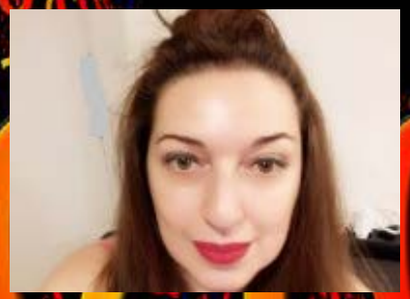
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Noviembre 2020 - nº 35

Compartiendo archivos de forma segura

"En seguridad la heterogeneidad es compleja de gestionar" (Jesús Alonso Murillo)



"El elemento humano es el gran olvidado de los planes de contingencia" (Maite Avelino)

Botech Labs, seguridad paquetizada y simple para el mundo pyme

"Cisco ha estado avanzando hacia el modelo SASE desde hace años" (Eutimio Fernández)

ITWebinars. Trabajo seguro desde cualquier lugar

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

Compartiendo archivos de forma segura

La movilidad, el BYOD, el cloud, han ido añadiendo complejidad tanto a la gestión de las tecnologías de la información, como a su seguridad. En un mundo cada vez más globalizado y sin fronteras, donde los datos se generan por TB en cada vez menos tiempo, controlar la transferencia de archivos es vital. Ya no sólo necesitamos saber quién accede a qué y desde dónde, sino qué hace con los archivos que gestiona, a quién los envía y por qué cauce, así como desde dónde llegan. Hay que tener en cuenta tanto la seguridad como el cumplimiento y la trazabilidad que nos permita obtener la máxima visibilidad y control de cómo se mueve nuestra información.

El CISO invitado de este número de IT Digital Security es Jesús Alonso Murillo, considerado uno de los 25 responsables de ciberseguridad más influyentes de España, con más de 15 años de experiencia en Seguridad de la Información, y responsable de la ciberseguridad de Ferrovial Servicios. Si tuviera un cheque en blanco le gustaría trabajar con herramientas de inteligencia artificial y Deep learning y cree que lo más básico en seguridad es la concienciación del empleado.

También entrevistamos a Eutimio Fernández, Director de Ciber-seguridad en Cisco España, quien asegura que “si no hay cambios o ningún desafío, no hay diversión”; a Maite Avelino, una experta sin pelos en la lengua para quien el cloud es como coger un coche de renting y que asegura que tecnología puntera en Europa hay para aburrir; a José Luis Laguna, Director de Systems Engineering en Fortinet, para quien lo básico es realizar un buen análisis de riesgos y tener una foto lo más precisa posible de en qué situación nos encontramos.

La actualidad llega marcada por el nacimiento de BOTECH Labs, los riesgos de los códigos QR y un debate celebrado recientemente por VMware sobre el teletrabajo, que los empleados han convertido ahora no en una ventaja sino en una condición natural que deben ofertar las empresas.

Por último OneTrust es el protagonista de un #ITWebinars sobre teletrabajo seguro en cualquier lugar, donde se ofrece un análisis del teletrabajo, cómo ha impactado en la empresa y qué elementos hay que tener en cuenta.

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

itds

Sumario

Actualidad

"No podemos dejar en manos del usuario el criterio de utilizar un código QR"
(Daniel González, MobileIron)

#ITWebinars

Trabajo seguro desde cualquier lugar: adaptándonos a la "nueva normalidad"

Entrevistas

Jesús Alonso Murillo,
Ferrovial Servicios

Eutimio Fernández,
Cisco

Maite Avelino
Experta en seguridad

José Luis Laguna,
Fortinet

No solo IT

El Poder Ejecutivo en la Nueva Sociedad Digital: ¿evoluciona o no?

Digitalización, datos, algoritmos y otras hierbas

Índice de anunciantes

Sophos
Eset
Bitdefender
Stomrshield
Panda Security
Secure&IT
Cytomic
IT Webinars
Documento Ejecutivo Teletrabajo
IT User
IT Reseller
CDR Impresión Digital
CDR Tecnología para tu empresa

Sophos Day 2020

Cybersecurity Summit

SOPHOS

EVOLVE

No se pierda a nuestros expertos

19 de Noviembre

Regístrese aquí

© Copyright 2020. Sophos Ltd. All rights reserved.

BOTECH Labs,
seguridad paquetizada y simple para el mundo pyme

En medio de la pandemia, con el teletrabajo campando a sus anchas y jornadas más largas de lo normal, BOTECH últimaba su nuevo proyecto, BOTECH Labs, una nueva compañía con un objetivo: ofrecer seguridad endpoint, cloud y de navegación de manera sencilla y paquetizada.

Fernando Carrazón, CCO de BOTECH FPI

"La mejor definición es raro", dice Fernando Carrazón, CCO de BOTECH FPI, cuando le preguntamos cómo están viendo este 2020. Dice Miguel Ángel Rojo, CEO de la misma empresa en una entrevista conjunta, que el año pasado fue excepcional, tanto que incluso superó sus expectativas. 2020… "arrancó muy bien, en marzo hubo que tirar de freno de mano" y en abril, mayo y junio se ha vivido de la inercia, de temas que estaban pendientes del año anterior; llegó un agosto que se pensaba que iba a estar más animado después del parón obligado de la pandemia, "pero no ha sido así. Ha sido un mes de agosto a la española, aquí no había nadie", añade Miguel Ángel Rojo.

La pandamia, dice Fernando Carrazón, ha hecho que los fabricantes se hayan acostumbrado a la nueva manera de ir a los clientes, y a los clientes a una nueva manera de recibir a los fabricantes. Esta 'nueva manera' está permitiendo "acceder de manera más fácil a ciertos clientes". Y es que las videoconferencias, esa lejanía y desapego que generan, permiten a un responsable de IT tomar decisiones más rápido y sin tanta incomodidad que cuando se está frente a frente con un comercial. La nueva manera, asegura el COO de BOTECH, es: "te doy 15 minutos de vídeo y si no me interesa te lo digo".

Inmersos en esta nueva forma de hacer negocio, en la distancia y a través de una cámara web, con los trabajadores en sus casas y el inevitable tiempo de reflexión que ha dado el confinamiento, lo cierto es que lejos de paralizar su actividad, BOTECH ha acelerado.

Hace tiempo que la compañía saltó las fronteras españolas, con una amplia presencia en México y haciendo negocio en Estados Unidos. Y como explica Fernando Carrazón, esta nueva manera de hacer las cosas está facilitando las relaciones y proyectos transoceánicos; "estamos empezando a movernos mucho más por allí. Tenemos varios proyectos y está siendo más fácil y habitual convocarnos a través de vídeo con clientes del otro lado del charco". Tan habitual como para que ambos directivos auguren que esta nueva manera de gestionar los negocios, de una manera telemática y a través de videoconferencia se vaya a extender durante el año que viene. Tanto es así que por el momento BOTECH no ha puesto plazo para la vuelta a la oficina.

La propuesta de BOTECH Labs es B2B2C, por lo que el cliente es un ISP, una telco, una asociación profesional, un banco, un ayuntamiento, aseguradoras...

Al mercado pyme tienes que llegar y posicionarte de una manera diferente y con un producto distinto

Al respecto, la compañía mantiene abierta sus oficinas para que se puedan realizar reuniones con las máximas garantías de espacio y un tiempo máximo de permanencia de una hora y media. Después de esa reunión entra en acción un equipo de limpieza anti COVID. “Todos nos estamos replanteando si el tamaño de oficina que tenemos es el que necesitamos”, reflexiona Miguel Ángel Rojo.

