios. Alemania quiere fortalecer aún más esa seguridad ya que quiere desarrollar el uso de la Inteligencia Artificial para la recuperación económica. ¿Es compatible?

El RGPD considera el estado del arte y fue diseñado para ser una regulación orientada al futuro, por lo menos durante los próximos 20 años. La Inteligencia Artificial (IA) no es nueva, sin embargo, a medida que se produce la transformación digital, el papel de la IA se hace cada vez más importante. En una economía impulsada por los

datos, la carrera está encaminada a desarrollar la mejor forma de IA para aprovechar al máximo las oportunidades económicas, teniendo en cuenta al mismo tiempo los derechos humanos fundamentales de la privacidad, la ética y la obligación moral de proteger a las personas. Hoy en día, es compatible siempre y cuando se apliquen la supervisión y estas obligaciones. Necesitamos que más expertos en inteligencia artificial y privacidad participen en este debate para asegurarnos de que encontramos el equilibrio correcto.

Hablando de la seguridad en la nube, ¿cree que es necesario un gran proveedor de nubes europeo?

El objetivo de GAIA-X es ofrecer opciones y alternativas. Veo esto como una gran iniciativa que amplía las opciones disponibles para ambos organizaciones y usuarios. Por tanto, creo que sí es necesario que exista un gran proveedor de nubes europeo para que Europa tenga soberanía digital, protección de datos europea, y que ofrezca confianza, transparencia y que esté orientada al mercado europeo.

"A medida que el espacio de IoT madura, no es demasiado tarde para establecer un mínimo de seguridad, sin embargo, no se sabe qué ocurrirá con los dispositivos de IoT ya existentes"

¿Cree que deberíamos seguir centrándonos en GAIA-X, el ecosistema digital abierto para Europa centrado en la Industria 4.0?

GAIA-X todavía tiene un camino por recorrer, sin embargo, se está siguiendo el enfoque correcto para asegurar que se convertirá en un ecosistema digital abierto para Europa. Europa solo tiene una

oportunidad para ello y una clave fundamental es lo que GAIA-X pretende ofrecer a través de la infraestructura y los servicios. La entrega de nuevas infraestructuras y servicios debe evaluarse continuamente a medida que el ecosistema madura.

La pandemia de salud ha tenido un fuerte impacto en la economía. ¿Cree que las empresas europeas pueden seguir invirtiendo en seguridad?

Una inversión continua en ciberseguridad es esencial. Aunque los presupuestos se congelen o incluso se reduzcan en 2021 debido a las consecuencias económicas de la pandemia, las organizaciones tienen la oportunidad de revisar sus requisitos y considerar qué es lo más importante para mejorar su postura como organización. Un ciberataque o una violación de datos en este momento perjudicará aún más los ingresos de una organización y podría poner fin a su negocio, por lo que es fundamental que las organizaciones mantengan su capacidad de recuperación.

Durante muchos años hemos hablado de la importancia de la consolidación de las tecnologías de seguridad y la crisis actual ha ayudado a identificar lo que es importante. Tenemos la oportunidad de transformar las redes y los servicios de seguridad y utilizar la nube para ofrecer estas capacidades. El estudio económico de la transformación de la red y la seguridad destaca dónde se puede ahorrar mientras se sigue apoyando el crecimiento de la línea principal de un negocio. Apoyar a los empleados y a la fuerza de trabajo en un momento difícil es fundamental, a la vez que se proporciona un acceso seguro a los servicios digitales y se garantiza la protección de los datos creados y consumidos. Muchas organizaciones son conscientes de la importancia de una estrategia basada en el riesgo y centrada en los datos, y de los beneficios que ofrece la nube para prestar servicios de seguridad.

Países como Finlandia o Estonia han organizado ejercicios de ciberdefensa durante sus presidencias. ¿Cree que este tipo de ejercicios son importantes?

Los ejercicios de ciberdefensa ayudan tanto a las empresas como a las naciones a estar mejor preparadas para un futuro incidente. No estar capacitado para un ciberataque puede causar resultados catastróficos, por lo que muchas organizaciones participan regularmente en ejercicios de Red Team / Blue Team y simulacros (wargames de host) con el uso de Cyber Range que permiten simular entornos operativos reales para identificar dónde existen lagunas y se requieren mejorar las capacidades. Aunque estos ejercicios pueden ser costosos en tiempo y recursos, al final demuestran su idoneidad en caso de prevenir un ciberataque o reducir drásticamente el tiempo de recuperación de un ataque.

Enlaces de interés...

- La ciberseguridad, en la terna de tecnologías que más impactarán en el futuro
- Las empresas deben aumentar la seguridad ante la afluencia de dispositivos IoT
- La necesidad de proteger IoT impulsa los servicios de autenticación de dispositivos

Compartir en RRSS

it TRENDS

OCTUBRE 2020

Hacia un nuevo orden digital inteligente y seguro

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

Hacia un nuevo orden digital inteligente y seguro

El pasado agosto, Mapfre publicaba que estaba sufriendo un ataque de ransomware en algunos sistemas de la compañía. La aseguradora, que no tuvo constancia de una brecha de datos, reaccionó rápidamente ante esta incidencia, tanto a nivel tecnológico -no tuvieron que ser días fáciles para el equipo de TI- como directivo, con una comunicación transparente y fluida en redes sociales. No solo se cayeron sus sistemas, también sus acciones. Entre los muchos mensajes que los dirigentes de Mapfre vertieron en sus perfiles, José Manuel Inchausti Pérez, vicepresidente y CEO para Iberia, indicó que "ni somos los primeros ni por desgracia seremos los últimos en recibir este tipo de ataques". Efectivamente, ni los primeros ni los últimos. Adif sí sufrió brecha de datos: 800 GB de información expuestos por no pagar el rescate. Otro caso reciente es el de Garmin, afectada por el ransomware WastedLocker el pasado mes de julio; o el de los hospitales españoles desde los que, supuestamente, se enviaban correos electrónicos con el asunto "Información sobre la Covid-19", y que llevaban un ransomware, llamado Netwalker, destinado a comprometer los sistemas informáticos de la red sanitaria.

Según la compañía Emsisoft, en 2019 se registraron en España más de 8.800 incidentes de ransomware, con un coste superior a 100 millones de euros para las empresas españolas. Panda Security, Secure&IT, Stormshield, Bitdefender, Trend Micro, VMware, Sophos, SonicWall y ESET, participaron en el IT Webinars "La persistencia del ransomware", para abordar las mejores prácticas que pueden aplicar las empresas para frenar y recuperarse de un ataque que les secuestre su información.

Además de ciberseguridad, el nuevo orden digital en el que nos movemos necesita también de las capacidades que le puede proporcionar la Inteligencia Artificial para optimizar sus procesos y agilizar el negocio. Bots digitales que automatizan tareas rutinarias y son capaces de interpretar los datos que en ellas se generan; atención al cliente personalizada; analítica predictiva; soluciones que detectan patrones repetidos y actúan sobre ellos, son algunas de sus aplicaciones. Automation Anywhere y Micro Focus abordaron estos usos en el ámbito empresarial en la sesión online "Inteligencia Artificial, ¿cómo lo aplico en mi empresa?".

Por otra parte, Alexandre Ramos, CIO de Liberty Seguros Europa, nos contaba en la entrevista IT Trends, cómo la compañía ha decidido migrar todos sus servicios a cloud para aprovechar la flexibilidad de la nube y operar de manera única los servicios de TI en toda la organización.

Y ya sabes que en IT Trends queremos conocer cómo evolucionan las estrategias tecnológicas de las empresas. Este año, la COVID-19 ha trastocado los planes de desarrollo en las empresas. ¿Cómo? ¿Hasta qué punto? Participa en nuestra encuesta "COVID-19, ¿cuánto y cómo ha influido en las estrategias de TI?" y pronto conocerás los resultados en un nuevo informe.

Hasta que llegue... descubre todos los contenidos que te ofrecemos en las siguientes páginas. ¡Gracias por leernos! ■

Arancha Asenjo
Directora de IT Trends
www.ittrends.es

itTRENDS

Entendiendo el ransomware:

el secuestro informático que pone en jaque a la empresa

Los virus informáticos no solo rompen los ordenadores o espían para chantajear a los usuarios. Además, existen cientos de tipos de virus que cifran todos los archivos de un ordenador, para después pedir un rescate económico para recuperarlos. Es un secuestro que deja el ordenador inutilizado. Esta clase de amenazas, el temido ransomware, se ha convertido en el ataque número uno en materia de seguridad informática. Y su evolución es larga y constante, con muchas variantes que los expertos en ciberseguridad detectan cada pocos meses.

El ransomware es un software malicioso con un único objetivo: extorsionar a sus víctimas. Es uno de los modelos comerciales criminales más abundantes que existen en la actualidad, principalmente por los rescates multimillonarios que los ciberdelincuentes exigen a individuos y corporaciones. Estas demandas son muy simples: pagar el rescate o perder los datos de su ordenador.

Generalmente, lo primero que un usuario u organización conoce de un ataque es cuando recibe una notificación en pantalla que les informa de que los datos de su ordenador se han cifrado y serán inaccesibles hasta que se haya

RANSOMWARE

pagado el rescate. Únicamente en el pago se les dará la clave de descifrado para acceder a sus datos. La falta de pago podría resultar en la destrucción de la clave, haciendo que los datos sean inaccesibles para siempre.

Llevamos unos años conociendo la existencia de diferentes casos de ransomware, pero la amenaza es mucho más longeva de lo que parece. En diciembre de 1989, cuando aún no había nacido la primera página web, 20.000 disquetes de 5,25 pulgadas se enviaron desde Londres a empresas tanto británicas como de otros países, a los suscriptores de la revista PC Business World' y a un congreso sobre el sida organizado por la Organización Mundial de la Salud: AIDS Information Introductory Diskette, ponía en su pegatina, que decía provenir de la PC Cyborg Corporation. En realidad, no era más que un engaño: cifraba el disco duro de los ordenadores y pedía un rescate. Un ransomware más rudimentario y mucho menos dañino que su tristemente famoso descendiente WannaCry, pero que también se difundió a escala global: llegó a unos 90 países por correo ordinario.

Sin embargo, no fue hasta 2012 cuando apareció el gusano Reveton: el primer malware que

En el informe global de seguridad de Trustwave de 2015 ya se estimó que los cibercriminales obtenían hasta un 1.425% de retorno de inversión por una campaña de ransomware.

mantenía los datos como rehenes hasta que se efectuara el pago del rescate. En el informe global de seguridad de Trustwave de 2015 ya se estimaba que los cibercriminales obtenían hasta un 1.425% de retorno de inversión por una campaña de código malicioso de esta naturaleza.

A finales de 2019, la aseguradora AIG emitió un informe que decía que el compromiso del correo electrónico empresarial (BEC) había reemplazado al ransomware como la principal amenaza que causan pérdidas comerciales. Los ataques BEC se convirtieron en la principal razón por la que las empresas realizaron una reclamación a sus ciberseguros el año pasado. Sin embargo, el Informe de reclamaciones de ciberseguros del primer semestre de 2020 de la compañía pone de manifiesto que el ransomware vuelve a ser la principal causa de reclamación a las ciberaseguradoras, al menos en la primera mitad del año.

CÓMO ATACA EL RANSOMWARE

La única buena noticia es que el ransomware no suele aparecer por sí solo. Debe estar activado para entregar su carga útil, generalmente a través de un enlace malicioso o un archivo adjunto en un correo electrónico. Existen cuatro pasos generalizados cuando un ordenador es infectado.

1 **El sistema está comprometido:** la mayoría de los ataques de ransomware comienzan como un ejercicio de ingeniería social, generalmente en forma de adjuntos o enlaces maliciosos. El objetivo es atraer al usuario a que haga clic en estos objetos para activar el malware.

2 **El malware toma el control:** una vez que el malware haya tomado el control del sistema, ciertos tipos de archivos se cifran y se les niega el acceso al usuario.

3 **Notificación a la víctima.** Para poder pagar el rescate, el usuario debe conocer las demandas de los delincuentes. En este punto, generalmente recibirán una notificación en la pantalla que explica las demandas y cómo pueden recuperar el acceso.

4 **Pago y devolución.** En la mayoría de los casos, los atacantes devuelven el control total a la víctima. Les interesa hacer esto; si no lo hicieran, pocas organizaciones estarían dispuestas a pagar si no creyeran que sus datos serían restaurados.

TIPOS DE ENGAÑOS

Hay una serie de accesos por los que el ransomware puede acceder a un ordenador. Uno de los sistemas de entrega más comunes es el spam de phishing: archivos adjuntos que llegan a la víctima en un correo electrónico y se hacen pasar por un archivo en el que deben confiar. Una vez que se descargan y abren, pueden hacerse cargo del ordenador de la víctima, especialmente si tienen herramientas de ingeniería social integradas que engañan a los usuarios para que permitan el acceso administrativo. Algunas otras formas de ransomware más agresivas, como NotPetya, aprovechan los agujeros de seguridad para infectar dispositivos sin necesidad de engañar a los usuarios. En algunas formas de malware, el atacante puede afirmar ser la policía y apagar el ordenador de la víctima porque ha hallado pornografía o software pirateado en ella, y exige el pago de una multa para hacer que las víctimas sean menos propensas a denunciar el ataque. Pero la mayoría de cibercriminales no se molesta en crear este tipo de engaños.

También existe una variación, llamada software de filtración, en la que el atacante amenaza con publicar datos confidenciales en el disco duro de la víctima si no paga un rescate. Pero, como encontrar y extraer dicha información es complicado, el ransomware de cifrado es el tipo más común.

¿A QUIÉN ATACA?

No hay un objetivo exacto. Puede llegar a individuos o a grandes empresas. Los atacantes pueden apuntar a empresas pequeñas y medianas o incluso a centros educativos como universidades, porque tienden a tener equipos de seguridad más pequeños y una base de usuarios dispar que comparte muchos archivos, lo que facilita la penetración de sus defensas.

Por otro lado, algunas organizaciones son objetivos tentadores porque parece más probable que paguen un rescate rápidamente. Por ejemplo, las agencias gubernamentales o las instalaciones médicas normalmente necesitan acceso inmediato a sus archivos. Los bufetes de abogados y otras organizaciones con datos confidenciales pueden estar dispuestos a pagar para mantener en secreto las noticias de un compromiso, y estas organizaciones pueden ser especialmente sensibles a los ataques de fugas. En definitiva, nadie está a salvo de ser atacado.

Las noticias de ataques de ransomware a diferentes empresas e instituciones públicas han ido en aumento durante estos últimos años. En 2019, la ciudad de Baltimore, Maryland (EE UU) fue atacada con una variante de ransomware llamada RobbinHood: el sistema del ayuntamiento permaneció bloqueado durante casi dos semanas. En España atacaron el también el año pasado el Ayuntamiento de Zaragoza, con un ransomware llamado sodinokibi,

que secuestró los servidores y 70 empleados se quedaron sin poder utilizar sus dispositivos.

LOS MÁS DAÑINOS

✱ **LOCKY** apareció en 2016 en un ataque lanzado por un grupo organizado de hackers. Tiene la capacidad de cifrar más de 160 tipos de archivos y se propaga engañando a las víctimas para que lo instalen mediante correos electrónicos falsos con archivos adjuntos infectados. Este método de transmisión se denomina phishing, Locky tiene como objetivo una amplia gama de tipos de archivos usados por diseñadores, desarrolladores, ingenieros y evaluadores.

✱ **WANNACRY** es el más conocido por haber afectado a más de 150 países en 2017. Fue diseñado para explotar una vulnerabilidad en Windows, que supuestamente fue creado por la Agencia de Seguridad Nacional de Estados Unidos y filtrado por el grupo The Shadow Brokers. WannaCry afectó a 230.000 dispositivos en todo el mundo y puso de manifiesto el daño que puede causar el uso de sistemas obsoletos, más vulnerables a ataques. El impacto financiero global de WannaCry fue sustancial: se estima que provocó pérdidas financieras por valor de 4.300 millones de dólares en todo el mundo.

Algunas organizaciones son objetivos tentadores porque parece más probable que paguen un rescate rápidamente

✱ **PETYA** es un ataque de ransomware que se lanzó por primera vez en 2016 y que resurgió en 2017 como GoldenEye. En lugar de cifrar archivos específicos, este ransomware cifra todo el disco duro de la víctima. Para ello, cifra la tabla maestra de archivos (MFT, del inglés "Master File Table"), lo que impide el acceso a los archivos del disco. Petya se propagaba por los departamentos de RRHH a través de un correo electrónico de solicitud de empleo falsa con un enlace a Dropbox infectado.

✱ **GOLDENEYE:** el resurgimiento de Petya, conocido como GoldenEye, culminó en un ataque de ransomware global en 2017. Bautizado como el hermano devastador de WannaCry, GoldenEye afectó a más de 2.000 objetivos, entre ellos importantes productores de petróleo en Rusia y varios bancos. GoldenEye obligó a los trabajadores de la central nuclear de Chernóbil a comprobar de forma manual los niveles de radiación, ya que se les había bloqueado el acceso a sus equipos Windows.

✱ **CRYPTOLOCKER** apareció por primera vez en 2007 y se propagó a través de archivos adjuntos de correo electrónico infectados. Una vez en el dispositivo, buscaba archivos valiosos y los cifraba para pedir un rescate. Se calcula que afectó a unas 500 000 ordenadores. La policía y las empresas de seguridad finalmente consiguieron detectar una red mundial de ordenadores secuestrados que se utilizaban para propagar el ransomware Cryptolocker.

De esta manera controlaron parte de la red cibercriminal y capturaban los datos en el momento en que se enviaban sin que los cibercriminales lo supieran. Esta acción posteriormente desembocó en el desarrollo de un portal online en el que las víctimas podían obtener una clave para desbloquear y liberar sus datos de forma gratuita sin necesidad de pagar a los criminales.

✱ **BAD RABBIT** es un ataque de ransomware realizado en 2017 que se esparció mediante un método denominado ataque drive-by, que hace uso de sitios web sin protección para llevar a cabo un ataque. Durante un ataque drive-by de ransomware, un usuario visita un sitio web legítimo sin saber que un hacker lo ha vulnerado.

Normalmente los ataques drive-by no necesitan interacción por parte de la víctima, un usuario se infecta si visita la página vulnerada. Sin embargo, en este caso se infectan cuando hacen clic para instalar algo que en realidad es malware disfrazado. Este elemento se conoce como instalador (dropper). Bad Rabbit solicitaba instalar Adobe Flash, pero lo que en realidad instalaba era un instalador de malware para propagar su infección.

✱ **RYUK** se propagó en agosto de 2018. Desactivaba la opción de restauración del sistema de Windows e impedía la restauración de los archivos cifrados si el usuario no contaba con una copia de seguridad. Ryuk también cifraba las unidades de red. Los efectos fueron devastadores, y muchas de las organizaciones que sufrieron el ataque en Estados Unidos pagaron los rescates exigidos. Se estima que los fondos recaudados con el ataque superan los 550.000 euros.

✱ **TROLDESH** se produjo en 2015 y se propagó a través de correos electrónicos de spam con enlaces o archivos adjuntos infectados. Curiosamente, los atacantes de Troldesh se pusieron en contacto con las víctimas directamente por correo electrónico para solicitar los rescates. Los cibercriminales incluso negociaron descuentos para las víctimas con las que entablaron una buena relación, algo muy poco común.Esta historia es sin duda la excepción, no la regla. Nunca es una buena idea negociar con cibercriminales.

✱ **GANDCRAB** amenazaba con revelar los hábitos de visualización de pornografía de la víctima. Los cibercriminales de GandCrab afirmaban haber secuestrado la webcam de los usuarios, exigían un rescate y amenazaban a las víctimas con publicar el vergonzoso material si no se les pagaba. Tras su primer lanzamiento en enero de 2018, GandCrab evolucionó pasando por varias versiones. Como parte de la iniciativa No More Ransom, los proveedores de seguridad para Internet y la policía colaboraron para desarrollar un descifrador de ransomware que rescatara los datos confidenciales de la víctima en manos de los cibercriminales.

✱ **JIGSAW** comenzó en 2016. Tenía este nombre porque incluía una imagen de la marioneta de la película Saw. Este ransomware iba eliminando gradualmente más y más archivos de la víctima cada hora que pasaba sin pagarse el rescate exigido. ■

Los ransomware con más alcance de los últimos años

- ♦ **Wannacry**
- ♦ **Locky**
- ♦ **Petya**
- ♦ **GoldenEye**
- ♦ **Criptolocker**
- ♦ **Bad Rabit**
- ♦ **Ryuk**
- ♦ **Troldesh**
- ♦ **GrandCrab**
- ♦ **Jigsaw**

MÁS INFORMACIÓN

Crecen los ataques de ransomware y DDoS en el marco de la pandemia

Aumentan los ataques de ransomware destinados al sector sanitario

Si te ha gustado este artículo, compártelo

CLAVES PARA EVITAR LA ENTRADA

Los expertos recomiendan crear un plan estructurado además de impartir educación digital a los empleados de las empresas, ya que siempre son el eslabón más débil. No obstante, se pueden tener en cuenta algunas consideraciones para impedir que un ransomware penetre en un dispositivo.

❖ **ACTUALIZACIÓN DEL SISTEMA Y APLICACIONES.** El mejor punto de partida es mantener el sistema operativo actualizado con los últimos parches de seguridad y todas las aplicaciones que tengamos instaladas. WanaCry aprovechó una vulnerabilidad en sistemas Windows.

❖ **LÍNEA DE DEFENSA.** Conviene instalar y mantener una solución antimalware, incluyendo un cortafuegos correctamente configurado para permitir el acceso exclusivo de las aplicaciones y servicios necesarios.

❖ **HERRAMIENTA ANTI RANSOMWARE.** Es una herramienta específica contra este tipo de ataques, que tratará de bloquear el proceso de cifrado de un ransomware. Realizará un dump de la memoria del código dañino en el momento de su ejecución, con el que es probable conseguir la clave de cifrado simétrico que se estuviera empleando.

❖ **FILTRO ANTISPAM.** Muchos de los ataques por Ransomware se distribuyen a través de campañas masivas de correo electrónico. Además de estos filtros, no se debe pinchar en enlaces o abrir archivos adjuntos de remitentes desconocidos.

❖ **BLOQUEADORES DE JAVASCRIPT.** Aplicaciones como Privacy Manager bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar la posibilidades de quedar infectado a través de la navegación web.

❖ **POLÍTICAS DE SEGURIDAD.** Herramientas como AppLocker, Cryptoprevent, o CryptoLocker Prevention Kit facilitan el establecimiento de políticas que impiden la ejecución de directorios comúnmente utilizados por el ransomware, como App Data, Local App Data, etc.

❖ **CUENTAS CON PRIVILEGIOS.** No utilizar cuentas con privilegios de administrador. El 86% de las amenazas contra Windows se pueden esquivar en caso de utilizar un usuario común en lugar de un administrador. Por eso es importante utilizar para tareas comunes un usuario común y solo dejar el administrador para cuando se vaya a hacer una serie de tareas relacionadas con la manipulación del sistema.

❖ **EXTENSIONES DE ARCHIVOS.** Mostrar las extensiones para tipos de ficheros conocidos es una buena práctica para identificar los posibles ficheros ejecutables que quieran hacerse pasar por otro tipo de fichero. No es raro ver a un fichero .exe con el icono de un documento de Word. Si no se ve la extensión, el usuario posiblemente no pueda distinguir si es un documento de Word o un ejecutable malicioso, aunque también es bueno recordar que un documento de Microsoft Office también puede contener malware.

❖ **MÁQUINAS VIRTUALES.** Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse.

❖ **BACKUP.** Realizar copias de seguridad de los datos importantes como tarea de mantenimiento regular es la medida más efectiva para minimizar los daños en caso de ser infectado.

Los equipos de seguridad ahora tienen que decodificar cómo trabajan los equipos de DevOps, cómo abordan la seguridad y cómo se puede incorporar la seguridad en ese proceso desde el principio, desde el desarrollo inicial del código hasta las pruebas, el control de calidad y la producción. Es necesario proporcionar a los desarrolladores la información correcta sobre la seguridad y las vulnerabilidades en las herramientas que utilizan, y en un lenguaje que puedan comprender fácilmente. La coordinación entre todos los departamentos es fundamental para detener las ciberamenazas.

NUEVO INFORME

DOCUMENTO EJECUTIVO

Teletrabajo en 2020:
el futuro se hace presente

ELABORADO POR itRESEARCH

Descarga este **documento ejecutivo** de itRESEARCH

#ITWEBINARS

La persistencia del Ransomware

6 de cada 10 organizaciones fueron víctimas de ransomware en 2019, una cifra que va en aumento año a año debido al incremento en los pagos de rescates. Más de un tercio de las organizaciones experimentaron seis o más ataques exitosos, y el 69% esperan sufrir uno este año.

Aunque inicialmente el ransomware se utilizaba de manera aleatoria, infectando usuarios a los que se pedían rescates de cientos de dólares por recuperar el control de sus ordenadores, los ataques se han hecho mucho más dirigidos y ambiciosos, llegando a colapsar empresas e incluso ciudades. Nadie está a salvo de una amenaza difícil de rastrear.

¿Cómo hacer frente a la amenaza? ¿Qué sectores están más expuestos? ¿Cómo puedes recuperarte de un ataque de ransomware? En este IT Webinars hemos reunido a un grupo de expertos para hablar de cómo hacer frente al ransomware, una de las ciberamenazas que más preocupan a los responsables de ciberseguridad de las empresas. Contamos con la participación de Panda Security, Secure&IT, Stormshield, Bitdefender, Trend Micro, VMware, Sophos, SonicWall y ESET. A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí. ■

Si te ha gustado este artículo, compártelo

HACIA UN NUEVO ORDEN DIGITAL INTELIGENTE Y SEGURO

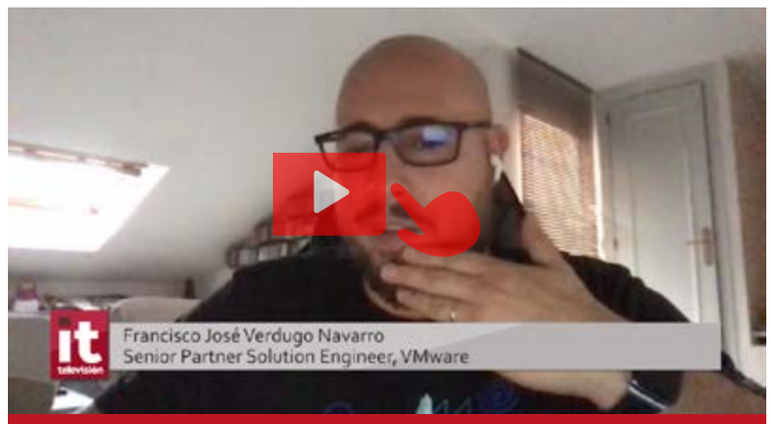
Francisco Valencia, Secure&IT

Borja Pérez, Stormshield Iberia

Alberto Tejero, Panda Security Iberia, a WatchGuard brand

Horatiu Bandoiu, Bitdefender

José de la Cruz, Trend Micro Iberia



Francisco José Verdugo, VMware

Alberto Rodas, Sophos

Sergio Martínez, SonicWall Iberia

Josep Albors, ESET España

it TRENDS

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

“A futuro, el ransomware va a ser muchísimo más duro de lo que es ahora”

El año pasado, el 51% de las empresas sufrieron un ataque de ransomware, y en el 73% por ciento de las ocasiones los datos acabaron siendo cifrados. De esta amenaza hablamos con Francisco Valencia, director general de Secure&IT, en la sesión online La Persistencia del Ransomware.

Asegura el directivo que las empresas tienen una falsa sensación de seguridad, que no creen que el malware les vaya a afectar, ni que vayan a sufrir un ataque. Pero lo cierto es que hay una amenaza muy clara, “hay grandísimos grupos de ciberdelincuencia organizada con distintos motivos que utilizan cientos o miles de herramientas distintas para poder lanzar sus ciberataques”. El ransomware, dice Francisco Valencia, se ha convertido en el ataque más mediático, “por lo tanto genera un impacto no solamente sobre los datos que se han perdido o sobre la operación que se ha dejado hacer, sino también desde el punto de vista re-

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

“El ransomware es un malware democrático, en el sentido que ataca a todas las empresas de todos los tamaños y todos los sectores”

putacional”. Es, además, “un tipo de malware que ataca a todas las empresas de todos los tamaños y todos los sectores”, que también se utiliza para ataques dirigidos y que genera enormes cantidades de dinero a los ciberdelincuentes que lo explotan.

“El futuro inmediato es un ransomware que va a ser muchísimo más duro de lo que es ahora”, porque si hasta ahora lo que ocurría es que se cifraban los datos, las nuevas versiones de esta lacra los roban y amenazan con hacerlos públicos si no se paga el rescate, “lo que puede tener un impacto mucho mayor”.

Asegura también Francisco Valencia que los ataques de ransomware han evolucionado hasta el punto de que ahora eliminan las copias que están en el shadow copy, son capaces de detectar y evadir técnicas de sanboxing, utilizan múltiples vectores de ataque, afectan a todos los sistemas operativos y emplean mecanismos de cifrado tremendamente avanzados.

Entre las medidas que se pueden tomar, menciona el director general de Secure&IT que el ransomware no es sólo un problema informático, sino de información, y que hay cuatro vectores fundamentales en los que la alta dirección de una empresa tiene que trabajar: cumplimiento normativo, procesos corporativos, seguridad informática y vigilancia de la seguridad.

Vea aquí la intervención de Secure&IT en La Persistencia del Ransomware

Si te ha gustado este artículo, compártelo

SECURE&IT. SEGURIDAD 360º

Secure&IT es una empresa española que cuenta con un equipo de auditores que trabajan de manera integrada en el análisis de riesgos de las empresas, siendo uno de los mayores la protección inadecuada de la información. La compañía cuenta con su propio SOC, que ha sido reconocido como CERT y que está dotado de sistemas y procesos avanzados, pudiendo monitorizar,lk vigilar, registarar, gestionar y actuar de manera inmediata ante eventos que afecten a la seguridad de la información de su empresa.

it TRENDS

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

"Es necesario entender cómo se ha producido el ataque"

El 26% por ciento de las víctimas de un ataque de ransomware en el que los datos se han cifrado, pagan el rescate. Hablamos con Borja Pérez, director general de Stormshield Iberia, en la sesión online La Persistencia del Ransomware sobre cómo ha percibido su compañía la evolución de esta amenaza, sobre la que asegura que antes de 2016 hablar de ransomware era hablar de CryptoLocker y que con Wannacry esta amenaza apareció en los medios de comunicación. Tras un descenso en 2018, "probablemente porque los cibercriminales orientaron sus esfuerzos hacia la minería de bitcoin", el ransomware no ha dejado de crecer y la nueva tendencia es no sólo cifrar los datos, sino amenazar con hacerlos públicos".

Este tipo de ataques, dice Borja Pérez, "está afectando a todos los sectores" y se producen tanto de manera masiva como más dirigidos, "un ataque más sofisticado que requiere más inversión también por parte de los delincuentes".

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

“Tener nuestros datos convenientemente cifrados significa que lo que se está llevando el atacante es pura basura criptográfica, información a la que no puede acceder”

¿Cómo se puede hacer frente al ranwomware? Menciona el director general de Stormshield Iberia algunas medidas “que no son tan complicadas”, como es tener un backup junto con una solución de disaster recovery, así como algunas medidas de seguridad básicas que protejan el puesto de trabajo y el perímetro, junto con una solución de cifrado de datos.

Las medidas coinciden con la propuesta de Stormshield, centrada en: Network Security, Endpoint Security y Data Security. Sobre Stormshield Endpoint Security dice Borja Pérez que es un agente ligero que se instala en los puestos y monitoriza el comportamiento de los procesos, bloqueando el que no sea legítimo –y no la aplicación para que el usuario pueda seguir trabajando. Este agente también protege las conexiones o dispositivos que se puedan conectar a él, bloqueando lo que no esté permitido por la organización. Menciona el directivo la tendencia del mercado hacia los EDR, o lo que es lo mismo, no sólo la detección, sino también la respuesta, “y entender cómo se ha producido el ataque, que debilidad ha encontrado el atacante y como lo está intentando hacer para mitigar posibles futuros ataques”.

La red también es importante y es vital saber lo que está pasando en el tráfico. Sobre el cifrado dice Borja Pérez que no es una mediante anti ransomware como tal, pero que teniendo en cuenta que la tendencias de los últimos ataques de ransomware es hacer públicos datos o de robarlos, el tener nuestros datos convenientemente cifrados significa que “lo que se está llevando el atacante es pura basura criptográfica, información a la que no puede acceder”.

Vea aquí la intervención de Stormshield en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

STORMSHIELD ENDPOINT SECURITY

Los ataques de hoy son cada vez más selectivos y sofisticados en un intento por eludir los sistemas de protección convencionales. Utilizan técnicas de infección avanzadas, como la explotación de vulnerabilidades desconocidas, y emplean mecanismos sofisticados para pasar desapercibidos en el sistema operativo. Las amenazas ya no se limitan a las redes: ahora se extienden a entornos sensibles o industriales donde el impacto potencial es considerable (riesgos de deterioro físico, parada de la línea de producción, etc.).

it TRENDS

ALBERTO TEJERO, DIRECTOR GENERAL DE PANDA SECURITY IBERIA, A WATCHGUARD BRAND

"Tenemos un problema de concienciación"

Sólo el 64 por ciento de las empresas que tienen un ciberseguro están cubiertas por el ransomware, una amenaza que cada vez preocupa más a los responsables de las empresas y de la que hablamos con Alberto Tejero, director general de Panda Security Iberia, una compañía de WatchGuard, quien comienza explicándonos que los problemas de ciberseguridad se han incrementado junto con el teletrabajo, que ha tenido que adoptarse a gran escala en pocas semanas o incluso días.

Durante la sesión online La Persistencia del Ransomware, dice Alberto Tejero que el phishing es una de las maneras en las que se ha propagado el ransomware. Ha habido un incremento del número de correos enviados en los últimos tiempos, lo que ha sido aprovechado por los ciberdelincuentes para enviar mensajes maliciosos con información sobre el confinamiento y el virus.

Otra vía de propagación del ransomware ha sido a través de vulnerabilidades en el softwa-

ALBERTO TEJERO, DIRECTOR GENERAL DE PANDA SECURITY IBERIA, A WATCHGUARD BRAND

“La propuesta de Panda Security pasa por Adaptive Defense 360, una solución EDR en la que se combinan diferentes capas de seguridad”

re, algo que ya vimos en los casos de Wannacry y Petya. “Pero sobre todo hay mucho phishing”, asegura el directivo de Panda Security.

La mayor complejidad en los ataques y los mensajes de phishing cada vez más dirigidos y profesionalizados hace que “los usuarios necesiten una solución un poco más avanzada”. La propuesta de Panda Security pasa por Adaptive Defense 360, una solución EDR en la que se combinan diferentes capas de seguridad, empezando por una tecnología de firmas y heurística para la detección de ataques, “como cualquier solución de seguridad antivirus tradicional”; una segunda capa de detección contextual que permite detectar ataques sin ficheros para pasar a una tecnología antiexploit “que también nos permite detectar ataques fileless que explotan vulnerabilidades.

A estas cuatro primeras capas le siguen otras dos. Un servicio gestionado que permite clasificar todo lo que se ejecuta en las máquinas, lo que permite detener ataques en la red interna y por movimientos laterales. La solución Adaptive Defense monitoriza todos los procesos en ejecución para permitir únicamente la ejecución de los clasificados como confiables por Panda Security

Y finalmente, algo que según Tejero les diferencia: un servicio de Threat Hunting, “en el que no sólo vemos los ataques de ransomware, sino de suplantación de identidad”.

Asegura Alberto Tejero que el mercado tiene un problema de concienciación y que el mercado tiene que darse cuenta de que teletrabajar en casa y estar en una oficina “no implica los mismos procedimientos de seguridad”.

Vea aquí la intervención de Panda Security en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

PANDA SECURITY REPORT. SODINOKIBI

Este documento recoge el análisis de una muestra del Ransomware “Sodinokibi”, también conocido como REvil, que apareció a lo largo de la primera mitad de 2019 y se caracteriza por su gran capacidad de evasión y el gran número de medidas que toma para evitar ser detectado por los motores antivirus.

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

“Es importante entender que cualquier organización puede ser un blanco de los atracadores”

Los cibercriminales consiguieron cifrar datos en el 73% de los ataques de ransomware lanzados el año pasado. En la sesión online La Persistencia del Ransomware aporta Horatiu Bandoiu, Channel Marketing Manager España & LATAM de Bitdefender,otros datos del mundo de la seguridad, extraídos de una encuesta realizada en diferentes países que recoge, entre otras cosas que el 63% de los responsables de ciberseguridad considera que estamos en una ciberguerra, que el 27% de las empresas no tienen una estrategia de seguridad o que el 72% creen que hay necesidad de un tipo más diverso de habilidades en la ciberguerra.

Sobre el ransomware dice el directivo de Bitdefender que los ataques se están incrementando “pero que la protección contra ellos no ha avanzado mucho en los últimos años”, a pesar de lo cual 3 de cada 5 han reforzado sus infraestructuras y están prestando atención a la formación de los empleados en ciberse-

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

“A los responsables de ciberseguridad les preocupa no sólo el impacto reputacional de un ataque de ransomware, sino las multas”

guridad, sobre todo ahora que muchos están teletrabajando. A los responsables de ciberseguridad les preocupados no sólo el impacto reputacional de un ataque, sino las multas, por lo que uno de cada seis está creando una partida presupuestaria para ello.