Nueva estrategia – BOTECH Labs

Este 2020, este año raro, ha dado para mucho. La nueva normalidad hay que asumirla, tanto o más que adoptar una transformación digital que se ha acelerado al máximo. Explica el CEO de BOTECH que “para nosotros va a haber un gran cambio”, que no es otro que la consecución de una estrategia que se inició a finales del año pasado y consiste en “aprovechando toda nuestra experiencia en grandes clientes crear servicios mucho más pequeños, paquetizables y enfocados al mundo pyme”. Un mercado, añade Rojo, en el que tienes que posicionarte de una manera diferente, con un producto diferente y al que tienes que llegar de una manera diferente, “con algo que sea súper sencillo y súper fácil”.

Esta nueva estrategia se concretó el pasado 9 de septiembre con el nacimiento de BOTECH Labs, una nueva compañía “que es la que va a contener toda la propiedad intelectual, todos los proyectos que tenemos con CEDETi, al tiempo que BOTECH FPI se queda como la compañía de servicios al cliente final”, explica Miguel Ángel Rojo, añadiendo que con BOTECH Labs se buscan incluso colaboraciones con otros canales “que antes para nosotros no estaban un poco en nuestro radar”, como empresas que se dedican a canalizar productos para pymes, e incluso otro tipo de mayoristas.

Hasta el momento se cuenta con algunas propuestas gratuitas, ya operativas, y próximamente se tendrán otras opciones encima de la mesa.

Todo comenzó con ISOPH

Hace unos meses, en mayo de este año, se anunciaba ISOPH, una tecnología gratuita para que empresas, pymes y autónomos puedan conocer la seguridad de sus equipos. La tecnología, el primer producto de BOTECH Labs, que se amplió en octubre de este año, permitía inicialmente conocer las vulnerabilidades que presenta el equipo en el que se instala, y proporciona información de gran valía para conocer el estado de seguridad y poder tomar medidas para evitar incidentes.

Miguel Ángel Rojo, CEO de BOTECH FPI

Hace unos meses, en mayo de este año, se anunciaba ISOPH, una tecnología gratuita para que empresas, pymes y autónomos puedan conocer la seguridad de sus equipos

Y si la primera entrega de la tecnología facilitaba el diagnóstico de los equipos para que se puedan tomar las medidas adecuadas, solucionar vulnerabilidades y tener tu equipo seguro, en la segunda entrega se ampliaban los servicios para la protección de la nube y la navegación.

Explica Fernando Carrazón que la compañía contaba con piezas de tecnología que se habían desarrollado para dar servicio a los clientes, desde soluciones de análisis forense para móviles o seguimiento de vulnerabilidades. Si esas piezas ya desarrolladas se hacen escalables gracias al cloud, “lo que te queda es pensar en cómo lo llevas a una pyme, a un autónomo”. Y aprovechando el confinamiento se empezaron a hacer los primeros experimentos, las primeras pruebas. Detrás de ellas una realidad: con el teletrabajo se ha perdido cierto control de los equipos que están utilizando los empleados, la mayoría de los cuales se han tenido que instalar zoom o software de acceso remoto que generaron algunos problemas de seguridad. “Ante la situación se lanza ISOPH, que es un agente que puede analizar el equipo esté donde esté para que la empresa puede tener controlados ciertos aspectos de la seguridad, como es tener las aplicaciones actualizadas, que la VPN se conecte como debe, qué vulnerabilidades tiene el equipo, y eso de manera desatendida porque ya no se está en la oficina”, explica Fernando Carrazón.

“Tecnológicamente no era complicado hacer las adaptaciones, las piezas de tecnología, pero sí nuestra manera de ofrecerlo”, dice el COO de BOTECH, porque se trata de una solución paquetizada, muy fácil de utilizar y que se entienda, que aporte valor al cliente, muy escalable y con precio ajustado, “porque ya no voy a ir a 10.000 usuarios, voy a un millón”.

Por el momento y tras las primeras pruebas, se tienen “un buen montón de equipos suscritos”. Son

Enlaces de interés...

- BOTECH Solutions
- BOTECH amplía sus servicios ISOPH para proteger nube, endpoint y navegación
- Conoce la seguridad de tus equipos de forma gratuita con ISOPH

BOTECH Labs aprovecha toda la experiencia en grandes clientes para crear servicios mucho más pequeños, paquetizables y enfocados al mundo pyme

muchos los que empiezan por esa parte gratuita, una manera de probar el producto, "y si te gusta me vuelves a llamar y te enseño la versión profesional", porque "qué mejor demo que algo que sea real y esté en funcionamiento".

La manera de llevarlo al mercado es de forma transparente, con marca de cliente final. "Es un concepto marca blanca. Somos el que está atrás y lo que nos interesa es el volumen de clientes", explica Miguel Ángel Rojo, añadiendo que la propuesta es B2B2C, y el cliente final es el de un ISP, una telco, una asociación profesional, un banco, un ayuntamiento, aseguradoras…

Explica Fernando Carrazón que al final BOTECH Labs lo que hace es "aunar todas las tecnologías que teníamos", y que se ha establecido un equipo de I+D específico porque "estoy creando tecnología que me están demandando, que ya tiene que tener un mantenimiento, tiene que tener un roadmap, una tecnología que hay que paquetizar y hay que ofrecer a un cliente y que "no podemos contaminar con los proyectos de la empresa de servicios". Continúa diciendo el directivo que "había que separar bien quién hace la parte de la tecnología de que quién hace los servicios. Por eso hemos creado BOTECH Labs".

En lo que respecta al negocio de la nueva BOTECH Labs, dice Miguel Ángel Rojo que ya hay tres grandes proyectos "que son los grandes impulsores para cerrar este trimestre y arrancar el próximo".

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

ESET Threat Intelligence
ESET Virus Radar
WeLive Security

PREVENCIÓN

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

RESPUESTA

ESET Enterprise Inspector
ESET Dynamic Threat Defense
ESET Security Management Center
ESET Cloud Administrator

DETECCIÓN

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

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

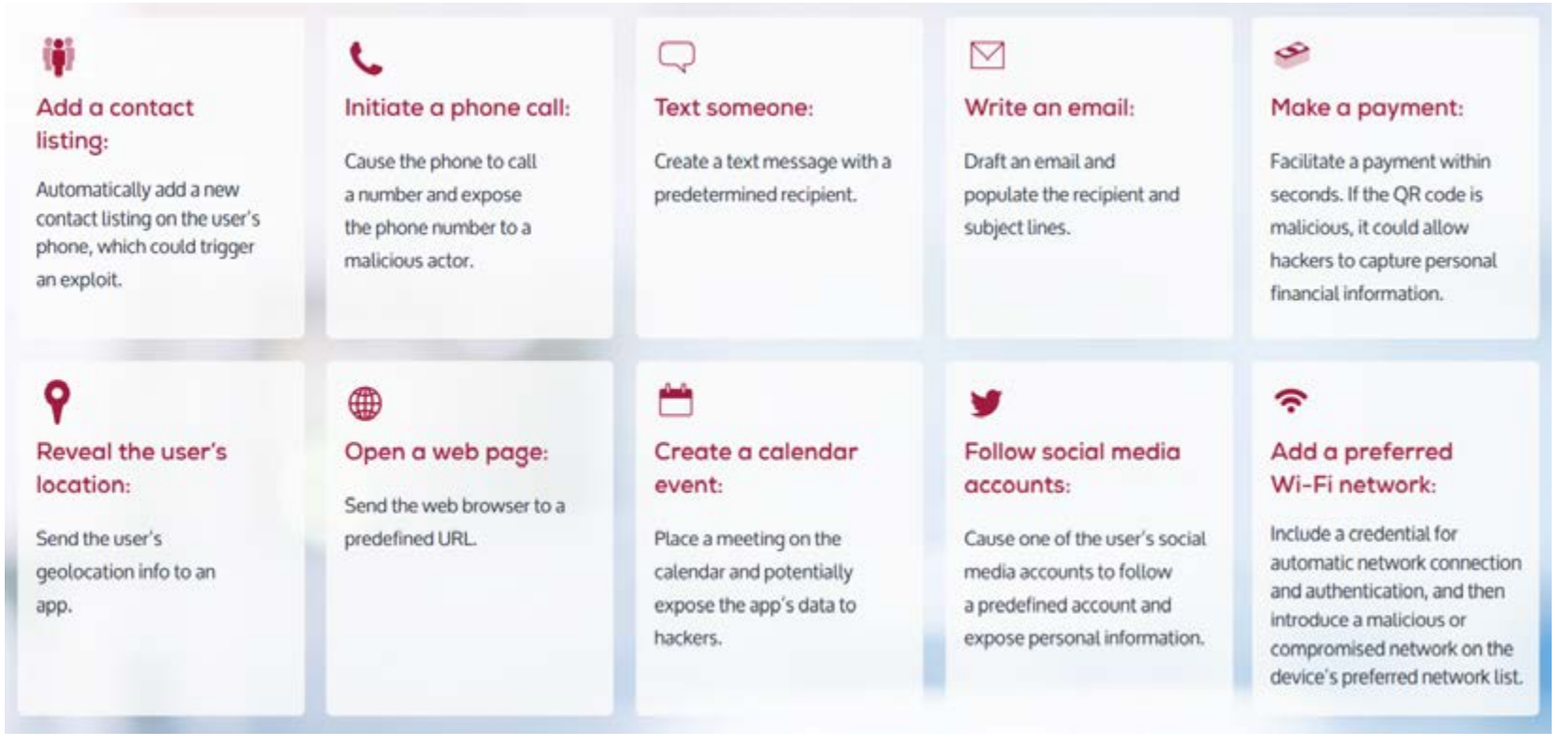
MADE IN EU

“No podemos dejar en manos del usuario el criterio de utilizar un código QR”

(Daniel González, MobileIron)

En más del 90% de los ataques está involucrado un dispositivos móvil, ha dicho Daniel González, senior key account de MobileIron, durante la presentación de un informe que pone de manifiesto el peligro que se enconde tras los códigos QR.

Evolución del código de barras, el código QR fue inventado en 1994 por Masahiro Hara, de la empresa japonesa Denso Wave, con el propósito era rastrear vehículos durante la fabricación. Uno de los mayores desafíos para el equipo fue hacer que la lectura de su código fuera lo más rápido posible, de ahí su nombre: Quick Response (QR). Este código no solo puede contener una gran cantidad de información, sino que también puede leerse más de 10 veces más rápido que otros códigos y su uso se ha generalizado hasta llegar al mercado de consumo.



En España somos líderes en el uso de códigos QR

Pero los código QR son, además, peligrosas trampas que los ciberdelincuentes utilizan con cada vez más asiduidad para llevar a los usuarios donde quieren. Así lo recoge un reciente informe de MobileIron, una empresa que, un año después, sigue teniendo la única plataforma certificada por el Gobierno de España para la gestión y automatización de dispositivos móviles.

El informe de la compañía dice, entre otras cosas, que en España el 90,4% de los usuarios móviles ya ha escaneado este tipo de códigos en los últimos seis meses, que un 74% estaría dispuesto a utilizar esta tecnología como método de pago en el futuro, y que un 44% estaría dispuesto a votar mediante un código QR.

"El uso de los códigos QR cada vez es más habitual, y esto lo saben los ciberdelincuentes",

https://www.itdigitalsecurity.es

EL CRECIENTE RIESGO DE LOS CÓDIGOS QR

El 51% de los usuarios se sientes preocupados por su privacidad o seguridad cuando utiliza códigos QR, pero los usa de todos modos. Es probable que veamos que el uso de códigos QR siga aumentando en los próximos años, especialmente porque facilitan cosas como los pagos, la autenticación y otras tareas diarias en un mundo sin contacto.

BYOD vs COPE

Existe cierto empeño por parte de las empresas por no securizar los dispositivos móviles. Desconocimiento y presupuesto son dos de las razones por las que esto sigue ocurriendo.

Explica Daniel González que a nivel tecnológico ya se pueden establecer contenedores en dispositivos personales y corporativos.

Desde antes de la entrada en vigor de GDPR en abril de 2018 los sistemas operativos, iOS, Android y Windows 10 vienen preparados para separar de forma inequívoca el entorno personal y laboral mediante certificados digitales.

Si de lo que se trata es de un dispositivo corporativo se habla de COPE (Corporate Owner personal Enablement), que permite establecer un contenedor personal y se le da la llave al empleado y se le dice: con esta llave lo que hagas dentro de ese contenedor es tuyo y es privado.

asegura Daniel González, senior key account de MobileIron, añadiendo que “en España somos líderes en el uso de códigos QR” y que el ciberdelincuente sabe que el teléfono móvil es un ordenador de bolsillo “y que lo llevamos desprotegido”.

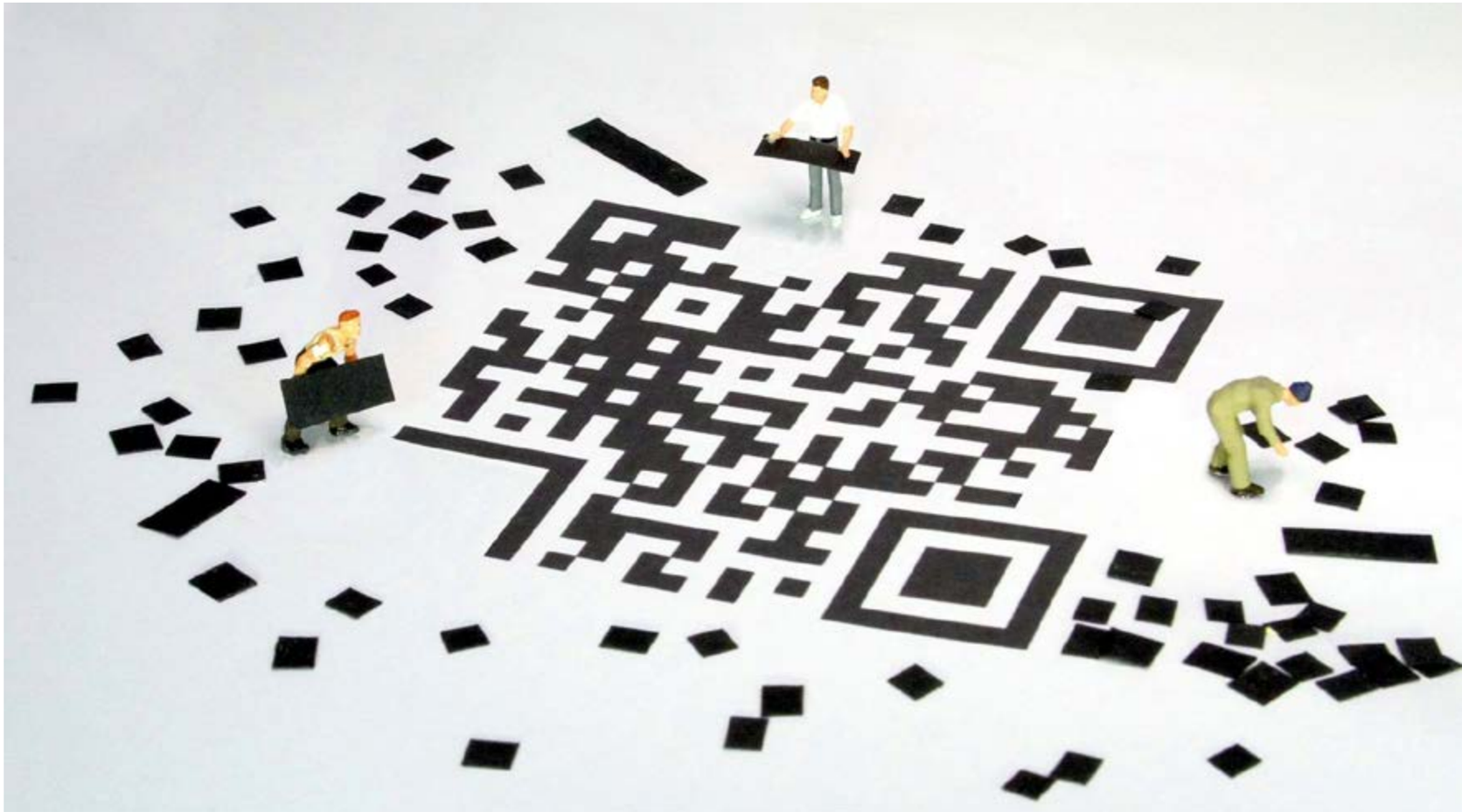
Lo cierto es que los usuarios desconocen muchas de las cosas que puede desencadenar el escaneo de un código QR. Lo que los usuarios asocian como habitual es que el escaneo de un código QR conlleve la apertura de una página web o la descarga de un PDF, dice el directivo de MobileIron, pero hay otros once usos “y aquí es donde está la trampa”. Añadir un contacto, iniciar una llamada telefónica, hacer un pago, escribir un correo electrónico, enviar un SMS a alguien, revelar la ubicación del usuario, añadir una red WiFi, seguir cuentas de redes sociales o crear un evento en el calendario son otro tipo de acciones que se ejecutan al escanear un código QR.