Tras mencionar el caso de Garmin, que el verano pasado sufrió un ataque de ransomware que dejó sin cobertura a sus clientes, dice Horatiu Bandoiu que “es importante entender que cualquier organización puede ser un blanco de los atracadores”.

Bitdefender, cuyas soluciones de seguridad han alcanzado la tercera generación, ofrece “un approach integrado” para lucha frente al ransomware. Explica el directivo de la compañía que la primera generación fue la de prevención; la segunda generación incorporó tecnología de próxima generación y EDR, “pero hemos visto que en menos de un año los atacantes ya se han adaptado”, lo que ha llevado a la compañía a adoptar una aproximación diferente, basado en ciberresiliencia, “que significa estar preparados para responder en cualquier momento en un ciclo que no acaba nunca, en el cual tienes que entender tus riesgos de seguridad, poner medidas de prevención, pero estar preparado para detectar las señales de que has sido atacado y responder, reduciendo los riesgos de seguridad”.

La clave pasa por GravityZone Enterprise, una suite completa capaz de prevenir, detectar, investigar, dar una respuesta adecuada y reforzar el sistema. Clave es también mantener una actitud ciberresiliente, lo cual significa tener capas de protección y tecnologías que buscan reducirla superficie de ataque, reforzar la capa de red “para poder identificar las técnicas de ataque, tecnologías de detección de ataques o tecnologías de detección y respuesta para una contención automática.”

Vea aquí la intervención de Bitdedfender en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

BITDEFENDER GRAVITYZONE ULTRA PLUS

Las soluciones tradicionales de detección y respuesta en los endpoints se basan únicamente en el análisis de datos de los endpoints para detectar las amenazas digitales. GravityZone Ultra Plus utiliza un modelo XDR y aplica el Machine Learning, la correlación de eventos y la inteligencia sobre amenazas a los datos recopilados desde todos los elementos de la infraestructura empresarial: endpoints (físicos o virtualizados), recursos en la nube y elementos de red.

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

“No debemos pagar nunca el rescate”

Pagar el rescate duplica el coste de un ataque de ransomware. Sobre esta amenaza dice José de la Cruz, director técnico de Trend Micro, que es un malware como otro cualquiera que lo que hace es infectar a un usuario, propagarse de manera muy rápida y secuestrar máquinas, sistemas operativos o información, cifrando archivos y carpetas.

En la sesión online La Persistencia del Ransomware asegura también el directivo de Trend Mico que el atacante quiere obtener una rentabilidad económica y explica la evolución de la amenaza desde que apareciera hacia 1989 con el AIDS Trojan hasta nuestros días, cuando los atacantes no sólo cifran la información y piden un rescate por ella, sino que amenazan con hacerla pública si no se paga el rescate, lo que puede tener un impacto muy grande de cara a normativas como GDPR.

¿Cómo pueden afrontar las empresas la lucha contra el ransomware? Ofrece José de la Cruz una serie de recomendaciones genéricas que empiezan con que no debemos pagar nunca el rescate porque, entre otras cosas, “no tenemos ninguna certeza de que nos vayan a devolver la información, y no tenemos ninguna certeza de que, aunque hayamos pagado, no vayan a continuar extorsionándonos una y otra vez”. Aislar nuestro entorno de Internet para impedir que el ataque prospere, apagar

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

“No tenemos ninguna certeza de que, aunque hayamos pagado, no vayan a continuar extorsionando una y otra vez”

cualquier sistema prescindible, ir recuperando los servicios de manera progresiva o hacer uso de herramientas EDR y analizadores de red son otras de las recomendaciones del director técnico de Trend Micro.

A la hora de prevenir, dice José de la Cruz que es necesario tener una copia de seguridad externa, “y cuando digo externa me refiero que no estoy relacionada directamente con nuestro sistema, es decir, que el atacante no la pueda corromper y que sea robusta”. Añade el directivo la necesidad de contar con una solución de parchado de sistemas físico y virtual, como puede ser la solución de Virtual Patching de Trend Micro. “No demos acceso libre a internet, ni a usuarios ni al sistema”, recomienda José de la Cruz, añadiendo que es necesaria una formación y concienciación del usuario y una supervisión continua.

En la parte de protección contra las amenazas de seguridad, incluido el ransomware, Trend Micro cuenta con diferentes productos para cada una de las fases de un ataque: entrada, infección, ejecución y limpieza. Entre la batería de productos menciona el directivo de Trend Micro un motor antispam, protección para la navegación, un buen motor antimalware que incorpore tecnología no solo basadas en machine learning sino en análisis de comportamiento, una sandboxing y una buena tecnología de EDR para la fase de limpieza “que nos aporte visibilidad de lo que está ocurriendo”.

Para la parte de concienciación se propone PhishInsight, una herramienta gratuita que permite hacer formación a los empleados y enseñarles cómo hacer frente a un ataque de phishing, por ejemplo.

Vea aquí la intervención de Trend Micro en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

PROTECCIÓN DEL LUGAR DE TRABAJO INTERRUMPIDO POR LA PANDEMIA

En un momento en el que muchas operaciones comerciales están inmovilizadas o incluso al borde del cierre, los cibercriminales continúan prosperando. Estos ciberdelincuentes se aprovechan de la crisis actual planteando nuevas amenazas y reforzando las existentes. Incluso con menos detecciones, el ransomware sigue siendo una amenaza a medida que los cibercriminales dotan con nuevas capacidades para apuntar a objetivos más grandes.

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

“Necesitamos un nuevo enfoque de seguridad que se fije más en el contexto”

El ransomware se ha convertido en una auténtica pesadilla para los responsables de ciberseguridad de las empresas. En la sesión online La Persistencia del Ransomware hablamos con Francisco José Verdugo, Senior Partner Solution Engineer de VMware, quien explica que nunca se ha tenido en cuenta sobre qué infraestructura se está ejecutando la amenaza, sobre qué usuario o dispositivo, a lo que se añade el problema de que “tenemos una cantidad ingente de vendedores de seguridad” y que siempre se ha hablado de una seguridad por capas. “La seguridad debe ser un deporte de equipo, que forme parte de la infraestructura, y que se centre en el contexto”, asegura Verdugo.

Desde VMware proponen un nuevo enfoque que se fije “en quién soy, con quién me hablo, dónde me estoy ejecutando, en qué sistema operativo estoy corriendo o dónde estoy para ser capaces de detectar ya no solamente lo co-

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

“Nunca se ha tenido en cuenta sobre qué infraestructura se está ejecutando la amenaza, sobre qué usuario o dispositivo”

nocido, sino también lo desconocido”, explica el directivo. A nivel de red se cuenta con NSX; en la parte de Cloud en relación con toda la parte de gobernanza con una solución que se llama Secure State; para la parte de cargas de trabajo y servidores virtuales la propuesta de VMware es vSphere; para gestionar la seguridad de los dispositivos, controlar aplicaciones y el control de identidades y de usuarios se utiliza Workspace One.

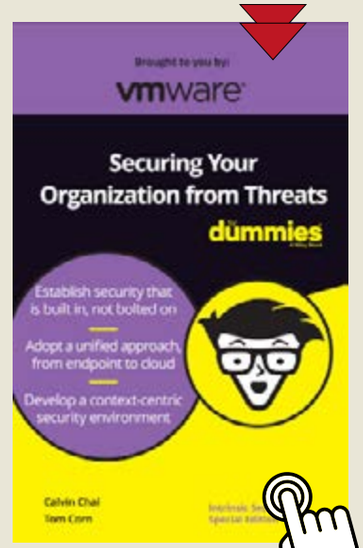
¿En qué consiste la Seguridad Intrínseca? “En dar de base esa capa de seguridad que en este caso proporciona Carbon Black, una compañía que se compró en agosto de 2019 y cuya inteligencia se está integrando en los distintos ámbitos”. Y la compra de Octarine, ¿cómo impacta en esta visión de la ciberseguridad? Explica Francisco José Verdugo que las aplicaciones de nueva generación siguen un modelo basado en contenedores donde los modelos de seguridad son muy distintos, “Octarine viene a cubrir una necesidad dentro de ese ámbito por su capacidad de proteger un entorno Kubernetes en cualquiera de las fases de vida”. Volviendo a la filosofía de una única consola, de una gestión simplificada, por lo que se opta es por integrar toda la funcionalidad de Octarine dentro de Carbon Black.

Sobre el ransomware dice el ejecutivo de VMware que “podemos decir que tenemos un cien por cien de efectividad contra él”. Propone además una serie de buenas prácticas que van desde la creación regular de copias de seguridad, aplicar los parches, utilizar antivirus de nueva generación capaz de detectar ataques que no estén en la memoria, o implementar programas de formación o concienciación.

Vea aquí la intervención de VMware en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

SEGURIDAD INSTRÍNSECA FOR DUMMIES



La seguridad intrínseca es un enfoque fundamentalmente diferente para proteger su negocio. No es un producto, una herramienta o un paquete para su organización, sino una estrategia para aprovechar su infraestructura existente y puntos de control de nuevas formas, en tiempo real, en aplicaciones, nubes y dispositivos.

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

“Se necesitan herramientas de nueva generación capaces de detectar comportamiento”

El 59% de los ataques con éxito cifraron datos que estaban almacenados en la nube pública. Durante la sesión online La Persistencia del Ransomware Alberto Rodas, Sales Engineer Manager Iberia Region de Sophos, asegura que la mitad de las empresas sufren un ataque de ransomware que tiene éxito en el 73% de las ocasiones. Añade el directivo que el coste promedio de la remediación de estos ataques son unos 760 mil dólares, que afectan a todos los sectores y que se utilizan múltiples técnicas para tener éxito.

El ataque de ransomware típico acaba con el cifrado de datos, algo que a menudo ocurre durante el fin de semana o aprovechando algún festivo, y suele iniciarse con un correo o enlace malicioso que afecta a un puesto, desde el que empieza a extenderse.

Propone Alberto Rodas unas buenas prácticas contra el ransomware, empezando por contar con una buena solución de seguridad.

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

“El ataque de ransomware típico acaba con el cifrado de datos, algo que a menudo ocurre durante el fin de semana”

Menciona el directivo de Sophos que muchas empresas cuentan con productos obsoletos, basados sólo en firmas y que se necesitan herramientas de nueva generación capaces de detectar comportamiento y detectar técnicas de explotación.

Se debe reducir la superficie de ataque, por lo que “si no necesito ciertos servicios, hay que quitarlos”. Una tercera buena práctica es el uso de VPN para accesos remotos de forma que nunca exponga mis sistemas a internet. El uso de autenticación multifactor es importantísimo, dice Alberto Rodas, así como prevenir los movimientos laterales.

Propone el directivo una arquitectura de red con Sophos XG Firewall y Sophos Intercept X EDR capaz de identificar todo lo que está ocurriendo en la red de la empresa, e incluso la monitorizando de aplicaciones cloud, pudiendo decir “cuáles son las permitidas y cuáles no”.

A nivel de puesto de trabajo se cuenta con Sophos Intercept X con capacidades de detección en tiempo de ejecución y control de comportamiento para detectar esa ejecución de ransomware, la propagación o el cifrado no deseado. “Pero además tenemos los servicios de detección y respuesta, donde con el módulo EDR el cliente puede realizar acciones, o hacerlas nosotros a través de Managed Threat Response, nuestro servicio de EDR gestionado”.

Muy interesante también la parte de Threat Hunting, un servicio en el que Sophos ha pre-establecido una serie de queries que se pueden adecuar a las necesidades de cada cliente.

Vea aquí la intervención de Sophos en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

MEJORES PRÁCTICAS PARA BLOQUEAR EL RANSOWMARE

Uno de los métodos más efectivos para protegerse contra los ataques de ransomware es con una solución de protección de endpoints configurada correctamente. En este documento técnico, analizaremos cómo funcionan los ataques de ransomware, cómo se pueden detener y las mejores prácticas para configurar su solución de punto final para la protección más sólida posible.

it TRENDS

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

“Hemos visto todo tipo de estrategias para conseguir ataques cada vez más dirigidos”

El 50% de los responsables de ciberseguridad está convencido de que su empresa pagaría un rescate para evitar la publicación de sus datos. Durante la sesión online La Persistencia del Ransomware hablamos con Sergio Martínez, responsable de SonicWall para la región de Iberia, sobre ransomware y lo que está ocurriendo en el mundo de la seguridad. Dice el directivo que esta pandemia ha sido una bendición para los cibercriminales, ya que “mientras que las empresas y las organizaciones tenían que dedicarse a sobrevivir, los cibercriminales han estado sacando tajada de esto”.

Según los informes de SonicWall, el ransomware está creciendo globalmente. Durante la pandemia “hemos visto todo tipo de estrategias para conseguir ataques cada vez más dirigidos y sobretodo basados en ransomware”, dice el directivo, explicando también que el RTDMI de la SonicWall, el algoritmo desarrollado por la compañía para realizar detecciones a nivel de sand-

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

“Hemos identificado una serie de productos y servicios que necesitan las empresas y hemos construido un SMB Pack para pymes”

boxing, ha detectado más de 120.000 variantes de malware nunca identificados. El informe de la compañía recoge también un crecimiento de los ataques a puertos no estándar así como de las amenazas encriptadas.

La propuesta Boundless Cybersecurity de la compañía se basa en el gap hay que entre lo que se necesita a nivel de seguridad y el presupuesto que pueden invertir las empresas para: conocer lo desconocido; tener un punto de visibilidad y control sobre lo que está sucediendo y ayudar a las empresas con estrategias y dispositivos que sean asumibles por los clientes.

“Hemos identificado una serie de productos y servicios que necesitan las empresas y hemos construido un SMB Pack para pymes”, asegura Sergio Martínez, diciendo que la idea es juntar un firewall fácil de instalar con un software para gestionarlo todo; un punto de acceso o puntos de acceso; un switch POE para dar alimentación a los puntos de acceso; seguridad para Office 365 y una antivirus de nueva generación, todo esto en una oferta basada en componentes.

Recuerda también Sergio Martínez que se ha lanzado recientemente la Generación 7 de los productos de la compañía; “se ha renovado nuestro sistema operativo y nuestro hardware”. Entre las mejoras el multiplicar el rendimiento de dispositivos “por dos, por tres, incluso por cuatro, con softwares para configurarnos en remoto”. Recientemente se han presentado los nuevos switches, que se gestionan también desde el mismo punto de gestión en la nube. La última línea de defensa es Capture Client, un antivirus basado en lo mejor del mercado “que añade nuestros algoritmos de detección de malware para tener un gran producto que dar seguridad a nuestros clientes”.

Vea aquí la intervención de SonicWall en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

INFORME SOBRE CIBERAMENAZAS 2020 DE SONICWALL

El Informe sobre Ciberamenas 2020 de SonicWall proporciona información detallada y un análisis exhaustivo del panorama de ciberamenazas. Entre los principales hallazgos del informe destaca que los ataques de ransomware dirigido están creciendo, que el cryptojacking continúa desmoronándose o que el Internet de las Cosas (IoT) es un tesoro para los ciberdelincuentes.

it TRENDS

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

“Hay que distinguir entre el ransomware genérico y el dirigido, mucho más peligroso”

El ransomware también está presente en la plataforma Android; entre los primeros ataques, uno detectado en Canadá bajo el disfraz de una aplicación de rastreo COVID-19. En la sesión online La Persistencia del Ransomware dice Josep Albors, responsable de investigación y concienciación de ESET España, que muchas personas y empresas siguen pensando en el ransomware como una amenaza que no ha variado en años. Sin embargo, “estamos hablando de una amenaza que no ha dejado de evolucionar en este tiempo y que ahora tiene muchas familias, muchas variantes y nuevas y peligrosas consecuencias”, asegura el directivo explicando que en un ataque de ransomware hay varias etapas, desde la explotación o infección, que les permite colarse en la empresa, para pasar a una segunda fase en la que el ransomware hace un reconocimiento de la red empresarial para ver qué equipos o qué información es más interesante para robarla y enviarla a los servidores controlados por delincuentes. Y una fase final que es la extorsión

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

“Hemos pasado de una amenaza cuyo máximo temor por parte de los usuarios era que te cifren los archivos, a una amenaza cuyo miedo actual es que los archivos sean robados y filtrados”

o filtrado de datos, lo que coloca a las empresas a un paso de incumplir normas como GDPR. “Emotet es una de las variantes que hemos visto evolucionar en base a este nuevo modelo de negocio”, dice Jose Albors.

Respecto a los vectores de ataque que utiliza el ransomware, el principal, asegura Josep Albors, es el compromiso mediante RDP, o escritorio remoto, muy explotado debido al aumento por el teletrabajo, seguido del phishing y las vulnerabilidades de software.

“Hay que distinguir entre un rasomware genérico, que una pyme podría afrontar, incluso un usuario particular, en el que hay un ataque clásico de cifrado, y los ataques dirigidos”, explica el directivo de ESET añadiendo que se ha visto un aumento muy elevado de ataques dirigidos a empresas multinacionales con una facturación muy elevada y que son víctimas de este tipo de ataques dirigidos, y algunos sectores, como la administración pública, infraestructuras sanitarias, centros de investigación o infraestructuras críticas.

Habla también Josep Albors del Ransomware como servicio, y explica que los ciberdelincuentes se dedican a crear kits de generación de ransomware para que otros delincuentes con mucho menos conocimiento técnico, o directamente sin apenas conocimiento técnico, puedan con unos cuantos clicks crear su propia amenaza y empezar a ganar dinero.

Termina el directivo de ESET ofreciendo una serie de consejos para hacer frente al ransomware: contar con una buena copia de backup; tener la información cifrada para que al usuario no le sirva de nada; y contar con una solución para la monitorización de la actividad de la red para detectar posibles amenazas.