"El ciberdelincuente sabe que el teléfono móvil es un ordenador de bolsillo y que los llevamos desprotegidos"

Daniel González,
senior key Account, MobileIron

Enlaces de interés...

- MobileIron mejora la seguridad de las apps con la compra de incapptic Connect
- Ivanti compra MobileIron y Pulse Secure
- Los trabajadores no quieren volver a la oficina



"No podemos dejar en manos del usuarios el criterio de utilizar un código QR", dice Daniel González, ni tampoco impedirle su uso "porque estaríamos poniendo trabas a la tecnología". Por lo tanto, "las empresas y los organismos tienen que dotarse de herramientas para que el móvil que llamamos smartphone sea realmente inteligente y pueda ayudar a los usuarios a detectar los códigos QR falsos".

MobileIron Threat Defense (MTD), que permite detectar y corregir de forma temprana los ataques en dispositivos, redes y aplicaciones en dispositivos móviles, es un módulo que se activa, o no, en la solución UEM (Unified Endpoint Management) de la compañía.

La solución, explica Daniel González, protege la red y datos corporativos contra las amenazas malintencionadas gracias al aprendizaje automático y la detección basada en comportamiento. Con medidas de cumplimiento basadas en políticas que proporcionan alertas de comportamientos peligrosos, MTD anula de forma proactiva los ataques en el dispositivo sin necesidad de conectividad en red, aíslan los dispositivos afectados de su red y eliminan las aplicaciones malintencionadas y su contenido. Por otra parte, se consigue más visibilidad y conocimiento del dispositivo, el sistema operativo, la red y los riesgos de las aplicaciones, así como otra información procesable para poder responder de forma más rápida y eficaz a las amenazas.

Los usuarios desconocen muchas de las cosas que puede desencadenar el escaneo de un código QR

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTION DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

“El teletrabajo se convierte en requisito esencial de los empleados”

(VMware)

Ya no hay marcha atrás. Los trabajadores tuvieron que hacer sitio en sus hogares y organizar sus horarios para garantizar la continuidad de negocio. Y ahora no quieren volver a sus oficinas, o por lo menos no de la misma manera y sin opciones. El teletrabajo se ha convertido, según un reciente estudio de VMware, no en una ventaja sino en una condición natural de trabajo.

"La difícil situación de los últimos meses ha obligado a las empresas a adaptarse rápidamente a nuevas prácticas laborales en las que ir a trabajar ya no significa acudir a la oficina", ha dicho Kristine Dahl Steidel, vicepresidente de la unidad de computación para usuarios finales de VMware para la región de EMEA, en una mesa redonda online en la que se debatió la realidad del teletrabajo en torno a un estudio sobre la percepción de las nuevas formas de trabajo.

Refiriéndose a una fuerza laboral distribuida como colaborativa, comprometida, visible y productiva que ya ha beneficiado a miles de empresas y millones de empleados, aseguraba también Kristine Dahl Steidel que "las empresas con una base digital deben adoptar una cultura y un enfoque del liderazgo que permitan crear una nueva forma de trabajo".

Lo cierto es que desde que comenzara la pandemia, el 41% de los trabajadores esperan poder trabajar de forma remota; ya no se ve como una ventaja, sino como una condición natural de trabajo. El informe recoge también que la cultura de la directiva no estimula el teletrabajo, según un 39% de los empleados, o que un 65% se siente presionado para seguir conectado más allá del horario laboral habitual. En todo caso, los elementos positivos pesan más, ya que el teletrabajo no sólo permite buscar talento en diferentes partes del mundo, sino que un 69% cree que las relaciones con los compañeros han mejorado, y un 67% se siente más confiado para hablar en reuniones de videoconferencia.

El teletrabajo también afecta al estado de ánimo, que ha mejorado un 28%, así como a la productividad, que se ha incrementado un 30%

Por cierto que las herramientas de videoconferencia se han convertido en el salvavidas del trabajador remoto y con más personas trabajando desde casa y colaborando a través de reuniones en línea, la seguridad de las mismas se ha convertido en el centro de atención.

Kristine Dahl Steidel, destacó que los empleados reconocen que su organización está cosechando los beneficios de trabajar de forma remota y que no pueden volver atrás. Sin embargo, existe la preocupación de que la dirección no se esfuerce lo suficiente por adaptarse y ofrecer a sus empleados más opciones y flexibilidad.

El teletrabajo también afecta al estado de ánimo, que ha mejorado un 28%, así como a la productividad, que se ha incrementado un 30%. Según el informe, el nuevo modelo de trabajo ha permitido atraer talento de primer nivel sobre todo en el caso de padres y madres trabajadoras, y ha provocado que la innovación llegue desde más lugares dentro de la empresa.

Teletrabajo más allá de la tecnología

Además de los retos tecnológicos que plantea el teletrabajo, durante el debate se mencionaron algunos otros. Por ejemplo Kristine Dahl Steidel aseguraba que esta nueva normalidad en la que el teletrabajo es protagonista invita a “reinventar todo”. Por ejemplo, añadía, habrá menos oficinas y menos viajes, mientras aumentan las posibilidades para los reclutadores. Al respecto Carl Benedikt Frey predice que las empresas deslocalizarán más actividades a los países en desarrollo, donde los costes salariales son más bajos.

También se mencionó durante el debate si los mandos intermedios son necesarios teniendo en cuenta que los trabajadores son ahora más independiente. Benedikt Frey dice que se necesitarán menos gerentes y las empresas tendrán que adaptarse a equipos cada vez más autónomos.

Respecto a la oficina del futuro… “Los rascacielos están desapareciendo y ya no es una obligación que las (nuevas) empresas se establezcan en el centro de las ciudades con alquileres elevados”, aseguraba también Benedikt Frey mientras Véronique Karcenty apuntaba que Orange está pensando en espacios de coworking.

Por cierto que los departamentos de TI ya no se ven como un inhibidor de las prácticas laborales distribuidas, donde los empleados pueden trabajar desde la sede, una oficina local, desde casa, en movimiento o una combinación de ubicaciones: menos de un tercio de las personas entrevistadas cree que el departamento de TI no está preparado para administrar una fuerza laboral remota.