Vea aquí la intervención de ESET en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

it whitepapers

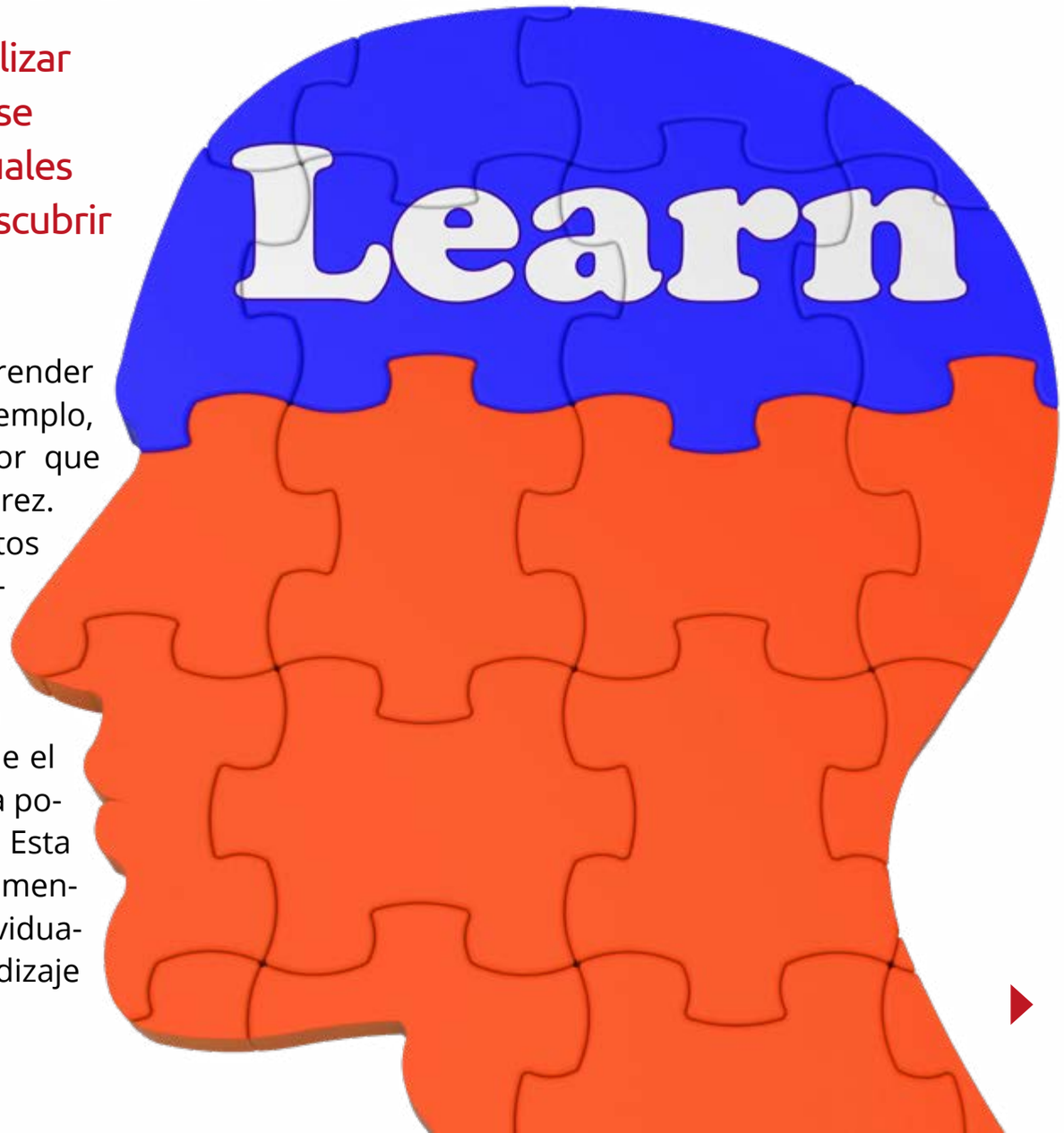
RANSOMWARE DESDE EL PUNTO DE VISTA EMPRESARIAL

Los objetivos de este documento son explicar por qué el ransomware sigue siendo una amenaza grave para su organización, independientemente de su tamaño, y qué puede hacer su organización para reducir la exposición y el daño de los ataques de ransomware.

itTRENDS

Inteligencia Artificial: explotando sus capacidades

La Inteligencia Artificial es la capacidad de un ordenador para realizar tareas comúnmente asociadas con seres inteligentes. El término se aplica al desarrollo de sistemas dotados de los procesos intelectuales característicos de los humanos, como la capacidad de razonar, descubrir significados, generalizar o aprender de experiencias pasadas.



Desde que se comenzó a desarrollar la informática, se ha demostrado que los ordenadores se pueden programar para realizar tareas muy complejas, como, por ejemplo, descubrir pruebas de teoremas matemáticos. Pero ¿qué es la inteligencia? Los psicólogos no caracterizan la inteligencia humana por un solo rasgo, sino por la combinación de muchas habilidades diversas. La IA se ha centrado principalmente en los siguientes componentes de la inteligencia: aprendizaje, razonamiento, resolución de problemas, percepción y uso del lenguaje.

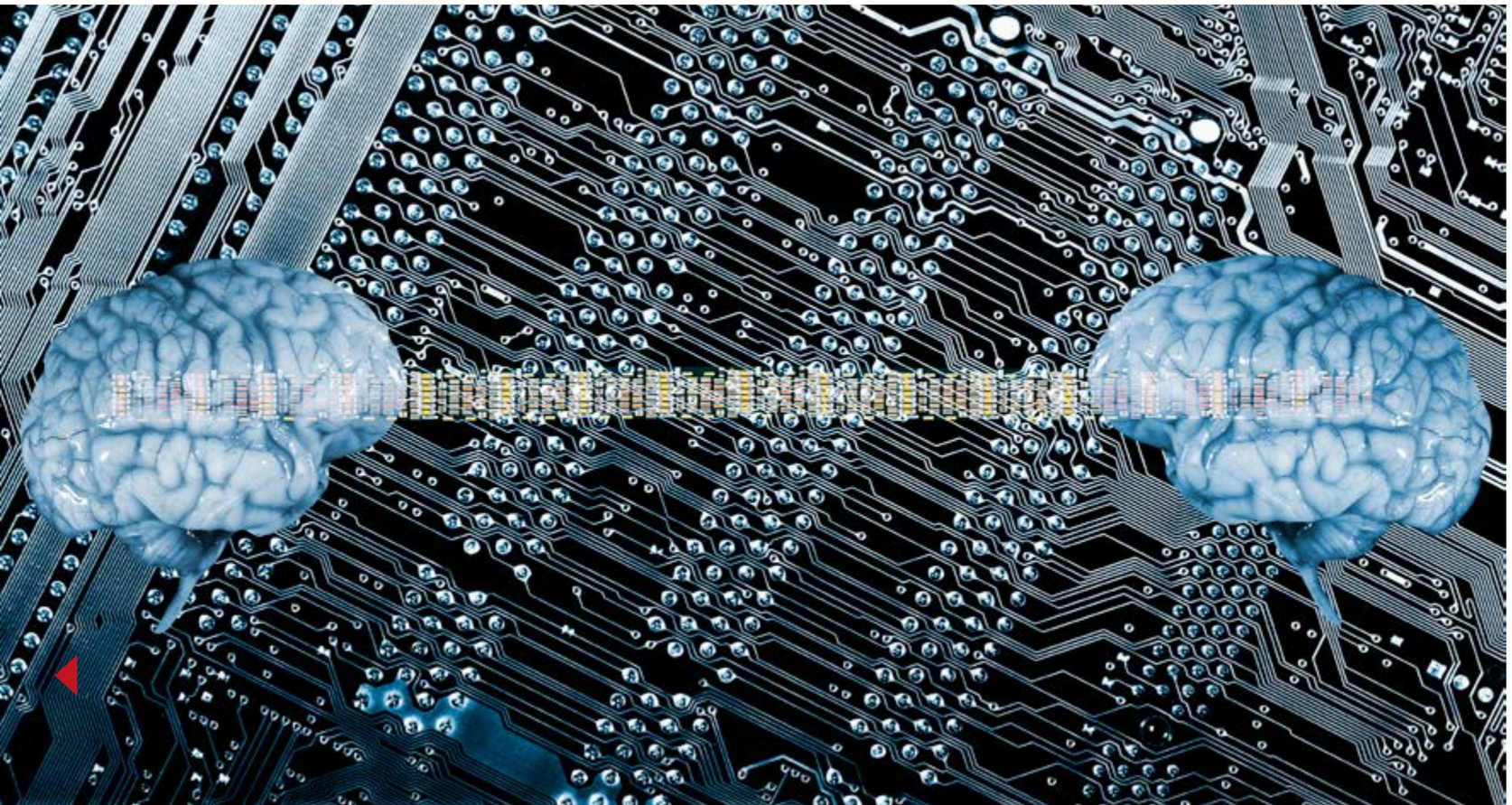
- **Aprendizaje:** Hay varias formas diferentes de aprendizaje aplicadas a la inteligencia artificial. El más simple es aprender por ensayo y error. Por ejemplo, un programa de ordenador que resuelva problemas de ajedrez.

Podría intentar movimientos al azar hasta encontrar el jaque mate. Entonces, el programa podría almacenar la solución con la posición para que la próxima vez que el sistema encuentre la misma posición recuerde la solución. Esta simple memorización de elementos y procedimientos individuales, conocida como aprendizaje

de memoria, es relativamente fácil de implementar en un ordenador.

Más desafiante es el problema de la generalización, que implica aplicar la experiencia pasada a situaciones nuevas análogas. Por ejemplo,

La IA se ha centrado principalmente en los siguientes componentes de la inteligencia: aprendizaje, razonamiento, resolución de problemas, percepción y uso del lenguaje



un programa que aprende el tiempo pasado de los verbos regulares en inglés de memoria no podrá producir el tiempo pasado de una verbo irregular nuevo, a menos que previamente se hayan introducido otras reglas.

❖ **Razonamiento:** Razonar es discurrir de manera adecuada en cada situación. Pueden ser deductivas o inductivas. La diferencia más significativa entre estas formas de razonamiento es que en el caso deductivo la verdad de las premisas garantiza la verdad de la conclusión, mientras que en el caso inductivo la verdad de la premisa apoya la conclusión sin dar una seguridad absoluta.

❖ **Resolución de problemas:** La resolución de problemas, particularmente en inteligencia artificial, puede caracterizarse como una búsqueda sistemática a través de una variedad de acciones posibles para alcanzar algún objetivo o solución predefinidos. En IA, los métodos de resolución de problemas se dividen en propósito especial y propósito general.

❖ **Percepción:** En la percepción, se escanea el entorno por medio de varios órganos sensoriales, reales o artificiales, y la escena se descompone en objetos separados en diversas relaciones espaciales. El análisis se complica por el hecho de que un objeto puede parecer diferente según el ángulo desde el que se ve, la dirección y la intensidad de la iluminación en la escena y cuánto contrasta el objeto con el campo circundante.

Actualmente, la percepción artificial está lo suficientemente avanzada como para permitir que los sensores ópticos identifiquen a las personas, los vehículos autónomos conduzcan a alta velocidad y los robots deambulen por las oficinas haciendo tareas menores.

❖ **Idioma:** Un idioma es un sistema de signos que tiene significado. En este sentido, el lenguaje no tiene por qué limitarse a la palabra hablada. Las señales de tráfico, por ejemplo, forman un lenguaje.

Una característica importante de los lenguajes humanos en toda regla, en contraste con

los gritos de los pájaros y las señales de tráfico, es su productividad. Un lenguaje productivo puede formular una variedad ilimitada de oraciones.

Es relativamente fácil diseñar programas que parezcan capaces de entender, en contextos específicos. Para responder con fluidez en un lenguaje humano a preguntas y declaraciones, por ejemplo. Aunque ninguno de estos programas comprende realmente el lenguaje, en principio pueden llegar al punto en el que su dominio de un lenguaje es indistinguible del de una persona.

IA APLICADA

Las máquinas no han tomado el control de nuestra vida, aunque así lo pronosticaban muchas novelas futuristas. Sin embargo, se han infiltrado en nuestros hábitos y rutinas. Si algo ha marcado la última década en materia tecnológica es la inteligencia artificial, que ayuda diariamente a millones de personas a hacer su trabajo más fácil y su ocio más ágil y variado. Desde asistentes personales con voz como Siri y Alexa, hasta tecnologías basadas en algoritmos de comportamiento, búsquedas web acorde a nuestras preferencias y vehículos autónomos que cuentan con capacidades predictivas. Pero también traducción de idiomas, chatbots en el ámbito sanitario y comercial, búsqueda e identificación de malware, recuento y clasificación de productos, videojuegos, realidad virtual...

Y es que, la Inteligencia Artificial ofrece un abanico enorme de aplicaciones posibles que ayudan a mejorar procesos internos de las compañías, aumentar la eficiencia y agilidad. Por ejemplo, la consultora CB Insights señala las industrias que más cambiaron a nivel mundial durante el año pasado por los sistemas de Inteligencia Artificial:

'Chatbots' médicos: la utilización de chatbots para la atención en línea es algo cada vez más cotidiano en países como EE.UU, tanto para la solución a preguntas médicas como para que los

ÉTICA E IA

Algunos gurús de la tecnología han tenido sus dudas sobre esta nueva ciencia. "Tenemos que ser super cuidadosos con la Inteligencia Artificial. Es potencialmente más peligrosa que las bombas nucleares", tuiteó Elon Musk en 2014. Un año después, le confesó a su biógrafo que su mayor preocupación era la posibilidad de que su amigo Larry Page, fundador de Google, estuviera creando un ejército de robots inteligentes para destruir la humanidad. Contaba el New York Times que Mark Zukerberg, fundador de Facebook, preocupado por estas y otras declaraciones similares le invitó a cenar para intentar tranquilizarle. Consideraba la actitud de Musk irracional, y temía que sus palabras despertaran una ola de iafobia. Pero según el diario, no funcionó. "Sigo creyendo de verdad que esto es muy peligroso", dijo en la mesa, según uno de los presentes.

La conclusión es sencilla: la IA es una herramienta positiva, pero ha de ser regulada. El marco de responsabilidad civil existente en Europa cubre la mayoría de los escenarios futuros en el ámbito de la IA, pero según vayan surgiendo nuevas herramientas, se expondrán varios problemas no resueltos. En el caso de un mal funcionamiento de la IA, por ejemplo, los expertos creen que será difícil diferenciar entre conducta negligente y no negligente. ¿Quién es exactamente responsable si un robot impulsado por IA hace daño a un peatón en un espacio público o comete un error en una cirugía? El Parlamento Europeo quiere proponer un mecanismo de trabajo que cubra todo el espectro de riesgos, así como los posibles daños causados por el uso de IA en sus diversas aplicaciones. Para asegurar que los avances benefician a toda la sociedad, es necesario un marco normativo acerca de qué principios éticos deben estar presentes necesariamente en la concepción, el desarrollo, implementación y funcionamiento de esta técnica.

usuarios localicen a los profesionales que mejor pueden atenderles. Este año están siendo de especial ayuda durante la pandemia de la covid-19.

Asistentes para la compra online: los bot se establecen cada vez más como el canal ideal para comercializar los productos en la Red, acompañando al cliente en todo el proceso de compra e, incluso, solucionando la mayoría de sus quejas. Desde el lado del consumidor, están ya en el mercado nuevos sistemas de tecnologías de búsqueda que personalizan aún más la información según sus preferencias, mientras que, desde la óptica de las marcas, la IA está permitiendo desarrollar sistemas para detectar de manera muy precisa las falsificaciones.

EL ORIGEN DE LA IA

Los científicos llevan décadas discutiendo sobre los orígenes de la IA. Hay cierto consenso en que Warren McCulloch y Walter Pitts descubrieron esta ciencia en 1943 tras un trabajo en el que propusieron el primer modelo de red neuronal artificial. Era un modelo bastante simple, pero McCulloch y Pitts demostraron que era capaz de aprender y responder funciones lógicas. El estudio de las redes neuronales sufrió un parón hasta que a mediados de los 80 se retomó la investigación.

El siguiente intento de definir Inteligencia Artificial lo hizo el matemático Alan Turing, considerado el padre de la computación y conocido por la máquina de Turing. Es decir, el modelo conceptual que utilizó para formalizar los conceptos del modelo computacional que seguimos utilizando actualmente. Este científico inglés demostró que las operaciones básicas que podía desarrollar su máquina, podía codificarse con cualquier algoritmo.

En 1950 publicó un artículo llamado Computing Machinery and Intelligence donde argumentaba que si una máquina puede interactuar como un humano, se puede decir que es inteligente.

Pese a los años que han pasado, el test de Turing es de vital importancia en el campo de la IA, ya que exige una serie de capacidades a la máquina, que a grandes rasgos, define lo que es inteligencia artificial actualmente. Una máquina que sea capaz de pasar el test de Turing ha de tener la capacidad de reconocer el lenguaje natural, razonar, aprender y representar el conocimiento.

Pagos: el aprendizaje automático aplicado al reconocimiento de imagen también está generando nuevos servicios como el de Amazon Go, que permite a los clientes pagar por productos en tiendas físicas sin pasar por caja, gracias a sistemas que identifican al usuario y los productos, y realizan el cobro de manera automática.

Prótesis inteligentes: en el campo de las prótesis, los científicos están realizando grandes progresos debido a los modelos de aprendizaje automático que, por medio de sensores adheridos al cuerpo, reciben y procesan datos y sirven para que se desarrollen comandos que hacen que los dispositivos se muevan casi inmediatamente. En la investigación clínica, la IA ya permite que se extraiga información valiosa de los registros médicos para sugerir ensayos relevantes.

Asistentes de viaje: el valor agregado de los chatbots es algo que perciben hoy los clientes a través del asesoramiento en las reservas, de las sugerencias que se les realizan online, de los asistentes virtuales o a la hora de valorar cualitativamente las opiniones recibidas.

Diagnósticos por IA: el supervisor sanitario norteamericano (FDA) ha dado luz verde a proyectos que utilizan la IA con dispositivos médicos, por ejemplo, para mejorar los diagnósticos mediante reconocimiento de imágenes.

IA en la banca: en el mundo de la banca, la IA ya ha demostrado su potencial. Cada vez son más habituales las herramientas de reconocimiento por voz, facial, chatbots etc.

EL FUTURO DE LA IA

Los CIO seguirán priorizando la evolución de sus compañías hacia modelos digitales. De todos ellos, es la inteligencia artificial, junto al desarrollo e implantación de soluciones colaborativas, la prioridad de inversión más importante para este 2020.

Según el informe IT Trends 2020, el año de la consolidación digital, un 18% de los consultados considera que la Inteligencia Artificial y el Machine Learning se aplicarán a corto plazo en sus negocios, y un 12% ya tiene estos avances implantados en su empresa. Este último porcentaje también apuesta por Blockchain, y el 10% por los Chatbots.

De acuerdo a las últimas estimaciones de ABI Research, el mercado de servicios de IA/ML para IoT se prepara para crecer con rapidez en los próximos años, pasando de los 1.090 millones de dólares estimados para este año a unos 10.600 millones para 2026. Esto se logrará gracias a que los proveedores de tecnologías IoT están facilitando a sus clientes el acceso a tecnologías de inteligencia artificial y aprendizaje automático para extraer más valor de los datos. Y esto incluye tanto las instalaciones locales como las infraestructuras perimetrales, la nube, las ofertas de Plataforma como Servicio (PaaS) y las ofertas de Software como Servicio (SaaS). ■

MÁS INFORMACIÓN

- Los sistemas de diagnóstico y monitorización ocular se expanden gracias a IoT y la IA
- La Armada Española moderniza el mantenimiento de sus buques con inteligencia artificial
- La videovigilancia evoluciona gracias a la inteligencia artificial
- Inteligencia artificial para mejorar los sistemas de riego

Si te ha gustado este artículo, compártelo

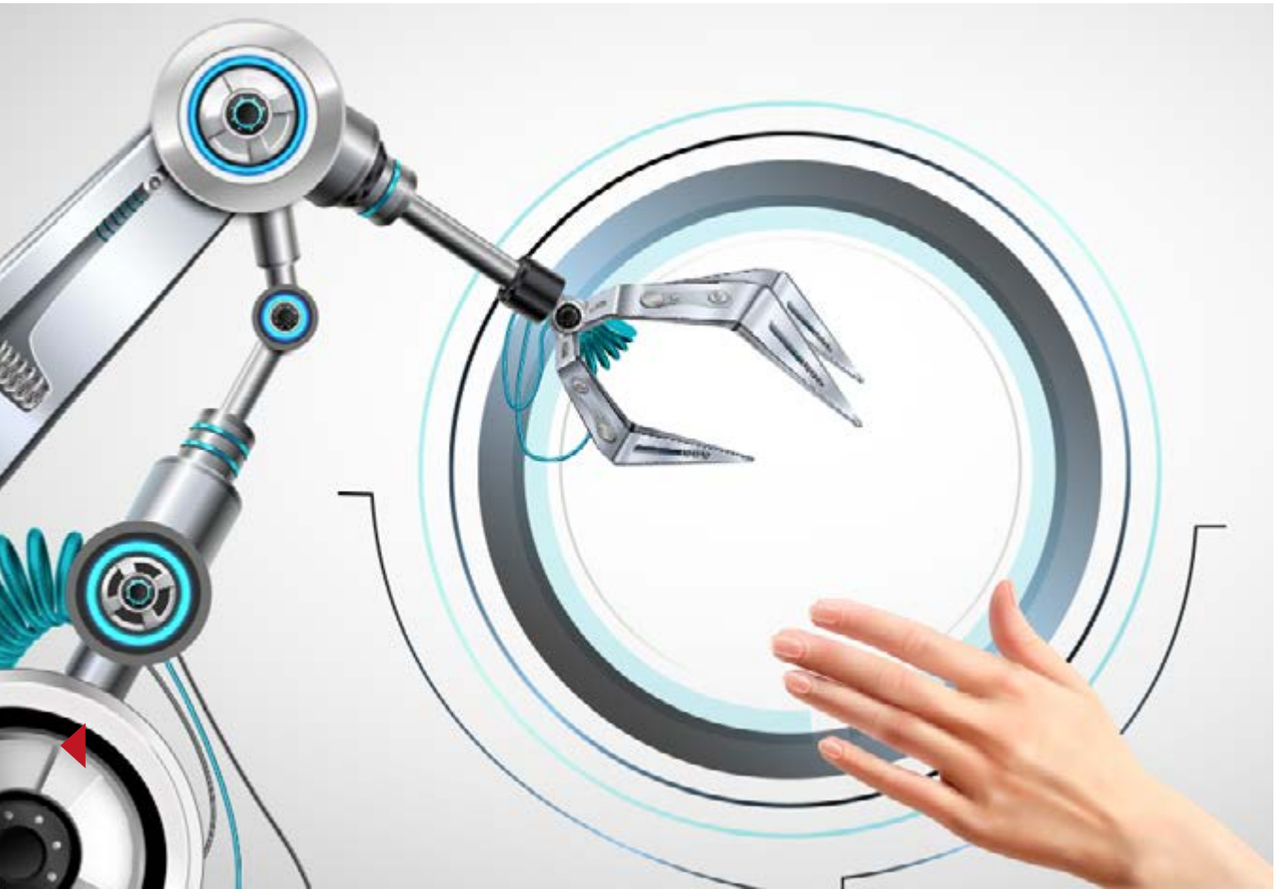
#ITWEBINARS

Inteligencia Artificial, ¿cómo lo aplico en mi empresa?

Inteligencia Artificial, aprendizaje automático, robotización y automatización, permiten la generación de máquinas y procesos inteligentes que funcionan casi como los humanos, y que son capaces de entender mejor a los clientes, de extraer información de los datos de una manera más eficaz, de optimizar los procesos empresariales o de gestionar de una manera más eficiente el despliegue de recursos.

El interés por la IA crece y las organizaciones tienen planes para implementarlos en sus empresas. Se prevé que entre 2020 y 2024 el gasto en IA pasara de 50.100 millones de dólares a 110.000 millones.

En este IT Webinars titulado Inteligencia Artificial, ¿cómo lo aplico en mi empresa?, Automation Anywhere y Micro Focus abordan el mercado, los tipos de Inteligencia Artificial y las aplicaciones de cada una de ella en el ámbito empresarial. Puedes ver la sesión completa aquí o leer a continuación sus conclusiones. ■



Si te ha gustado este artículo, compártelo

Gerardo Murias, Automation Anywhere

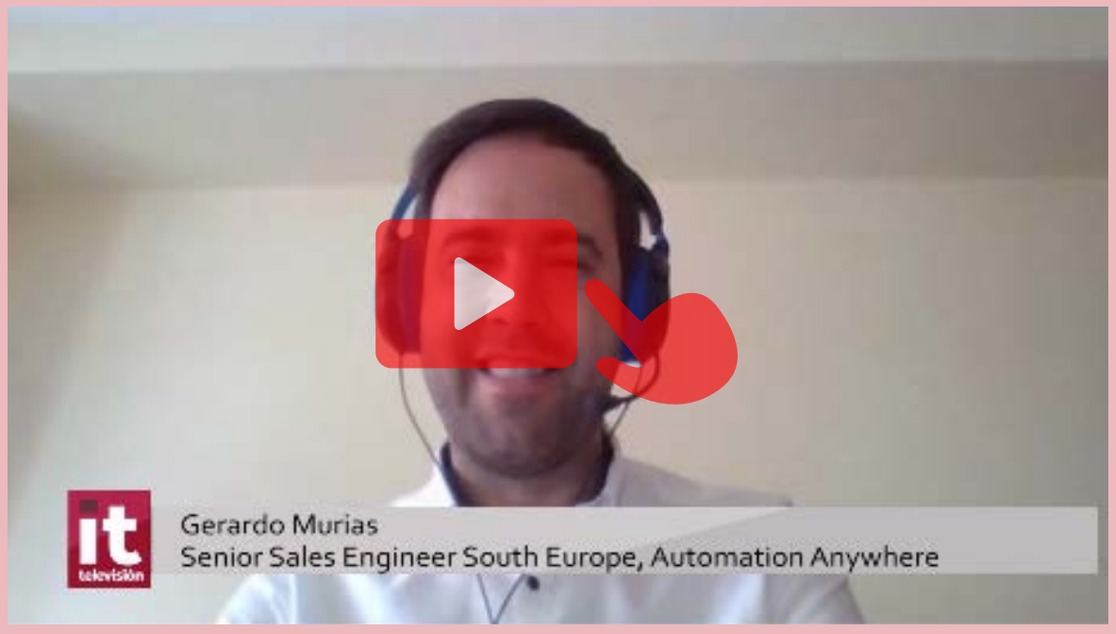
Ramsés Gallego, Micro Focus

it TRENDS

GERARDO MURIAS, INGENIERO DE VENTAS PARA EL SUR DE EUROPA, AUTOMATION ANYWHERE

“La combinación de IA y RPA ofrece a las empresas una ventaja competitiva”

Mejoras en los procesos, mayor automatización, innovación, rapidez y precisión, son algunos de los beneficios que la aplicación de la Inteligencia Artificial puede aportar a las organizaciones, y muchas están viendo su empleo con interés. “El 80% de las empresas en Europa consideran prioritaria la incorporación de IA”, explicó Gerardo Murias, ingeniero de ventas para el sur de Europa de Automation Anywhere durante el webinar Inteligencia Artificial, ¿cómo lo aplico en mi empresa? Sin embargo, “solo el 8% de países la están utilizando de forma efectiva. En EE UU ya hay un verdadero aumento de productividad en mejora de procesos con la aplicación práctica de la IA”.



GERARDO MURIAS, INGENIERO DE VENTAS PARA EL SUR DE EUROPA, AUTOMATION ANYWHERE

Para entender bien el concepto de Inteligencia Artificial y sus aportaciones, Murias explicó que “no es lo mismo Automatización que automatización inteligente, ni esto es lo mismo que la hiper automatización, ni ésta lo mismo que la fuerza de trabajo digital”. “La automatización inteligente es una herramienta que permite a los usuarios de una empresa ser capaces de automatizar sus procesos end-to-end, que puedan obtener métricas de analítica inmediatas y también añadir una capa extra mediante IA capaz de usar esos datos para aportar ventajas competitivas”, dijo.

Esta automatización inteligente se apoya en la RPA, que permite automatizar procesos de negocio tediosos o de mucho volumen de trabajo. “Un robot que tenga su propio asistente artificial ayuda a las empresas para que los trabajadores puedan enfocarse en tareas de mayor valor añadido. Es un paso más allá porque hay datos no estructurados que pueden venir de un correo electrónico, con una estructura no siempre predecible y un robot puede ocuparse de ello sin interacción humana. La fuerza de trabajo digital es la suma de todo. Un robot controlado por un humano, que procesa las tareas más tediosas de 7 a 10 veces más rápido”, explicó el ingeniero.

A su vez, se suma la inteligencia predictiva, que se emplea para tareas como registro de alumnos en universidades, clasificación de imágenes, e-learning, Deep learning... "La intersección entre RPA y IA podría dar lugar a aplicaciones para el reconocimiento facial y del habla, redes neuronales, aprendizaje profundo etc. Los bots cognitivos son RPA con computación cognitiva y la computación cognitiva libera a los bots de los límites de tareas y datos predefinidos y estructurados", prosiguió Murias. Y es que los bots, por sí solos, solo pueden realizar acciones específicas. "Por ejemplo un usuario del departamento de facturación que trabaje con un correo de Outlook que lleve un Excel y que tenga que procesar asientos contables. Puede reconocer cada fila de Excel, descargar el archivo etc. A nivel de diferentes áreas de negocio, la mayor parte de los datos no son estructurados, pero los bots no pueden juzgar situaciones ambiguas. En ese sentido entra la fuerza de trabajo digital y la capacidad de integrar la IA en un proceso de automatización", detalló.

La plataforma de Automation Anywhere replica las acciones que un humano tomaría, más la parte cognitiva que es añadir datos no estructurados. Además, incluye análisis inteligente para añadir competitividad al negocio. "IQ bot es decir datos y estructura; es la parte de nuestra herramienta end-to-end que procesa los datos no estructurados y semiestructurados y que, mediante aprendizaje por refuerzo, crea modelos de trabajo que permiten a un robot aprender una tarea y hacer una extracción inteligente de datos para ponerlos en un CSV, un Excel... Es aprendizaje sin supervisión con visión artificial, con lógica parcial. Aporta que el robot sea autónomo y su extracción de datos responde a un patrón", afirmó Murias.

La plataforma también cuenta con una capacidad de analítica que "procesa y analiza los datos a tiempo real y es capaz de saber las facturas que se han lanzado, el volumen medio de trabajo, la media de facturación que lleva en el mes para aportar ventaja competitiva...", añadió siguiendo con el ejemplo descrito en su intervención. Los casos de éxito de la empresa son aplicables a casi cualquier modelo funcional. "Trabajamos con empresas de banca y seguros, sanidad, fabricación.... Cuando aplicamos la RPA optimizamos los costos de trabajo, incrementamos la velocidad, la precisión y la disponibilidad, mejoramos el cumplimiento de los controles y la auditabilidad, proporcionamos inteligencia empresarial, transformación digital y mejora la moral de los empleados", comentó Murias.

En su intervención, el ingeniero de ventas de Automation Anywhere comentó el caso de ANZ Bank, donde en tres años han implementado más de 2.500 robots y actualmente continúan implementando 100 nuevos cada trimestre: "En banca, permite hacer un seguimiento automatizado de las actividades financieras de los clientes y se puede detectar fraude electrónico o cualquier anomalía. Encontrar brechas de seguridad en tarjetas de crédito, cuentas bancarias... para ello se analizan enormes cantidades de datos sin errores que cuando son miles de datos, un humano puede equivocarse".

Puedes ver la intervención de Automation Anywhere aquí. ■

it whitepapers

AUTOMATIZACIÓN CON INTELIGENCIA ARTIFICIAL, LA CLAVE DEL ÉXITO DE RPA

Primero vinieron los bots: robots de software creados con herramientas de automatización para ejecutar tareas definidas. Estos bots han aumentado la eficiencia, la productividad y la rentabilidad en todas las industrias a nivel mundial. Pero, en la actualidad, la RPA ya no se limita a las tareas y datos predefinidos.

Si te ha gustado este artículo, compártelo

RAMSÉS GALLEGO, DIRECTOR DE SEGURIDAD, RIESGOS Y GOBERNANZA EN MICRO FOCUS

“Cuando un robot ha visto billones de veces una imagen y crea un patrón de comportamiento, puede indicar lo que es mejor hacer en una compañía”

La Inteligencia Artificial lleva años desarrollándose gracias a la suma de diferentes técnicas. Ramsés Gallego, Director de Seguridad, Riesgos y Gobernanza en Micro Focus, explicó durante la sesión Inteligencia Artificial, ¿cómo lo aplico en mi empresa?, de qué manera la IA que hoy conocemos suponía una nueva revolución. “En la Revolución Industrial, las máquinas se diseñaron para amplificar y expandir la capacidad humana y la Inteligencia Artificial como la conocemos hoy ayuda a amplificar y orquestar las capacidades humanas cuando tienen que ver con procesos de automatización y lidiar con muchas fuentes de información a la vez”, explicó, para posteriormente identificar los cuatro tipos de inteligencia artificial: supervisado, no supervisado, aprendizaje reforzado y aprendizaje profundo. “Las aplicamos a gestión de servicio para descubrir patrones de comportamiento, para ver cómo se resuelve rápidamente un incidente, el patrón de acceso de un perfil... Cuando un robot ha visto billones de veces una imagen o se ha creado un patrón de comportamiento, puede indi-

RAMSÉS GALLEGO, DIRECTOR DE SEGURIDAD, RIESGOS Y GOBERNANZA EN MICRO FOCUS

car lo que es mejor hacer en una compañía. También puede detectar comportamientos anómalos o no adecuados y prevenir daños", dijo el experto.

Gracias a estas tipologías de IA, empresas como Micro Focus descubren patrones en la línea de seguridad o carga de pruebas, lo que les facilita la detección de anomalías en el código o de incidentes de seguridad. "Es imposible que una persona haga pruebas funcionales en más de 200 plataformas diferentes como aplicaciones móviles, la nube, mainframe, CRM … Para eso los algoritmos son fundamentales", prosiguió Gallego.

"Los humanos tenemos problemas o estamos cansados o tenemos errores, y las máquinas no. La máquina, 24 horas 7 días a la semana, no tiene un mal día. El algoritmo nunca se equivoca. Hace lo que tiene que hacer de manera incansable. Las cargas de trabajo disminuyen, nos aportan retroalimentación también y casi en tiempo real", añadió.

Con esta ayuda, una empresa puede plantearse qué tareas necesita mejorar y hacerse varias preguntas. "¿Por qué hago esto, para controlar los costes, el riesgo, mejorar el servicio interna o externamente? A partir de ahí, hay que ver qué procesos de grandes volúmenes o transacciones puedo automatizar. Cuántos de ellos tienen que ver con información e incluso preguntarnos qué es lo que no conocen los entornos que han ido creciendo en la empresa como el departamento de riesgo o de desarrollo. No conozco a nadie que pueda lidiar con trillones de eventos al día, pero conozco algunos algoritmos sí pueden hacerlo", recalcó el portavoz de Micro Focus.

La IA que implementa Micro Focus puede aplicarse a casi todos los sectores. "Ayudamos en múltiples dimensiones. Seguridad, identificación de patrones, amenazas, descubrimiento de vulnerabilidades, controles inadecuados, datos a los que alguien no debe tener acceso… En la línea de gestión al servicio, identificación con una foto para saber quién ha usado algo, observar el problema, la ubicación, quién ha sido la última persona que ha accedido… Ayudamos en el mainframe, la nube, gestión de servicio, gestión de bases de datos, seguridad en el entorno financiero, hospitalario, educativo, de seguros, de gobierno. En resumen, no solo transformación digital sino transformación radical", matizó Gallego. "El futuro tiene que ver con que esos sistemas bien orquestados dan beneficios a la compañía y reducen el perímetro de riesgo. Es el futuro del ahora", concluyó.

Puedes ver la intervención de Micro Focus en este webinar sobre Inteligencia Artificial, aquí. ■

LA IMPORTANCIA DE LAS OPERACIONES DE ANÁLISIS EN IT

La Analítica de Operaciones de TI facilita el trabajo diario de TI. Los especialistas en operaciones de TI deben estar familiarizados con los tipos de análisis que se utilizan cada vez más en su industria. Han de aprovechar cualquier capacidad analítica que esté incorporada en sus herramientas, y deben saber cuándo buscar orientación de otros equipos de la organización como seguridad, big data, equipos de inteligencia empresarial, etc, cuando tengan preguntas o quieran mejorar sus habilidades analíticas.

Si te ha gustado este artículo, compártelo

itTRENDS

Ayúdanos a conocer la realidad digital

COVID-19, ¿cuánto y cómo ha influido en las estrategias de TI?

¡PARTICIPA!

en nuestra Encuesta

itRESEARCH

it TRENDS

7 pasos para apreciar el valor de las aplicaciones modernas

Antonio Gallego,
Senior Manager, Solution Engineering, Kubernetes en VMware EMEA

La interrupción masiva de nuestra actividad que acabamos de vivir, así como las disrupciones que seguimos experimentando, pueden haber alterado la vida tal y como la conocemos, pero algunas cosas permanecen inmutables. El negocio define tanto objetivos como estrategias, y TI responde en consonancia creando tanto las aplicaciones como los servicios, así como las experiencias que, por un lado, los clientes demandan y, por otro, los empleados necesitan.

Ser capaz de modernizar las aplicaciones de la empresa significa poder entregarlas rápidamente, con confiabilidad y seguridad, ya sea en la nube nativa que use el negocio o en las distintas nubes que TI gestiona, ya sea en el centro de datos o en un entorno repartido por múltiples nubes. Las empresas entienden que, sin estos servicios, satisfacer las necesidades de los clientes será muy difícil: una reciente encuesta de VMware descubrió que el 80% de líderes tecnológicos y de desarrollo de aplicaciones de EMEA creen que, de no modernizar con éxito las aplicaciones, las organizaciones no podrán ofrecer la mejor experiencia a sus clientes.

De hecho, no solo las aplicaciones modernizadas ayudan a las empresas a ofrecer mejores resultados, sino que las empresas que cuentan con un mayor rendimiento han demostrado ser las que desarrollan y ponen a disposición de los usuarios nuevas aplicaciones y servicios a gran velocidad. El estudio confirmó que dos tercios (66%) de las nuevas aplicaciones llegan a los entornos de producción en las empresas de alto rendimiento, en comparación con el 41% correspondiente a organizaciones con un menor rendimiento. Asimismo, el 70% de las entregas o cambios en las aplicaciones llegan a producción en el plazo previsto para las organizaciones de alto rendimiento, frente a

solo el 41% para las organizaciones de menor rendimiento.