Focalizarse en los resultados es, según Carl Benedikt Frey, director del programa sobre el futuro laboral en la Universidad de Oxford, en lo que deben centrarse las organizaciones "para adoptar plenamente la modalidad del trabajo desde cualquier lugar".

Para Véronique Karcenty, directora de espacio de trabajo digital de Orange Francia, "no deberíamos subestimar el cambio que se debe producir en las

it whitepapers

TELETRABAJO EN 2020, EL FUTURO SE HACE PRESENTE

IT Research, en su ánimo por estudiar la realidad digital, ha puesto en esta ocasión su atención en el desarrollo de los planes de teletrabajo a raíz del confinamiento vivido por la población española en este 2020, y la posición de trabajadores y directivos ante esta situación. Descargue este informe y conozca cómo se han desarrollado estas políticas de teletrabajo, su futuro y qué elementos técnicos han jugado un papel fundamental en su desarrollo.

Enlaces de interés...

- INCIBE y Google forman a las empresas sobre cómo implementar el teletrabajo sin riesgos
- Amenazas a las empresas en España durante la pandemia
- Consejos para evitar las ciberamenazas ligadas al teletrabajo

Aun presentando indudables ventajas, el teletrabajo también presenta algunos retos, como es la seguridad y protección de los empleados

estrategias de gestión del personal para motivar a los empleados y mantener su productividad. Si bien el liderazgo de los directores ejecutivos es importante para determinar la estrategia general, son los jefes directos quienes necesitan mostrar confianza, estimular a su equipo e infundir la idea de un objetivo común".

Retos

Decíamos al comienzo que aun presentando indudables ventajas, el teletrabajo también presenta algunos retos, como es la seguridad y protección de los empleados.

"La magnitud actual de la fuerza laboral distribuida, debido a la pandemia, ha potenciado la proliferación de tecnologías y plataformas digitales, aseguran desde VMware. La situación actual ha provocado que mientras intentan continuar con sus operaciones, las organizaciones trasladan más aplicaciones a la nube, lo que en muchas ocasiones genera nuevos silos de información.

Además, a medida que las fuerzas laborales se encogen y expanden, y algunos empleados prefieren quedarse en casa, el conjunto de dispositivos de las organizaciones que admiten la modalidad de trabajo remoto es cada vez más heterogéneo, con la adopción de estrategias BYOD. En consecuencia, cada dispositivo nuevo conectado a la red empresarial representa un posible blanco de ataque para los hackers.

Todos estos factores alteran el perímetro de seguridad de las empresas, lo que hace imprescindible contar con modelos de seguridad de confianza cero.

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/

‘En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar’

(Jesús Alonso Murillo, Ferrovial Servicios)

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

Ha sido considerado uno de los 25 responsables de ciberseguridad más influyentes de España, ese puñado de profesionales a los que llamar en caso de crisis. Acumula más de 15 años de experiencia en Seguridad de la Información, tanto en compañías de consultoría como de telecomunicaciones, el sector financiero y, el más reciente, los servicios. Jesús Alonso Murillo es el CISO de Ferrovial Servicios, si tuviera un cheque en blanco le gustaría trabajar con herramientas de inteligencia artificial y Deep learning y cree que lo más básico en seguridad es la concienciación del empleado.

No hace mucho que Jesús ha estrenado su puesto como CISO de Ferrovial Servicios después de gestionar la seguridad y el riesgo TI en BBVA. Estar al día en tecnología es una de las cualidades que debe tener un buen CISO, asegura, además de "estar cerca de negocio" para, entre otras cosas, hacerles comprender "por qué alguna vez les dices que no y otras veces les pones trabas".

A la pandemia sanitaria se le hizo frente "como todos, corriendo un poco". Nadie se esperaba tener a toda la plantilla trabajando en remoto, que al mismo tiempo algunos pidieran trabajar en la oficina para abordar determinados proyectos, o que, al menos en los inicios, hubiera cierta necesidad de estar continuamente conectado a sistemas de videoconferencia.

Sobre si la seguridad ha dejado de considerarse un gasto, asegura Jesús Alonso que en realidad es una inversión porque "sin seguridad, no somos competitivos, y un incidente puede hacernos perder toda nuestra reputación y exponernos a multas millonarias". En todo caso, no es la realidad española, donde más allá de sectores fuertemente regulados, "se sigue viendo como un gasto, dado que la seguridad total no existe, y siempre es necesario más presupuesto". Añade también el CISO de Ferrovial Servicios que la realidad es que mientras a los responsables de ciberseguridad les cuesta defender los presupuestos, a los cibercriminales cada vez les cuesta menos financiarse; "no hay más que ver la capitalización del Ramsonware que existe últimamente".

"El trabajo en remoto exige un cambio de paradigma. Ahora todos trabajamos desde casa, y los entornos que teníamos perimetrados han perdido el sentido"

"La heterogeneidad es difícil de gestionar, y sobre todo de financiar", apunta Jesús Alonso cuando le preguntamos cuáles son los grandes problemas de ciberseguridad a los que se enfrenta Ferrovial Servicios. "Necesitamos balancear diferentes soluciones y tecnologías para servicios y proyectos muy complejos, así como para otros más sencillos, pero igual de expuestos", añade el directivo. Esos problemas, por cierto han cambiado en la pandemia, cuando el teletrabajo "y los entornos que teníamos perimetrados han perdido el sentido".

Aunque los estudios señalan un aumento del 430% en los ataques contra la cadena de suministro, ser parte de esa cadena no le quita el sueño a Jesús Alonso Murillo. Dice que nadie está fuera del foco de los ciberdelincuentes y por tanto proteger y protegerte como parte de la cadena de suministro

"Un buen contrato es la mejor manera de abordar la nube de manera segura"

"forma parte del día a día". La clave, añade, "es tener monitorizados tus sistemas, hacer análisis diarios y que te des cuenta de lo que está pasando", que no es poco. En todo caso, en Ferrovial Servicios "revisamos y tenemos control de la cadena de suministro, de aquellos proveedores que nos dan servicio, a los que damos servicio, y tecnologías asociadas a los servicios que prestamos y las que nos prestan". En definitiva, se tienen controles tanto técnicos como a través de contratos con cada uno de ellos.

La situación, aclara, lleva a que "cuanto más extiendas el perímetro, tanto para el trabajo del usuario final, el endpoint, como para la cadena de suministro de los servicios que prestas, más complicado es la protección. Pero hay mecanismos para tratar de apantallarlo y cortarlo antes de que se extienda".

Un cloud seguro

Un buen contrato es, según la experiencia de Jesús Alonso, la mejor manera de abordar la nube de manera segura. Dice el directivo que en ocasiones la tarea no es sencilla, pero que la mejor garantía es contar con un buen contrato "que te permita revisar y supervisar los controles y seguridad que tiene dicho entorno", además de pedir las certificaciones necesarias, revisando bien el alcance

"Para muchos negocios se sigue viendo como un gasto, dado que la seguridad total no existe, y siempre es necesario más presupuesto"

de las mismas, para asegurarnos que se aplican los controles adecuados". Por último asegura que es importante "poder revisar periódicamente con nuestros equipos de defensa interna dichos entornos (hasta donde nos dejan), para revisar el punto de compromiso de los mismos".

La concienciación de los usuarios es la "tecnología" de seguridad imprescindible en cualquier empresa. "Sin esa 'tecnología', el resto no sirve para nada", afirma el CISO de Ferrovial Servicios. Explica que si no nos damos cuenta de que no podemos trabajar con información en local, compartirla en un cloud público, enviarla por correo, sacarla en un pendrive, abrir una web de dudosa procedencia… el resto de tecnologías son "detectivas" y "preventivas", pero la experiencia nos dice que donde hay una persona tiene que haber conciencia de seguridad.

En todo caso, Jesús Alonso apuesta por los mecanismos de monitorización, detección y respuesta, así como análisis de comportamiento o parcheo de vulnerabilidad. Y aunque no como tecnología de seguridad, apunta como útiles las tecnologías de isolation, o de IRM, "muy útil de cara a la información que maneja el usuario".

Si tuviera un talón en blanco, ¿qué tecnología le gustaría implementar? "Inteligencia artificial y Deep learning en el análisis de logs e información que recogen los sistemas para prevenir ataques que no existen en patrones de forma proactiva", concreta el directivo añadiendo que algunas de estar tecnologías aún están en fase de estudio pero que si pudiera implementarlas "me parecería algo muy divertido de hacer".

A punto de acabar de año, la última pregunta que le hacemos a Jesús Alonso Murillo es si espera que haya algún cambio significativo en 2021 en torno a la seguridad. Tiene claro que el cambio lo estamos viviendo, "y es en torno al trabajo en remoto, y la descentralización total, que ha venido para quedarse; la tecnología hemos visto que nos acompaña, y la seguridad, existe. Ahora tenemos que convivir con ambas endureciendo los controles, para un trabajo en remoto, menos esporádico y para más usuarios".

Añade que la vuelta a las oficinas será parcial y que contar con una licencia por usuario para el acceso remoto no va a ser una excepción, "va a ser sí o sí a partir de ya".

Enlaces de interés...

- 'No tiene sentido ver la seguridad como un gasto' (Rubén Fernández, Grupo DIA)
- 'Está demostrado que cada vez que inviertes en educación el nivel de fraude baja' (Iker Osorio, Cetelem)
- 'El Shadow IT sigue siendo un grandísimo problema hoy en día y con cloud todavía más' (Globalia)
- "Un servicio gestionado puede ser tan bueno como estés dispuesto a hacerlo" (Iván Sánchez, Sanitas)

Compartir en RRSS

WatchGuard

panda
a WatchGuard brand

La aniquilación del ransomware

No permitas que un ransomware paralice tu negocio.

'La clave de SASE es la capacidad de combinar la SD-WAN y la seguridad en la nube en una solución integrada'

(Eutimio Fernández, Cisco)

Atrás han quedado los tiempos en los que costaba ver a Cisco como una empresa de seguridad. Eutimio Fernández, Director de Ciber-seguridad en Cisco España, es el gran artífice de este cambio. Los más de 25 años que lleva trabajando en ciberseguridad le han permitido ver crecer un mercado valorado en más de 150.000 millones de dólares en 2019, y con unas inmejorables perspectivas de crecimiento.

Rosalía Arroyo

Eutimio Fernández llegó a Cisco en 2013, cuando Sourcefire, la empresa que lideraba en España, fue comprada por el que se ha conocido durante años como el gigante de las redes. Sourcefire, por la que se pagó 2.700 millones de dólares y que desarrollaba tecnologías para la protección de la red y la detección de amenazas, no hacía sino sumar en el creciente portfolio de tecnologías de seguridad de Cisco, que a comienzos del mismo año ya se había hecho con Cognitive Security. El año anterior había comprado Virtuata, y los años siguientes vieron las adquisiciones de ThreatGRID, que ofrecía análisis de malware dinámico, y Neohapsis, que proporcionaba gestión del riesgo y cumplimiento en 2014; OpenDNS, Portcullis y Lancope en 2015; CloudLock en 2016, lo que le permitió adentrarse en el mundo de los CASB; Observable Networks en 2017, DuoSecurity en 2018... Y como no sólo se seguridad viven las empresas, por el camino la compañía también sumó algunas adquisiciones expertas en orquestar y mejorar la visibilidad de la red, creando un oferta completa.

En lo que a redes se refiere los cambios durante los últimos años han sido enormes. De grandes estructuras monolíticas y propietarias hemos pasado a

"Cisco Managed Detection and Response (MDR) combina un equipo de expertos avalados por Cisco Talos que pueden reducir el tiempo de detección y respuesta de meses a horas"

una red definida por software capaz de dar el mismo tipo y calidad de servicio a un cloud flexible del que hoy se espera mucho y del que mañana no se quiere nada. Redes y seguridad han confluido y estamos en la era del SD-WAN, del SASE, del Zero Trust Network (ZTN)… y sobre todo esto preguntamos a Eutimio Fernández, el hombre que asegura que "si no hay cambios o ningún desafío, no hay diversión".

¿En qué momento está el negocio de seguridad de Cisco?

En su mejor momento. Cisco es el mayor proveedor de seguridad empresarial del mundo (cuota en términos de ingresos según Canalys). Contamos con más de 5.000 profesionales dedicados y una inversión superior a los 6.000 millones de dólares en los 5 últimos años, con adquisiciones como Duo Security.

El 30 de junio anunciamos Cisco SecureX. Es la plataforma de seguridad cloud nativa más amplia de la industria, que reinventa la forma en que nuestros clientes experimentan la seguridad, haciéndola más sencilla y automatizada. Cisco SecureX conecta las soluciones de seguridad con toda la infraestructura de las organizaciones ofreciendo una experiencia consistente y simplificada. Unifica la visibilidad, facilita la automatización y refuerza la protección en la red, los terminales, la nube y las aplicaciones.

¿Qué ha pasado para que el concepto SASE (Secure Access Service Edge) se haya puesto tan de moda?

Estamos en la era multi-cloud. Las organizaciones albergan y acceden a sus datos y aplicaciones desde cualquier lugar y dispositivo. Además, el creciente número de trabajadores remotos, requiere un acceso seguro a las aplicaciones, pero también con un rendimiento óptimo.

"Umbrella proporciona la escalabilidad y la fiabilidad necesarias para proteger la fuerza de trabajo remota de hoy en día"

Con un 60% de las organizaciones que esperan que la mayoría de las aplicaciones estén en la nube para el año 2021 y más del 50% de la fuerza de trabajo operando de forma remota según ESG, el nuevo modelo SASE definido por Gartner que converge servicios de red y de seguridad permite conectar de forma segura a cualquier usuario o dispositivo a cualquier aplicación con la mejor experiencia. La clave de SASE es la capacidad de combinar la SD-WAN y la seguridad en la nube en una solución integrada, ayudando a las fuerzas de trabajo distribuidas a mantenerse conectadas y seguras.

¿Por qué habría que adoptar un modelo SASE?
SASE permite identificar a los usuarios, dispositivos y sistemas de IoT/OT, proporcionando un acceso directo y seguro a las aplicaciones alojadas en cualquier lugar, incluyendo centros de datos, nubes privadas y públicas (como Azure, AWS, Google Cloud) y proveedores de SaaS. Para ello, combina la red WAN con funcionalidades de seguridad de como SWG (Secure Web Gateway), Cloud Access Security Broker (CASB) o FWaaS. Al proporcionar servicios de seguridad y de red integrados desde la nube, las organizaciones pueden conectar de forma segura cualquier usuario o dispositivo a cualquier aplicación con la mejor experiencia.

¿Cuál es la aproximación de Cisco en torno a SASE?
Cisco ha estado avanzando hacia este modelo desde hace años, con adquisiciones clave en redes (Meraki, Viptela) y seguridad (OpenDNS, CloudLock, Duo) así como muchas innovaciones desarrolladas internamente. SASE se basa en la convergencia de SD-WAN administrada desde la nube y la seguridad Cloud, dos capacidades clave en las que Cisco es pionero y un líder contrastado. Más de 20.000 organizaciones de todo el mundo han comenzado el camino hacia SASE mediante la implementación de SD-WAN de Cisco, y más de 22.000 han adoptado los servicios de seguridad en la nube de Cisco Umbrella.