El objetivo de dar soporte y modernizar aplicaciones heredadas mientras se adoptan nuevas prácticas relacionadas con aplicaciones nativas desplegadas en la nube, ha obligado a TI a replantearse cómo gestionar tanto las unas (las heredadas) como las otras (las modernas), teniendo que hacerlo, además, de forma segura, en un mundo de múltiples nubes. Para acelerar el ritmo de innovación, los departamentos de TI deben simplificar las operaciones y la administración.

¿Por dónde empezar? El punto de partida suele ser siempre establecer el valor que la aplicación debería entregar a la empresa, si bien esto deriva en más preguntas, las cuales deben responderse tanto para que TI sepa dónde y cómo 'ejecutar todas las cosas' (traducción literal de lo que en VMware llamamos "run-all-the-things"), como para que las empresas entiendan el valor que sus aplicaciones modernas deberían tener para el negocio.

1 ¿Cuáles son las prioridades y el enfoque del negocio digital?

Tradicionalmente TI ha identificado a la empresa como su cliente interno. Con el tiempo ha derivado en una denominación inapropiada e incluso incorrecta. Ahora los clientes de TI pueden elegir, es decir, pueden usar otros proveedores si no están satisfechos con el servicio. Antaño las empresas no tenían esa flexibilidad; estaban "atrapadas" con lo que les daba TI: incluso algunas se consideraban casi rehenes, en vez de clientes.

Una vez que se haya acordado un plan de actuación, los equipos de TI deben tener claro cómo van a cumplirlo

Poco a poco, la tecnología ha permitido muchas más opciones y las unidades de negocio se han ido dando cuenta de que tenían acceso a la última tecnología en la misma medida que TI y a veces más. Por lo tanto, si TI no da el servicio esperado, un jefe de departamento o de unidad de negocio puede buscar los recursos que necesita en otro lugar, con todos los riesgos que esto conlleva para la empresa.

Ahora TI tiene que servir a la empresa como un cliente real, no cautivo: comprender sus necesidades, sus desafíos y sus objetivos y demostrar cómo TI puede apoyar esas ambiciones. Es una conversación bidireccional en la que las unidades de negocio y los equipos de infraestructura hablan un idioma común y se ayudan mutuamente a comprender lo que ambos intentan lograr.

2 ¿Qué aplicaciones hay que poner en funcionamiento?

Liderar desde ese entendimiento es tener claro qué aplicaciones se necesitan y qué soporte hay que prestar. Es una conversación a mantener con las unidades de negocio y, de hecho, con cualquier persona relevante dentro de la empresa. La decisión resultante debe ser tanto comercial como técnica.

Una vez que se haya acordado un plan de actuación, los equipos de TI deben tener claro cómo van a cumplirlo. Para empezar, ¿cuentan con el equipo adecuado? Existe un malentendido común consistente en que un desarrollador puede simplemente "desarrollar" cualquier aplicación, mientras que la realidad es que las personas son competentes en lenguajes y plataformas de programación específicos.

El desafío consiste en que hay muchas posibilidades de que los equipos de TI no solo se centren en una aplicación, sino en muchas: todas con requisitos diferentes y diferentes áreas interesadas. Por lo tanto, en última instancia, las aplicaciones deben priorizarse siempre con el objetivo de satisfacer las necesidades de la empresa, a ser posible dentro de los conjuntos de habilidades y parámetros de los entornos de desarrollo disponibles.

3 ¿En qué plataforma habría que hacer ejecutar las aplicaciones?

Con organizaciones que mantienen múltiples entornos para satisfacer las demandas de sus aplicaciones, cada una con requisitos tecnológicos únicos, encontrar la plataforma no es el único desafío. Lo realmente difícil es que el desarrollo y la administración son más complejos que nunca, con TI y desarrolladores que navegan por aplicaciones tradicionales, servicios nativos de la nube, Software como Servicio (SaaS) y servicios locales, por poner solo algunos ejemplos.

Aquí es donde se necesita un terreno de juego común entre los equipos de TI, las líneas de negocios y los desarrolladores, donde tener una sola plataforma digital es fundamental para eliminar el potencial surgimiento de silos, permitir una mejor implementación de recursos y proporcionar un enfoque coherente para administrar aplicaciones, infraestructura y necesidades comerciales conjuntas.

Se trata de crear una plataforma común para "ejecutar todas las cosas" (run-all-the-things). Una base digital definida por software que proporciona la plataforma y la elección de dónde ejecutar TI, para impulsar el valor comercial, crear el mejor entorno para desarrolladores y ayudar a TI a administrar de manera efectiva la tecnología existente y nueva a través de cualquier nube para cualquier aplicación en cualquier dispositivo con, además, seguridad intrínseca.

Solo a través de la integración intrínseca de la seguridad, TI puede garantizar las condiciones adecuadas de seguridad para cualquier aplicación, nube y dispositivo.

Una plataforma capaz de proporcionar todas las aplicaciones, lo cual permite a los desarrolladores utilizar las últimas metodologías de desarrollo y tecnologías de contenedores con el fin de reducir el tiempo de producción. Todo con una gestión y operaciones consistentes.

En última instancia se trata de permitir que las empresas pongan a disposición del cliente un mejor software de la forma más rápida; automatizar el ciclo de vida de las aplicaciones modernas, eliminar las barreras de entrada sobre las diferentes modalidades y distribuciones de Kubernetes y facilitar la adopción de aplicaciones basadas en contenedores e incluso ejecutar Kubernetes de la misma forma en diferentes nubes. Al hacerlo, la empresa puede posicionarse para contar con una nueva ola de aplicaciones modernas; democratizar Kubernetes permite ofrecer las aplicaciones que pueden transformar e incluso incrementar la competitividad de la empresa.

4 Entonces, ¿dónde ejecutar las aplicaciones?

La cuestión de los datos. Las empresas tienen múltiples entornos por varias razones: una de ellas puede ser la necesidad de cumplir con las demandas regulatorias, de cumplimiento normativo o de los requisitos de los clientes para el almacenamiento geográfico de datos.

También puede haber una razón tecnológica para mantener los datos y las aplicaciones lo más cerca posible del usuario final, si la latencia máxima no es negociable, por ejemplo. Entra en juego, además, la ubicación y propiedad de los datos -cuya regulación varía de un país a otro- y que debe tenerse en cuenta al tomar decisiones sobre la posible implementación distribuida de la aplicación.

La cuestión del "dónde" a menudo se desglosa en elementos comerciales y técnicos. La respuesta está en reunir estas consideraciones para avanzar con ambos grupos de elementos satisfechos de manera exhaustiva.

5 ¿Cómo entregarlas a los usuarios?

Una vez que las bases estén puestas en su lugar, es hora de considerar cómo llega-

rán realmente las aplicaciones al usuario. Esto a menudo se pasa por alto y, sin embargo, el objetivo de implementar aplicaciones modernizadas es que los usuarios interactúen con ellas y reciban la experiencia que esperan. No importa si son clientes, empleados o cualquier otra parte interesada: la medida del valor entregado de cada aplicación no se puede medir, ni siquiera considerar, hasta que está en manos del usuario.

Eso también se aplicaría a las actualizaciones: un empleado podría tener algunas de las aplicaciones más potentes del mundo en la palma de su mano, pero al tener que actualizar manualmente cada una, su verdadero valor no se lograría hasta que eso ocurriera.

Es por eso por lo que el trabajo reciente en La Poste, el servicio postal francés, es tan convincente. Ya había digitalizado a su personal de primera línea dándoles a los trabajadores postales teléfonos inteligentes, programados con aplicaciones que les permitían ofrecer servicios adicionales mientras realizaban sus rondas diarias. Tanto el desafío como la oportunidad consistían en administrar las actualizaciones en toda su fuerza de trabajo remota.

Cuando la empresa implementó una plataforma para administrar las aplicaciones de forma remota, consiguió que los trabajadores individuales estuvieran mejor equipados para atender a los clientes y aumentar los ingresos de la empresa. El "valor" de las aplicaciones se había conseguido.

6 ¿Cómo asegurarlas?

Aplicaciones, datos, infraestructura: todo tiene que ser completamente seguro: las amenazas acechan en cada etapa. La naturaleza sofisticada de los ciberataques de hoy exige respuestas sofisticadas, por lo que es muy importante construir seguridad de extremo a extremo que cubra aplicaciones, cargas de trabajo, puntos finales de gestión e infraestructura.

No puede ser materia de última hora, incluida justo antes de la entrega del servicio. Solo a través de la integración intrínseca de la seguridad, TI puede garantizar las condiciones adecuadas de seguridad para cualquier aplicación, nube y dispositivo.

7 ¿Cómo gestionar todo?

Finalmente llega la gerencia. Como ya hemos mencionado en el paso tres, los equipos de TI deben poder controlar todos estos diferentes elementos, en un momento en que el talento y los recursos se ven puestos a prueba, algo que debe abordarse en un 93% (según nuestra investigación), ya que los encuestados respondieron mayoritariamente que involucrar a personas con conjuntos de habilidades técnicas variadas es una parte esencial del éxito de los esfuerzos de transformación digital.

Debe ser una infraestructura simplificada, con operaciones consistentes y un modelo para la construcción y operación de aplicaciones modernas en múltiples entornos, ya sea en las instalaciones o en la nube.

De todo ello se desprende que las empresas deben estar a los mandos para poder construir, ejecutar, administrar, asegurar y proporcionar cualquier aplicación rápidamente, si quieren satisfacer las necesidades de sus clientes tanto en los tiempos turbulentos de hoy como también, y de modo imprescindible, como una forma de preparar su negocio en el futuro. Esto ejerce una gran presión sobre los equipos de TI extendidos, pero es un trabajo que debe realizarse. Las organizaciones que implementan una única base digital, que crean una infraestructura que permite el rápido desarrollo y la implementación de aplicaciones modernas serán capaces de darse cuenta del inmenso valor de estos nuevos servicios y ofertas, posicionándose adecuadamente para alcanzar el éxito en el futuro. ■

Si te ha gustado este artículo, compártelo

Diálogos it TRENDS

Liberty Seguros se muda al cloud para ganar agilidad

Liberty Seguros ha trasladado todo su negocio retail a la nube pública para eliminar la complejidad y dependencia de las tecnologías e infraestructuras tradicionales. Alexandre Ramos, CIO de Liberty Seguros para Europa, detalla en esta entrevista el proceso de transformación y elección, así como los principales beneficios obtenidos por la firma.

NUEVO INFORME

DOCUMENTO EJECUTIVO

Teletrabajo en 2020:
el futuro se hace presente

ELABORADO POR itRESEARCH

Descarga este **documento ejecutivo** de itRESEARCH

Phishing, la amenaza eterna

Que el correo electrónico se haya convertido en el principal vector de ataque para los ciberdelincuentes no es casual teniendo en cuenta que se ha convertido en una herramienta de trabajo esencial en los entornos empresariales. Según datos de mercado, en 2019 se procesaron una media de 294 billones de email diarios. Estos volúmenes son los que hacen del phishing una herramienta de incalculable valor para los ciberdelincuentes, ya que multiplica exponencialmente su público objetivo y por tanto la probabilidad de éxito en los ataques.

Los orígenes del phishing parecen estar asociados a la compañía norteamericana AOL. Durante los años 90 AOL fue uno de los principales proveedores de servicios de Internet, con más de un millón de clientes suscritos a su servicio. Dicen que no todos estaban dispuestos a pagar para acceder a Interne después del periodo de prueba de 30 días, y fueron muchos los que encontraron la manera de hacerse pasar por administradores de AOL para obtener credenciales de inicio de sesión con la intención de continuar accediendo a Internet de forma gratuita.

Las personas que comerciaban con software y herramientas pirateados e ilegales, formaron un grupo, “warez community”, que se dedicaba a robar datos de usuario, incluido el nombre de usuario, la contraseña y otra información personal. Con esta información robada y junto con un algoritmo que desarrollaron, comenzaron a generar números de

"El engaño forma parte de la historia desde el principio, pero sobre todo de la naturaleza humana. Por eso el phishing es tan efectivo, y es difícil de protegerse frente a él, porque se basa en la confianza"

Sergio Martínez,
Director General, SonicWall Iberia

Spam vs Phishing

El spam es un correo electrónico no deseado que se envía de forma masiva a una lista de destinatarios. Normalmente se envían únicamente con el propósito de vender un servicio o producto. Los spammers suelen enviar estos correos electrónicos a una larga lista de destinatarios, con la esperanza de que al menos algunos de ellos respondan. La intención detrás del envío de estos correos electrónicos no deseados es simplemente atraer a los destinatarios para que compren productos dudosos o participen en esquemas fraudulentos y cuasi legales.

Podríamos decir que el phishing es el spam malicioso. Un correo electrónico de phishing es un tipo de correo electrónico no deseado que se envía específicamente para engañar a la víctima para que comparta sus datos personales, como los detalles de la tarjeta de crédito/débito, los detalles de la cuenta bancaria, las contraseñas, etc., lo que puede dar lugar a casos de fraude financiero por robo de identidad. A veces, estos correos electrónicos están dirigidos específicamente a extraer información personal sobre una determinada empresa o usuario.

tarjetas de crédito aleatorios que se usaron para abrir nuevas cuentas de AOL y otras cosas, como enviar spam a otros miembros de AOL. Estos mensajes fueron elaborados meticulosamente y tenían los mismos colores, fuentes y texto que utilizaba AOL por lo que los usuarios cayeron en la trampa.

Según recoge Phisprotection.com a medida que el uso y popularidad de Internet aumentaban, los estafadores adaptaron sus tácticas para hacerse pasar por de administradores de un ISP, enviando correos electrónicos a las cuentas de los clientes del con el fin de obtener las credenciales de inicio de sesión del usuario. Habiendo engañado a alguien, el hacker podía acceder a Internet desde la cuenta de ese usuario con la ventaja de enviar spam desde la dirección de correo electrónico del usuario.

El virus I Love You demostró el potencial que tenía el correo electrónico como herramienta inalienable phishing. El 4 de mayo de 2000 los buzones de correo de todo el mundo, empezando por los de Filipinas recibieron un mensaje que desencadenaría el caos. Todos los que no pudieron resistirse a abrir una supuesta carta de amor se vieron infectados por un virus que se instaló en la máquina y se reenvió a todos los contactos de la libreta de direcciones del Outlook. Se calcula que más de 45 millones de usuarios se vieron afectados.

"Es preciso complementar la protección perimetral tradicional con nuevas barreras que incorporen sistemas de detección basados en inteligencia artificial y detección de patrones de comportamiento de los usuarios"

Miguel López, Senior Regional Sales Manager - Iberia, Barracuda Networks

El que se considera como el primer ataque de phishing a sitios de comercio electrónico se produjo en junio de 2001 y fue contra el site E-Gold; en 2003 a los ciberdelincuentes les dio por registrar dominios nuevos que se parecían a los nombres de sitios populares como eBay y PayPal para después enviar correos electrónicos falsos a clientes de estas empresas. Los clientes que fueron víctimas de estos correos electrónicos de phishing fueron engañados para que proporcionaran los detalles de su tarjeta de crédito y otra información personal.

En 2004 los ciberdelincuentes explotaron la rentabilidad del phishing y comenzaron a atacar bancos, empresas y a los clientes de ambos. En los años siguientes y hasta la actualidad, las tácticas no han cambiado mucho, no así los mensajes, mucho más cuidados, y las recompensas; ya no se trata de conseguir acceso gratuito a internet, o demostrar lo mucho que se puede hacer. Hoy en día las estafas de phishing pueden causar mucho daño y, en definitiva, ¿por qué empeñarse en atacar un firewall si un correo bien diseñado te abre las puertas de una empresa?

La idea básica detrás del phishing es simple. La víctima recibe un correo electrónico que indica que una cuenta se ha suspendido, que tiene que revisar un documento, que se le envía la factura que estaba esperando… y se le pide que inicie sesión para reactiva su cuenta o se descargue el documento en cuestión.

Se tiende a pensar que es fácil detectar este tipo de mensajes, pero es en lo que más han evolucionado los ciberdelincuentes, en dar autenticidad a esos correos. Al contrario de lo que parece, los

INFORME SOBRE PHISHING 2020

La Encuesta sobre ataques de phishing de 2020 revela las últimas tendencias, desafíos y mejores prácticas para la seguridad del correo electrónico, lo que proporciona a las organizaciones la información necesaria para protegerse mejor contra las amenazas avanzadas actuales. En los datos recogidos destaca que más de un tercio de los encuestados (36%) no estaban seguros de que los empleados de sus organizaciones pudieran detectar y evitar un ataque de phishing por correo electrónico en tiempo real. Además, un 38% dijo que durante el año pasado, alguien dentro de su organización ha sido víctima de un ataque de phishing.

"Las empresas deben asumir que siempre habrá alguien que hará clic en un enlace o adjunto malicioso, de ahí que necesiten protegerse y concienciar en ciberseguridad a los usuarios"

Fernando Anaya, Country Manager, Proofpoint

"Es necesario aumentar la concienciación de los usuarios para que desconfíen incluso de los correos y mensajes más elaborados si no han sido solicitados"

Josep Albors, responsable de concienciación e investigación, ESET España

ataques de phishing se planifican inteligentemente y se ejecutan meticulosamente.

Las redes sociales se han convertido en filones de información que los ciberdelincuentes saben explotar cuidadosamente para personalizar sus correos. El phishing masivo ha dado paso al spear phishing, o phishing dirigido. El diablo está en los detalles, los mismos que proporcionamos en las redes, los mismos que se recogen e incorporan para que el mensaje sea más creíble, para que ese archivo que parece proceder de una fuente confiable desate el terror, para que ese enlace que promete acceder al documento que estabas esperando lleve a la ruina a una empresa.

Las brechas de Target o Home Depot son sólo algunas de las que se sabe que empezaron con un spear phishing.

Fraude del CEO

Además del phishing más básico y el phishing dirigido, hay otros tipos. En el más común los estafadores se hacen pasar por una empresa legítima en un intento de robar los datos personales de las personas o las credenciales de inicio de sesión con correos masivos que utilizan con frecuencia amenazas y un sentido de urgencia para asustar a los usuarios para que hagan lo que quieren los atacantes. Ya hemos comentado que el spear phishing es más dirigido gracias a que se tienen detalles personales de las víctimas.

El fraude del CEO da un paso más en esa personalización. También conocidos como ataques BEC (Business Email Compromise), consisten en comprometer la cuenta de correo de un alto cargo para

autorizar operaciones, como transferencias bancarias fraudulentas a una institución financiera de su elección.