Hace unos meses, anunciamos la integración de Cisco Umbrella con Cisco SD-WAN en una solución SASE, que permite a las empresas protegerse frente a los principales ataques que surgen del modelo SaaS y del acceso a Internet. Cisco Umbrella ofrece una puerta de enlace web segura (SWG), seguridad de la capa DNS, cortafuegos y funcionalidad CASB

en un mismo servicio de nube integrado. Si añadimos nuestra apuesta por la seguridad zero trust en el acceso -con soluciones como la autenticación multi-factor de Duo Security- refuerza la seguridad de los trabajadores remotos, mejora el rendimiento de las aplicaciones y reduce costes y complejidad.

Hace tiempo que Cisco dice que la seguridad está en la red, pero, ¿se puede mantener la seguridad y el rendimiento en un mundo totalmente descentralizado?
Precisamente, la respuesta a esa descentralización es la SD-WAN combinada con la seguridad Cloud. Con la proliferación de aplicaciones, cargas de trabajo y servicios cada vez más distribuidos a través del Cloud y el extremo de la red, las organizaciones se enfrentan a nuevos retos para la WAN.

Las nuevas plataformas Catalyst 8000 Edge de Cisco tienden un puente entre el extremo de la WAN y el extremo de la nube, ayudando a los clientes a proporcionar conectividad automatizada y segura a las aplicaciones a través de la nube, el centro de datos y el extremo de la red. Para aquellos que pretenden adoptar una arquitectura SASE, Cisco SD-WAN converge la SD-WAN gestionada en la nube y la seguridad Cloud en una misma solución. Para los clientes que requieren una solución on-premise, ofrece una completa seguridad SD-WAN.

¿Cómo afecta el cloud, la pérdida de perímetro, a la seguridad de las empresas? ¿Y el teletrabajo?
La seguridad sigue siendo la principal preocupación de los CIOs. Para el 73% es su primer reto, seguido de la complejidad TI (67%) y los entornos multi-cloud (61%). El incremento de trabajadores remotos provocado por la pandemia ha añadido aún más complejidad a este escenario. Con usuarios, dispositivos y nubes extendiéndose fuera del perímetro de red tradicional, se requieren nuevas aproximaciones de seguridad para un acceso seguro y fiable sin afectar a la experiencia de usuario.

Cisco Umbrella se lanzó en 2017 y se ha convertido en el corazón de la propuesta de Cisco, ¿cómo ha evolucionado? ¿Hacia dónde va?
Cisco Umbrella unifica las funcionalidades de puerta de enlace web segura (SWG), seguridad de la capa DNS, cortafuegos y CASB en una misma plataforma integrada y cloud nativa. Construida como una arquitectura basada en micro-servicios,

"Cisco ha estado avanzando hacia el modelo SASE desde hace años, con adquisiciones clave en redes (Meraki, Viptela) y seguridad (OpenDNS, CloudLock, Duo) así como muchas innovaciones desarrolladas internamente"

Enlaces de interés...

- El trabajo a distancia: reto y oportunidad para la seguridad de las empresas
- Catalyst 8000 Edge, nueva familia de routers de Cisco para impulsar la conectividad segura en cloud

El creciente número de trabajadores remotos requiere un acceso seguro a las aplicaciones, pero también con un rendimiento óptimo

Umbrella proporciona la escalabilidad y la fiabilidad necesarias para proteger la fuerza de trabajo remota de hoy en día.

Avalada por la inteligencia frente a amenazas de Cisco Talos, el equipo de investigación no gubernamental más grande del mundo, Umbrella ha sido clasificada recientemente como la solución número 1 de la industria por su eficacia en seguridad. Con el anuncio de Cisco SD-WAN 17.2 el pasado mes de junio, Cisco Umbrella se integra con Cisco SD-WAN en una solución SASE lista para implementar.

Hace tiempo que los fabricantes de seguridad de red miraron hacia el endpoint, hace unos años hacia el mercado EDR, y más recientemente hacia el MDR. ¿Cuál es la propuesta de Cisco al respecto? Las propuestas MDR, ¿no incomodan al canal de distribución?

La propuesta MDR añade inteligencia a las estrategias de seguridad, combinando expertos, procesos y tecnología para ofrecer los mecanismos de protección y remediación más avanzados, incluyendo técnicas como threat hunting. Cisco Managed Detection and Response (MDR) combina un equipo de expertos avalados por Cisco Talos que pueden reducir el tiempo de detección y respuesta de meses a horas. El servicio aprovecha la arquitectura de seguridad integrada de Cisco para una detección de amenazas y una respuesta líder en la industria, 24x7x365, con acciones de respuesta relevante, significativa y priorizada.

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

‘El elemento humano es el gran olvidado de los planes de contingencia’

(Maite Avelino)

Rosalía Arroyo

Tiene las ideas claras y pocos pelos en la lengua. En esta entrevista Maite Avelino habla como experta, con la mucha experiencia que le da ser una colaboradora habitual de ISACA, la pasión por su trabajo y saber lo que se cuece dentro de la administración pública. Dice que el Cloud es como coger un coche de renting, que cuando algo es gratis el servicio eres tú, que querer tener un proveedor de Cloud europeo es por un mínimo de sentido común, que aún vivimos en un mundo más físico que virtual, que la formación es otra de las grandes olvidadas, que tecnología puntera en Europa hay para aburrir y que no es que falten profesionales, es que falta gente que quiera trabajar por 500 euros y que encima sea excepcional.

Empezamos la entrevista hablado de lo aprendido durante la de pandemia y la respuesta le sale al momento: “Lo que hemos aprendido es que siempre que se piensan en procedimientos de contingencia nos preocupamos de la parte técnica y se nos olvida que los sistemas los opera gente”. Dice Maite Avelino que, por mucho que tú automatices, siempre termina habiendo un equipo detrás, y el

"El problema del Cloud no es tanto la seguridad sino la legislación"

problema es que “esta vez ha fallado la gente” y añade que “el recurso humano es el más valioso y que hay que protegerlo”.

Dentro de la generalidad reconoce que sí ha habido algunas empresas que han prestado más cuidado a ese componente humano, como los grandes bancos o alguna operadora que “empezó a reservar gente por si caían los de primera fila en la batalla”. Asegura que en general “no existen planes de contingencia serios, que incluyan lo que puede pasar cuando la gente falle porque está enferma, porque no puedo acudir al centro de trabajo u otras circunstancias excepcionales” y que por eso se ha trabajado “a marchas forzadas” en el teletrabajo, un modelo que muchas empresas contemplaban de manera parcial, para casos y días concretos, “pero no era algo serio, legislado, regulado y sobre todo que también afecta a los sistemas, porque no es lo mismo acceder de vez en cuando a mirar el correo que estar ocho horas al día o más conectado a un sistema corporativo”.

Ese teletrabajo como norma y no de manera puntual requiere de unos recursos, por ejemplo de equipamiento y licencias de VPN que permitan securizar los accesos “porque ya no se trata de que alguien (normalmente un técnico de TI) se pueda conectar esporádicamente, sino que lo utilicen el 80% o 100% de la plantilla de manera constante”, dice la experta.

El teletrabajo ha sido una necesidad para la gran mayoría de las empresas. No ha calado tanto en la administración pública, y cuanto se ha hecho ha sido en su mayor parte porque la opinión pública y las necesidades excepcionales de tramitación como el caso de los ERTEs así lo precisaba, añadiendo Maite Avelino que “todavía vivimos bastante en un mundo físico, no en un mundo virtual”.