Un reciente informe de Agari recoge un crecimiento del 48% de los ataques BEC en el segundo trimestre de este año respecto al primero. Además, según el último Informe de tendencias de actividad de phishing del Anti-Phishing Working Group, en el segundo trimestre de 2020 la pérdida promedio por un ataque BEC que involucró una transferencia bancaria fraudulenta fue de 80.143 dólares frente los 54.000 dólares del primer trimestre. Dice también el informe que las estafas de transferencias bancarias fraudulentas representan el 18% de todos los ataques BEC y que las estafas con tarjetas de regalo son el tipo más común de estafa BEC, representando el 66% de los ataques BEC.

Por otra parte, según el Informe sobre delitos en Internet de 2019 del FBI, los ataques BEC fueron el quinto tipo más común de ciberataque, y las estafas

¿QUÉ ES EL PHISHING? **CLICAR PARA VER EL VÍDEO**

representaron más de la mitad de todas las pérdidas por delitos cibernéticos. En 2019, las pérdidas por ataques BEC alcanzaron los 1.800 millones de dólares, pero dado que muchas empresas no informan de este tipo de perdidas, es probable que el total real sea mucho mayor.

Vishing

Aunque lo más habitual es que el phishing esté asociado a un correo electrónico, los ciberdelincuentes no dejan de inventar y han optado por dejar mensajes de voz y crear el vishing, o Voice Phishing. Relativamente escasos, este tipo de ataque se está expandiendo durante este año. Al menos es lo que recoge un informe de Mimecast, que predice que los ataques de vishing podrían convertirse en actividades diarias en 2020.

Además, un aviso lanzado por el FBI advertía hace unos meses que desde julio de 2020 las estafas vishing se han convertido en campañas

coordinadas y sofisticadas destinadas a obtener información confidencial, de propiedad y secretos comerciales de las empresas. Explica que las estafas vishing siguen un curso de acción común: para empezar, el grupo de ciberdelincuencia identifica un objetivo de la empresa e investiga su fuerza laboral, recopilando información sobre las víctimas de los empleados desde diferentes fuentes, entre ellas las redes sociales. A partir de los distintos perfiles de redes sociales de un individuo, los atacantes pueden conocer el nombre del empleado, la ubicación, el lugar de trabajo, el puesto, la duración en la empresa y, a veces, incluso el domicilio del empleado.

A continuación, el grupo de ciberdelincuencia o los piratas informáticos registran un dominio y crean páginas web de phishing que duplican la página de inicio de sesión VPN interna de una empresa. Estas páginas web de phishing también tienen la capacidad de capturar autenticación de dos factores o contraseñas de un solo uso, reflejando los propios protocolos de seguridad de la empresa.

Después los atacantes contactan con los empleados y se ganan su confianza gracias a la información recopilada para convencerle de necesita iniciar sesión en algún servicio a través de una página web falsa. El empleado teclea su nombre de usuario y contraseña en el dominio, hace clic en el enlace de inicio de sesión, completa la autenticación de doble factor si se requiere y deja el acceso abierto a los ciberdelincuentes. El resultado es que la información confidencial, de propiedad y secreto comercial de la empresa está en juego.

"El phishing es uno de los tipos de ataques de ingeniería social más antiguos, pero también uno de los más flexibles, capaz de adaptarse y disfrazarse de formas muy diferentes"

Alfonso Ramírez, Director General, Kaspersky Iberia

"El correo electrónico es uno de los sistemas de comunicación más inseguros y expuestos de los que se utilizan hoy en día"

Iván Mateos, Sales Engineer, Sophos Iberia

Para protegerse contra los ataques de vishing, los usuarios deben evitar responder llamadas de números de teléfono desconocidos y nunca dar información personal por teléfono.

Smishing

Otro tipo de phishing sin correo electrónico, cada vez más común y peligroso es el phishing de SMS para dispositivos móviles. Estos ataques, a menudo llamados SMiShing, se inician en forma de un mensaje de texto disfrazado de una comunicación de una marca confiable como un banco o un servicio de pago, o incluso una persona de confianza, y con frecuencia utiliza un enlace disfrazado. Las personas tienden a responder a los mensajes de texto mucho más rápido que al correo electrónico, y sus pantallas pueden ocultar pistas importantes sobre las páginas web que visitan, lo que convierte a SMiShing en un vector de ataque muy efectivo y, por lo tanto, peligroso.

Si proteger contra el phishing es complicado, cuando la amenaza está directamente relacionada con el móvil, la protección es aún más difícil. Los empleados confían cada vez más en los dispositivos móviles como parte de sus tareas comerciales y personales diarias. Y con la popularidad de BYOD móvil, las políticas de seguridad poco claras y las protecciones relativamente deficientes en dispositivos móviles, los usuarios de estos dispositivos tienen un mayor riesgo de sufrir amenazas de phishing móvil.

Bancos y agencias antifraude de todo el mundo advierten que los mensajes de texto fraudulentos son cada vez más numerosos y sofisticados, aunque es difícil obtener estadísticas que confirmen estas afirmaciones.

Pharming

El pharming es como el phishing en el sentido en que ambas técnicas intentan atraer a la víctima a un sitio web falso para obtener sus datos confidenciales. Sin embargo, existen algunas diferencias clave y un componente de peligrosidad importante en el primero.

En el phishing, las víctimas suelen ser engañadas para que hagan clic en enlaces sospechosos en sus correos electrónicos o se escondan detrás de anuncios en línea. Son llevados a sitios falsos, que pueden infectar sus dispositivos con virus o robar sus datos de otras formas. En el pharming, la víctima también es dirigida a un sitio web falso, pero no necesita hacer clic en ningún enlace. El tráfico se redirige sin la interferencia de la víctima. De hecho, es posible que no haya señales de advertencia de que está en un sitio web falso.

Este método de phishing aprovecha el envenenamiento de la caché contra el sistema de nombres

de dominio (DNS). Explican los expertos que para que este ataque tenga éxito, primero se necesita instalar un virus o un troyano en el dispositivo para redirigir el tráfico web. Una vez iniciado el ataque el, cuando la víctima quiera acceder a su cuenta de redes sociales, por ejemplo, e ingrese la URL correcta, aparecerá un sitio idéntico pero falso. Lo peor es que no tendrá idea de que es fraudulento.

¿Por qué sigue siendo tan efectivo?

El phishing, cuyas primeras muestras aparecieron hace más de 30 años, es una amenaza muy actual. Sigue teniendo éxito porque se basa en el engaño y el engaño, en opinión de Sergio Martínez, "forma parte de la historia desde el principio, pero sobre todo de la naturaleza humana. Por eso es tan efectivo, y es difícil de protegerse frente a él, porque se basa en la confianza".

Según Ivan Mateos, Sales Engine de Sophos Iberia, el 93% de los ciberataques comienza por el correo electrónico. ¿Por qué? "Porque es la forma más sencilla de llegar a muchas personas sin que éstas ni siquiera hayan movido un dedo", y añade que "a estas comunicaciones a veces les prestamos más atención y otras veces simplemente las leemos en diagonal sin pararnos a pensar mucho en ellas, no verificamos si el remitente es quien dice ser, no pensamos en si el contenido del mensaje será seguro o incluso en si tiene sentido que estemos recibiendo ese mensaje".

El phishing sigue siendo efectivo no sólo porque se realiza a gran escala, sino porque siendo uno de

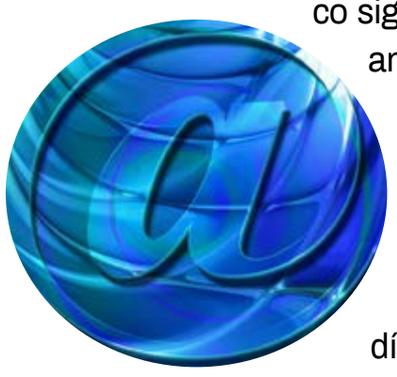
"Disponer de una protección antivirus ya no es suficiente. La mejor opción es optar por soluciones de seguridad avanzada"

Alberto Tejero, director general de Panda Security Iberia, a WatchGuard Brand

ataques de ingeniería social más antiguos, es también uno de los más flexibles, “capaz de adaptarse y disfrazarse de formas muy diferentes para atraer a los usuarios incautos a un sitio y engañarlos para que introduzcan su información personal”, dice Alfonso Ramírez, director general de Kaspersky Iberia.

Para Miguel López, Senior Regional Sales Manager de Barracuda Iberia, el Phishing sigue siendo una de las mayores amenazas a la seguridad corporativa porque lo largo del tiempo ha ido evolucionando y adaptándose desde el típico ataque automatizado y masivo hasta convertirse en un medio de inserción dentro del entorno corporativo mucho más personalizado.

Explica Fernando Anaya, Country Manager de Proofpoint, que hemos asistido a un cambio de paradigma en el que se ha pasado de proteger la infraestructura a poner el foco en las personas, ya que estas conforman la última línea de defensa de las organizaciones y son quienes están en el punto de mira. Asegura el directivo que más del 99% de los ciberataques dependen de la interacción humana para activarse y que “el correo electrónico sigue siendo el vector de amenaza más utilizado por una razón muy simple: funciona”.



La ingente cantidad de correos electrónicos que se procesan cada día, sumado al teletrabajo

"Debemos mejorar la formación y concienciación del usuario, pues éste es una parte fundamental de la seguridad de una compañía"

José de la Cruz, director técnico, Trend Micro Iberia

que aprovechan la nueva distancia entre compañeros del entorno laborar para fingir, cada vez más, falsas identidades y para aumentar la presión, no hace sino darle más alas al Phishing. Desde Retarus recuerdan además de los empleados que teletrabajan son cada vez más activos en las redes sociales, y que por consiguiente la ingeniería social es más fácil porque hay más información.

Apunta Josep Albors, director de investigación y concienciación de ESET España, que a pesar de que las técnicas de phishing han evolucionado a lo largo de todo este tiempo, “el principal motivo por el que siguen siendo efectivas es la suplantación de empresas y organismos oficiales conocidos unido a una mejora considerable en las webs utilizadas para llevar a cabo esta suplantación”. Añade además que la redacción de los mensajes también ha experimentado una mejora en algunos casos y ya es algo habitual ver cómo las webs fraudulentas utilizan certificados válidos para obtener el famoso candado verde que tanta confianza inspira a los usuarios.

“El cibercriminal ni siquiera necesita entrar en el sistema del usuario”, dice Alberto Tejero, director general de Iberia de Panda Security, a WatchGuard Brand. Para el directivo el phishing sigue siendo tan efectivo para los cibercriminales porque para estos ataques se usan herramientas accesibles, no requieren de mucho esfuerzo, y la mayoría de las acciones se hacen de forma automatizada.

El desconocimiento y falta de concienciación por parte del usuario son, en opinión de José de la

Cruz, Director Técnico de Trend Micro, algunas de las razones de persistencia y éxito continuado en el tiempo del phishing.

Asegurando que el phishing se ha convertido en una pandemia, que al igual que la sanitaria, es sumamente dañina para los usuarios y organizaciones por su capacidad de propagación, dice José Luis Laguna, Director Systems Engineering Fortinet España y Portugal, que la situación actual ha creado un caldo de cultivo para su expansión: los teletrabajadores conectándose desde redes domésticas a la red corporativa son un objetivo fácil.

Medidas antiphising

Como hemos ido viendo, los ataques de phishing han ido en aumento en los últimos años. La situación actual de pandemia, que provocando que muchas organizaciones adopten el teletrabajo de manera acelerada, ha provocado un enorme incremento en los ataques de phishing.

De hecho, según datos de Barracuda, los ataques de phishing por correo electrónico han aumentado un increíble 667% durante los últimos meses, cuando se ha visto a los atacantes haciéndose pasar por la Organización Mundial de la Salud o empresas de desinfección contra el virus.

Detener los ataques de phishing varía dependiendo del nivel de seguridad de cada empresas, o de lo que sofisticado que sea el ataque. Para Miguel López “es preciso complementar la protección perimetral tradicional con nuevas barreras que incorporen sistemas de detección basados en inteligencia

"Ya se trate de estafas de phishing, malware dirigido o una combinación de ambos, hay un rasgo común en todos estos ataques: la gran mayoría se enviará directamente a la bandeja de entrada"

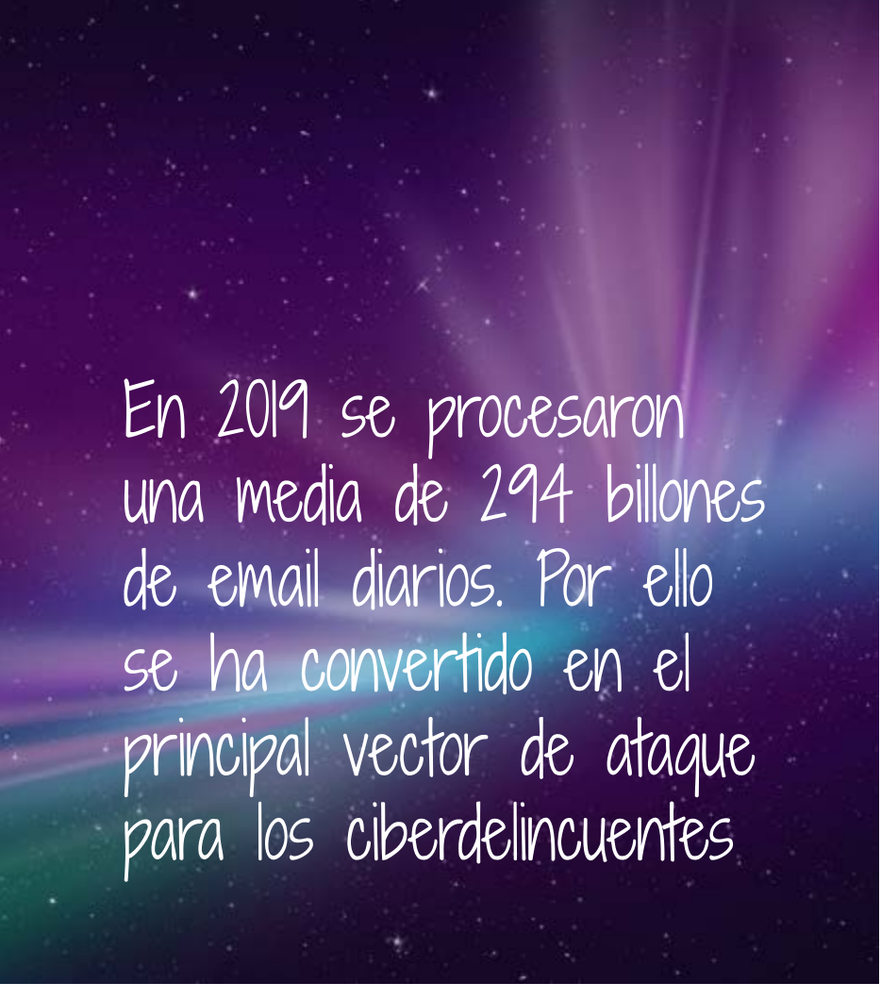
José Luis Laguna, Director Systems Engineering, Fortinet España y Portugal

artificial y detección de patrones de comportamiento de los usuarios". Añade el directivo de Barracuda que se debe prestar especial atención a los ataques internos ya que muchas veces el Phishing Dirigido puede combinarse con ataques de Account Take Over, o compromiso de cuentas, donde el ataque se lanza desde la cuenta de un compañero cuyas credenciales han sido comprometidas; "adicionalmente, el phishing suele aprovecharse también de la falta de formación en materia de autoprotección digital de los usuarios, lo que también hace muy recomendable establecer sistemas de formación y simulación de ataques que permita que sean los propios usuarios los que se auto-protejan y eviten comportamientos peligrosos".

Si, según Sergio Martínez, el phishing se basa en el engaño y en la confianza, "el principio básico para protegerse ante el engaño, es la desconfianza absoluta, el "Zero-trust". Hay que preguntarse si tú eres quién dice ser, si los datos que se reciben son fiables… "Todas las compañías, incluida Sonicwall, estamos presentando soluciones Zero-trust para ayudar a las empresas y organizaciones a gestionar este entorno endiablado COVID en el que nos hemos zambullido tan rápido, y esta es la única forma de protegerse si queremos minimizar el impacto del factor humano".

Fernando Anaya considera "vital" que las empresas inviertan en soluciones avanzadas para el correo electrónico a fin de detectar y bloquear amenazas entrantes, identificando también a los empleados con mayor riesgo o más atacados (VAP). Añade el directivo de Proofpoint que si esto se combina con una formación de los usuarios acerca de las amenazas más comunes, incluidas simulaciones de ataques para defenderse de forma eficaz y sostenible contra el phishing, "las organizaciones desplegarán el nivel adecuado de protección y mitigación donde más se necesite".

Josep Albors también coincide en que es necesario aumentar la concienciación de los usuarios "para que desconfíen incluso de los correos y mensajes más elaborados si no han sido solicitados" y añade que, en la parte técnica las soluciones de seguridad deben seguir innovando su capacidad de detección de correos electrónicos sospechosos, así como mejorarse "la detección de webs sospechosas de pertenecer a una campaña de phishing revisando, por ejemplo, la información relacionada con la fecha en la que se dieron de alta o la organización a la que se ha otorgado el certificado si esté está presente".



Para evitar ser víctimas de phishing es importante la concienciación de los empleados, y tener en cuenta una serie de medidas “sencillas pero eficaces”, asegura Alfonso Ramírez. Entre las que menciona el directivo de Kaspersky destacan: Comprobar siempre las direcciones online de los mensajes desconocidos o inesperados; si no se está seguro de que el sitio web sea genuino y seguro, no introducir nunca las credenciales; utilizar una solución de seguridad que incorpore tecnologías antiphishing basadas en el comportamiento.

Compartir en RRSS

Iván Mateos propone dos líneas diferentes y a su vez complementarias a la hora de hacer frente al phishing. Por un lado proteger a la empresa, es decir, proteger tanto la salida como la entrada del correo aplicando toda la tecnología existente antispam y antimalware para verificar la seguridad y legitimidad de cada uno de los emails, e incluso el contenido de estos. Y por otro lado proteger al empleado mediante formación y concienciación continua.

En opinión de Alberto Tejero, disponer de una protección antivirus ya no es suficiente. “Los intentos de suplantación de identidad son cada vez más sofisticados y son capaces de sortear las barreras de las soluciones de seguridad tradicional. Ante esta situación, la mejor opción es optar por soluciones de seguridad avanzada”, dice el directivo de Panda Security, a WatchGuard Brand, añadiendo que en los ataques de phishing también es importante bloquear las conexiones DNS malintencionadas, pues los atacantes se apoyan en los DNS para ejecutar ataques en víctimas desprevenidas y que “cualquier organización debe contar planes de educación y formación automatizada para poder combatir de forma más efectiva el phishing”.

Asegurando que el empleado tiene en su mano el convertirse en un eslabón más de la cadena de seguridad de la compañía o un habilitador de posibles infecciones, dice el director técnico de Trend Micro que la diferencia entre uno u otro está en la formación y concienciación; “n usuario consciente de los riesgos a los que se expone personalmente y a la compañía para la que trabaja va realizar un uso responsable de las herramientas de trabajo que tiene a su disposición”.

Entre las medidas básicas apuntadas por José Luis Laguna para tratar de evitar los ataques de phishing, menciona el directivo de Fortinet que lo primero es “hacer sentir a los empleados que forman parte del equipo de ciberseguridad de la compañía” haciéndoles entender las repercusiones que puede tener una brecha de seguridad en el negocio. El segundo paso, añade, es proporcionar a los empleados las herramientas necesarias para su protección. Así, por ejemplo, dotar a los usuarios de mecanismos de autenticación multifactorial, de modo que si sus credenciales se ven comprometidas, no podrán hacer uso de las mismas sin el segundo factor de autenticación.

Enlaces de interés...

- Alerta: nueva estafa de phishing que suplanta a la Agencia Tributaria
- ¿Por qué el phishing continúa siendo un problema y no deja de crecer?
- El sector financiero es el más atacado por correos electrónicos de phishing
- España es el país más afectado por phishing, con el 8,38% del total de los ataques

it User
TECH & BUSINESS

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

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la 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.

El Poder Legislativo en la Nueva Sociedad Digital:

¿Evoluciona o no?

Me repito, ya no se discute si estamos llegando a la Era Digital de la Humanidad, ESTAMOS YA en esta nueva Era, y tal vez la pandemia del Covid 19 lo está dejando todavía más claro por el incremento de relaciones digitales personales, educativas, sanitarias, comerciales, con las administraciones del Estado...

Compartir en RRSS

Simplificando la teoría de los 3 poderes del Estado democrático, se asigna a cada uno de ellos una labor fundamental que establece un equilibrio. Nadie discute este principio del siglo XVIII, que nos ha dado ya dos siglos y medio de un gran avance de la humanidad.

Al Poder Legislativo se le asigna en exclusiva la importantísima tarea de elaborar las leyes de acuerdo a las necesidades de los ciudadanos y colaborar en el equilibrio de poderes mediante la permanente actualización de las leyes vigentes, elaboración de leyes nuevas que se adapten a la evolución de la sociedad y eliminación de leyes obsoletas que ya no aportan nada las nuevas realidades de la sociedad.

Mediante este sencillo modelo, el Poder Legislativo limita al Poder Ejecutivo a mantenerse dentro de las leyes vigentes y al Poder Judicial a mantener la administración de justicia dentro de las mismas leyes vigentes. Magnífico y simple modelo que sirvió durante muchas décadas, siglos incluso, a una gran evolución de la sociedad a través de tres Revoluciones Industriales que finalmente nos han traído a la Cuarta Revolución, digital esta vez, que en solo los 20 primeros años del siglo XXI ha llegado con tal cantidad y velocidad de cambios, que la Nueva Sociedad Digital se encuentra ahora con una situación donde tenemos un enorme déficit de leyes nuevas que regulen realidades actuales que ni se soñaban hace solo 20 años, multitud de leyes obsoletas que solo interfieren con los procesos actuales y leyes útiles para la realidad

La proactividad para abordar nuevos temas Digitales o incluir modificaciones provocadas por cambios digitales en la sociedad por parte del Poder legislativo es insignificante

Al Poder Legislativo se le asigna en exclusiva la importantísima tarea de elaborar las leyes de acuerdo a las necesidades de los ciudadanos

actual que necesitan reformas urgentes para adecuarse a la nueva Realidad Digital.

Por otra parte, el Poder Legislativo en estos dos siglos y medio de democracias modernas ha ido perdiendo el foco de su objetivo principal, mantener las leyes vigentes para que el Estado de Derecho funcione de la mejor manera y al ritmo de evolución de la Sociedad. Se ha ido convirtiendo cada vez más en una auditoria política del Poder Ejecutivo y finalmente en un centro de confrontación de ideologías políticas que cada vez tienen menos que ver con la realidad de los Ciudadanos Digitales, a los que confina a una pregunta cada 4 años.

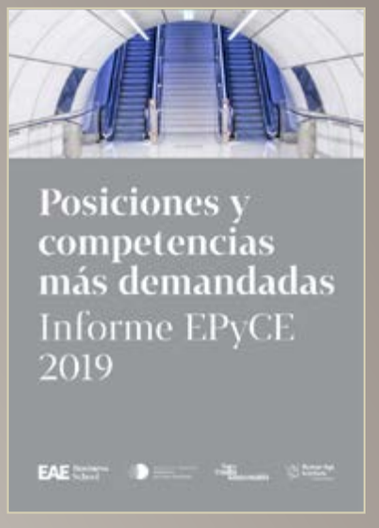
Ciertamente, la Evolución Digital del Poder Legislativo es casi inexistente, y lo peor de esta situación es que la Nueva Sociedad Digital sigue su acelerado avance con un déficit cada vez mayor de legislación apropiada a las nuevas situaciones que trae todos los días esta Revolución Digital.

Dos aspectos en los que el poder Legislativo debería evolucionar digitalmente, la proactividad al abordar los nuevos temas sobre los que legislar y la participación de los Ciudadanos Digitales en el proceso de elaboración y aprobación de dichas nuevas leyes, son ya muy urgentes y no ayudan, incluso llegan a entorpecer, el avance imparable hacia una sociedad cada más digitalizada, moderna y participativa. No quiero pensar que esto se deba a que este avance tecnológico de la humanidad se ha producido fuera de las guías ideológicas de los grupos políticos que absortos en discusiones improductivas no son capaces de ver como la tecnología y la digitalización de la sociedad los adelantan a toda velocidad poniéndoles en evidencia ante los nuevos Ciudadanos Digitales.

it whitepapers

POSICIONES Y COMPETENCIAS MÁS DEMANDADAS: INFORME EPYCE

¿Quieres conocer cuáles son los perfiles más demandados por las empresas españolas? ¿Qué papel tiene la tecnología en la generación de nuevos puestos que generan empleo? La Asociación Española de Directores de Recursos Humanos (AEDRH) junto con EAE Business School, Foro Inserta de la Fundación Once y Human Age Institute de ManpowerGroup han presentado la sexta edición de un informe que ofrece una clara visión de las profesiones más demandadas en la empresa española.



Dos aspectos en los que el poder Legislativo debería evolucionar digitalmente serían la proactividad al abordar los nuevos temas sobre los que legislar y la participación de los Ciudadanos Digitales en el proceso de elaboración y aprobación de dichas nuevas leyes

La proactividad para abordar nuevos temas Digitales o incluir modificaciones provocadas por cambios digitales en la sociedad por parte del Poder legislativo es insignificante, ignorando los cambios que se han producido en los últimos 20 años; ya ni siquiera en los programas políticos que cada 4 años se presentan a los Ciudadanos se habla de los cambios que se producen diariamente en la Nueva Sociedad Digital, no digamos ya establecer mecanismos donde los Ciudadanos Digitales puedan manifestar su opinión y necesidades.

Y qué decir de mecanismos que permitan la participación de los Ciudadanos Digitales en los procesos de elaboración de nuevas leyes digitales; los métodos actuales obsoletos hacen que una minoría electa decida según sus intereses políticos cuando existen ya herramientas digitales que permitirían tener opiniones continuas de la Ciudadanía Digital que con el ritmo de cambio tecnológico pueden variar no ya en años sino en meses o incluso en semanas.

Y qué decir del aspecto de control parlamentario que cada vez usa más tiempo del Poder Legislativo provocando discusiones en muchos casos

estériles e inútiles que limitan la participación de los Ciudadanos Digitales a ver, oír, aplaudir o abuchear y callar. Creo que ya hay herramientas digitales que permitirían participar a los Ciudadanos Digitales para que los temas de discusión sean más productivos y no meros combates ideológicos.

Este inmovilismo tecnológico del Poder Legislativo tiene un efecto de entorpecer el mejor funcionamiento de los otros dos poderes del estado.

Por una parte, obliga al Poder Judicial a enfrentarse a situaciones donde no existen leyes que regulen nuevas situaciones y, por tanto, los jueces deban tomar decisiones en ausencia de leyes apropiadas y en cierta manera suplir las carencias causadas por esta situación.

Por otra parte, el Poder Ejecutivo se encuentra muchas veces en situaciones donde la realidad digital ha superado de tal manera a los mecanismos o leyes con los que se puede actuar, que se tienen que tomar decisiones sin el debido soporte legislativo.

Está claro que el Poder Legislativo necesita evolucionar digitalmente con urgencia, no solo en estos dos aspectos sino en muchos otros más que no son menos importantes. No olvidemos que todos los días nacen nuevos Ciudadanos Digitales que vienen a reemplazar a generaciones que por ley de vida van abandonando esta sociedad.

Y los Ciudadanos Digitales quieren soluciones inmediatas, rápidas, eficientes… ya se sabe, con la digitalización, o cambias o desapareces.

Enlaces de interés...

- Separación de poderes
- Poder Legislativo


it Reseller
TECH&CONSULTING
nº 60
OCTUBRE 2020
Cloud Computing
Camino hacia un negocio en crecimiento
JUNTOS HACIA EL CENTRO DE DATOS DEL FUTURO
La pyme y cómo liderar su transformación, a debate
Tendencias en el sector del networking, a debate
it Reseller
TECH&CONSULTING
Cada mes en la revista,
cada día en la web.

JORGE DÍAZ-CARDIEL

SOCIO DIRECTOR GENERAL DE ADVICE STRATEGIC CONSULTANTS

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

La demanda de digitalización impulsa la recuperación económica en EEUU

Compartir en RRSS

El lunes 14 de septiembre, los índices bursátiles repuntaban, tras una semana previa de caídas de los valores tecnológicos. Un fin de semana de por medio y unas cuantas noticias positivas en el sector TI y digital y las bolsas suben de nuevo.

Por supuesto, la realidad es más compleja, pero puede resumirse: los valores tecnológicos alcanzaron este verano máximos históricos desde febrero de 2020, antes de que estallara la pandemia. Apple alcanzó los dos billones de dólares en capitalización bursátil. También Microsoft, Alphabet-Google, Facebook, Amazon, Netflix… todas obtuvieron en el segundo trimestre excelentes resultados, lo que tuvo su reflejo en el aumento de su valor en Bolsa. Ya era hora de hacer beneficios por parte de los que compraron acciones de esas empresas a precios más baratos que los de la semana pasada: vendieron y las bolsas cayeron. Es lo más normal del mundo y lo explica muy bien el inversor billonario Howard Marks, CEO de Oaktree Capital y autor de “The most important thing” and “Business cicles”.

Insisto, nada nuevo bajo el sol, aun cuando hubo analistas financieros, periodistas, inversores despistados y gentes con su propia agenda y no necesariamente buena intención, que hablaron del apocalipsis del ecosistema tecnológico, el fin de Silicon Valley, de la “manifestación del desacoplamiento entre la economía real” y la “exuberancia irracional de los mercados de valores”, frase famosa de Alan Greenspan, entonces presidente de la Reserva Federal o FED, en el punto álgido de las “punto.com” que, sin haber demostrado nada, sin

activos ni resultados, tenían valoraciones bursátiles tan exorbitantes que, por ejemplo, permitieron a AOL (America On Line, Steve Case) comprar TimeWarner por una cantidad tan desproporcionada de dinero que, cuando estalló la burbuja, AOL casi arrastra a la ruina a TimeWarner, como le sucedió a miles de empresas "digitales" que fueron a la ruina causando una recesión económica. Entonces había simplones que afirmaban (¡en 1999!) "Los negocios, o son digitales o no son negocios" (PWC).

En la primera quincena de septiembre de 2020 (dos décadas después) vemos un vídeo de una directiva de McKinsey donde afirma que "en los seis meses de pandemia hemos avanzado más de seis años en Transformación Digital". La muchacha (denominación de origen toledana) no aclara de qué está hablando: su empresa, su sector, la economía, la sociedad, su casa, su familia, su cuenta corriente, ella y una prima de su pueblo, Europa, América, el mundo… Vamos a asumir que se trata de una hipérbole o, incluso una metáfora, "a figure of speech".

Un amigo que trabaja en Telefónica me dijo que, en el primer trimestre del año, "hemos vendido más tecnologías de la digitalización que lo que hubiéramos vendido en cinco años de normalidad sin pandemia". Y, ciertamente, los resultados de la empresa de Telefónica que agrupa los negocios y servicios digitales (Telefónica Tech), crecen a dos dígitos y aporta el 20% del beneficio del grupo. Esto me parece más concreto y plausible: se concreta en el anuncio de resultados trimestral.

¿Qué diferencia hay entre la exuberancia irracional tecnológica digital de hoy y la de hace 20 años? Antaño, no había fundamentales. Las "punto.com" vendían humo, promesas vacías de las que cuestan caro en "blood and treasure" que le gusta decir al economista norteamericano y premio nobel de Economía Joseph Stiglitz: quiebras de empresas, despidos masivos y decepción y tristeza entre la mayoría, versus unos inversores listillos que sabían de qué iba la fiesta y se hicieron billonarios a costa de causar una recesión mundial. El entonces presidente de Disney (The Walt Disney Company), Michael Eisner (1984-2005) rechazó el deal de AOL con acaloradas discusiones con Steve Case, que acabó engatusando al presidente de TimeWarner, cuyo nombre omito y casi causa una de las quiebras más grandes de Corporate América.

En 1999 y 2000 no había demanda de digitalización, sino de computación. Era la Tercera Revolución Industrial que hizo la fortuna de HP, IBM, Apple (en su segunda resurrección, esta vez capitaneada por Steve Jobs, fundador), Microsoft, Dell, Kodak, Oracle, Sun Microsystems, SAP, Intel y mil empresas tecnológicas más. Ordenadores conectados

La recuperación económica en EE.UU. toma velocidad gracias a la digitalización

a Internet, sistemas operativos, microprocesadores, workstations, mainframes, impresoras, redes, conectividad y networking, hardware y software es lo que requería el mercado. Y poder de computación.

Steve Jobs lo entendió muy bien desde Apple (en 2001 empieza con el iPod y continúa con los nuevos Mac, y el iPhone en 2007, el iPad en 2010 y así hasta llegar a ser la empresa más valiosa del mundo) y desde Pixar, donde gracias a la computación que la Ley Moore le provee, (de la Intel que dirige Andy Grove), puede hacer películas extraordinarias como Toy Story o Cars. Una de las primeras decisiones de Bob Iger, presidente y CEO de Disney que sucede a Michael Eisner, es comprar Pixar a Steve Jobs. Disney es hoy lo que es gracias a esa compra y a las que vinieron después: Marvel, Lucas Film y 20th Century Fox. Recientemente, Disney lanzó Disney+ o su servicio de televisión en streaming que, también, en seis meses, de manera tangible, ha conseguido el número de clientes que esperaba conseguir en años (50 millones de suscriptores).

En 1999 y 2000 se requería Computación y no Digitalización, insisto. En 2020, con la maldita pandemia incluida, las empresas y las personas piden Transformación Digital. No es necesario generar la demanda, como en 2000, sino que es un lugar común que, sobre la computación, para triunfar en los negocios y en el puesto de trabajo, es necesaria la siguiente capa, la digital: 5G, Cloud Computing, Inteligencia Artificial y Machine Learning, Automatización de Procesos, Robótica, Impresión 3D, Big Data, Ciberseguridad, Conectividad Instantánea sin latencia, son necesarios. “La necesidad agudiza el ingenio” dicen algunos. Otros afirman que lo que hace la necesidad es generar ansiedad, pero “ius suum cuique tribuendi”, a cada uno, hay que darle lo suyo.

> Las famosas chorradas como "cambio de paradigma" o "cada crisis es una oportunidad", aquí no aplican por indecentes, porque la pandemia ha causado muchos cientos de miles de muertos y millones de enfermos

Las famosas chorradas como “cambio de paradigma” o “cada crisis es una oportunidad”, aquí no aplican por indecentes, porque la pandemia ha causado muchos cientos de miles de muertos y millones de enfermos. Lo que sí hay es demanda. Por eso, las empresas TI-Digitales (FAANG) como Facebook, Amazon, Apple, Netflix y Google, a las que habría que añadir a Microsoft, son las reinas de mambo de las redes sociales y la publicidad online; el comercio electrónico, la logística y la cadena de suministro, televisión en streaming y buscadores de Internet más publicidad online. Todas estas empresas han creado plataformas para ven-

der online (como los famosos market-places del año 2000 que se fueron al garete), tienen una muy rentable fuente de ingresos en Cloud con Amazon Web Services (AWS), Microsoft Azure, Google Cloud… han lanzado sus televisiones en streaming: Amazon Prime Video, Apple+, Netflix y puede añadirse, desde Disney+ a Movistar+, entre otros muchos.

Son solo ejemplos, porque estas empresas utilizan intensivamente y venden a mansalva cloud, Big Data, Inteligencia Artificial, conectividad... En estos negocios está el dinero (Show me the money!!!!, de Jerry McGuire, Tom Cruise) y lo están demandando las administraciones públicas y las grandes empresas. El siguiente paso será ayudar a la pyme y a los autónomos. Curiosamente, en España, por contraste con EE.UU., quienes más impulsan la digitalización entre pymes y autónomos son Fundación Bancaria La Caixa, para, mediante la educación, cerrar la brecha digital; CaixaBank, líder mundial en banca digital y, con Bankia, décimo banco de Europa, El Corte Inglés con la omnicanalidad y Cellnex Telecom con la gestión de infraestructuras de telecomunicaciones inalámbricas.

España no es EE.UU., cuya economía está digitalizada en un 30% (World Bank, IMF, World Economic Forum, Advice Strategic Consultants y National Bureau of Statistics o INE americano), pero Castilla y Aragón todavía tienen bazas que jugar para sacar a España de la recesión económica gracias a la digitalización.

Enlaces de interés...

- Howard Marks, The Most Important Think
- Joseph Stiglitz

Ah! Y no olvidemos que Microsoft se ha llevado buena parte del contrato de cloud del Pentágono; la operación norteamericana de TikTok acabará siendo comprada por Oracle (a quien interesa menos la red social que la plataforma de cloud que impulsará su negocio al nivel de las otras tecnológicas; y Nvidia se hace con ARM en el mercado de semiconductores y procesadores. Softbank, conglomerado japonés dueño de ARM está desinvirtiendo en empresas tecnológicas, aunque temo ese dinero no se reinvierta, sino que vaya a enjugar deuda… Y, cuando Microsoft lanza Surface Duo y su nueva Xbox, Apple obtiene el apoyo de un juez de primera instancia, que le da la razón en su litigio con Epic Games (Fortnite).

¿Anecdóticas estas noticias? No. Son varios, entre miles, ejemplos de cómo la recuperación económica en EE.UU. toma velocidad gracias a la digitalización, “que no necesita un cartero o un portero, que le llame dos veces”, porque el personal hará colas kilométricas para comprar los nuevos productos de Apple anunciados el 15 de septiembre y, viendo a terceros, es objetivo decir que la gente se vuelve literalmente loca con Fortnite…