Un mundo físico que cuesta llevar a lo digital por falta de medios, y sobre todo de dinero. A la Administración Pública siempre se le ha exigido que implemente los planes sin incremento de gasto, pero la magia no existe, dice Maite Avelino añadiendo que “la seguridad es un no acabar. Algo con lo que tienes que ser muy creativo, estar al día, que requiere de una formación constante porque los malos no descansan, son muy hábiles y tienen mucho tiempo para innovar”.

"No es que falten profesionales, es que falta gente que quiera trabajar por 500 euros y encima sea excepcional"

Sobre la formación, asegura esta experta que "ahorra tiempo" cuanto has de enfrentarte a un incidente de seguridad, y apunta que son muchas las ocasiones en las que son los funcionarios quienes corren con los gastos de las certificaciones profesionales de organismo privados (ISACA, ISC2, EH, etc.)

El acuerdo con el Centro Criptológico Nacional, INAP y otras asociaciones son de gran ayuda en una formación que "es otra de las grandes olvidadas".

La formación y las certificaciones profesionales no sólo permiten hacer las cosas mejor en menos tiempo (ser más eficiente), dice Avelino, sino que es la única manera de requerir mínimo de calidad a los proveedores de las empresas que prestan servicios en ciberseguridad a la Administración, especialmente en servicios críticos como la gestión de incidentes. No obstante, las empresas, cuando van a licitar, se quejan de que esas certificaciones les cuestan dinero".

Pasión por las siglas, del CASB al SASE pasando por el BYOD. "Hace años no había tanta sigla, lo que pasa es que esto es muy comercial, muy moderno. Igual que hay pasión por las siglas en ciberseguridad la hay en cualquier cosa, y generalmente la gente cuanto menos idea tiene de lo que está hablando, más siglas emplea para ocultar su desconocimiento", asegura esta experta.

Dice también Maite Avelino que hay una tendencia a consolidar los servicios de ciberseguridad en la Administración General del Estado, algo que están liderando el Centro Criptológico Nacional y la Secretaría General de Administración Digital (SGAD), "y todo eso está muy bien. Yo les tengo mucho respeto, las herramientas están muy bien, y son gratuitas. Pero, en este caso, como son gratis, el servicio por detrás debes proporcionarlo tú".

Maite Avelino asegura haber probado muchas de esas herramientas, asegura que son buenas, pero insiste en que lo que no se gasta en equipamiento y en externalización de un producto se gasta en personal. Las herramientas del Centro Criotológico Nacional requieren que haya alguien por detrás operándolas y echándole horas, porque en automático no puedes operarlas correctamente, requieren de analistas por detrás. Y requieren de gente formada, con lo cual lo que no me estoy gastando en comprar una solución "llave en mano" lo voy a gastar en pagar a alguien que opere esa herramienta, y el problema entonces es que no hay funcionarios para operarla, o no les han formado de antemano.

El Cloud

"El cloud es como coger un coche de renting", dice Maite Avelino cuando le preguntamos cómo está viendo la adopción de la Nube tanto en la empresa como en la administración pública. "Se tienen que tener claras las necesidades para poder hacer una compra, sea de cloud o sea on-premise o sea híbrida", asegura la experta añadiendo que lo que no se hace es "un análisis de necesidades y un análisis de riesgo". El Cloud es extremadamente útil en entornos de desarrollo, pero hay un problema, "pierdes la propiedad o el control de los datos cuanto están en Cloud, y cuando son datos de pruebas de desarrollo es un riesgo asumible, cuando son datos de expedientes de gente que estás tramitando, que puedes ocasionar un caos en el Estado es un problema, sobre todo cuando a la persona que opera tus servicios en el Cloud no lo la tienes en Alcobendas, sino en California, en Bangladesh o a saber en dónde".

El problema del Cloud, continúa diciendo Maite Avelino, no es tanto la seguridad sino la legislación. ¿Qué pasa si un día el propietario del Cloud decide cerrarlo?, se pregunta. "Parece que en Europa somos muy quisquillosos con el tema de que el cloud esté en Europa o en el propio país. Esto

"La seguridad es un no acabar. Algo con lo que tienes que ser muy creativo y estar al día"

"En general no existen planes de contingencia serios, que incluyan lo que puede pasar cuando la gente falle porque está enferma, porque no puedo acudir al centro de trabajo u otras circunstancias excepcionales"

Enlaces de interés...

- Entrevistas ITDS
- Convenio entre el CCN y el INAP para formar a los empleados públicos en ciberseguridad
- Un tercio de las empresas expone servicios de red inseguros en Internet

no es por robarle cuota de negocio a Amazon o a Google, es por un mínimo de sentido común".

¿Es necesario un proveedor de Cloud europeo? "Sí, incluso a nivel nacional para ciertas cosas críticas, según además el RD 14/2019", dice Maite Avelino. Reflexiona esta experta que lo que pasa en Europa es que "hay 27 reinos de taifas que se reúnen para reunirse, para luego volver a reunirse; es burocracia, burocracia y más burocracia. Y así no hay manera".

Añade Avelino que al final nos come el terreno, "cualquiera que sea más ágil y más espabilado" y que las empresas no quieren esperar a la burocracia, quieren tener una solución llave en mano y al final se acaban yendo al Cloud americano, "y luego ya veremos las consecuencias".

Estos reinos de taifas a los que se refiere Maite Avelino no sólo impactan negativamente en que pueda haber un Cloud europeo, sino en la propia tecnología de la región. Asegura esta experta que "tecnología puntera en Europa hay para aburrir. Hay muy buenas empresas que además están mucho mejor preparadas que las grandes empresas americanas a las que estamos acostumbrados a recurrir, "pero el problema es que no hay dinero para pagarlas y para pagar a sus empleados, un empleado en USA cobra tres veces más que uno en España". No es que falten profesionales, es que falta gente que quiera trabajar por 500 euros y encima sea excepcional".

Compartir en RRSS

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.

12
NOVIEMBRE
11:00 CET

REGISTRO

Brechas de seguridad, ¿hay opciones?

Las fugas de datos no discriminan. Ahora están más de moda que nunca, no sólo porque los ciberdelincuentes siguen perfeccionando sus actividades, sino porque normativas como GDPR obligan a informar sobre ellas. Adif, Mapfre, Tesla, Honda, EasyJet... son algunas de las empresas protagonistas este año de un ciberincidente. ¿Quieres evitar ser una de ellas? ¡No te pierdas este webinar!

Arquitecturas de Seguridad, ¿qué ventajas ofrecen?

26
NOVIEMBRE
11:00 CET

Acompáñanos en este IT Webinar en el que diferentes expertos de seguridad explicarán las ventajas de contar con una plataforma unificada de seguridad capaz de orquestar diferentes elementos y automatizar las operaciones para conseguir una seguridad más coherente y flexible.

REGISTRO

#ITWEBINARS

IT Trends 2021. La TI salva el negocio

2020 ha estado marcado por la pandemia y la migración masiva al teletrabajo. La TI ha salvado el negocio, convirtiéndose en soporte vital para su continuidad. Además, asistimos a la progresiva penetración de tecnologías que están ayudando a las organizaciones a innovar y generar nuevos productos y servicios, así como modelos de negocio. ¿Qué tendencias tecnológicas dominarán 2021?

2021, ¿el año de la ciberdefensa?

Únete a este Encuentros IT Trends sobre Ciberseguridad en 2021 y descubre qué ocurre en el mundo del cibercrimen, qué tipos de ataques se están produciendo y cómo pueden afectar a tu empresa. Y sobre todo, qué nos espera en 2021.

REGISTRO

15
DICIEMBRE
11:00 CET

17
DICIEMBRE
11:00 CET

REGISTRO

‘La inteligencia artificial es imprescindible porque es lo que están utilizando los atacantes’

(José Luis Laguna, Fortinet)

Este año se celebran los 20 años de Fortinet, una compañía con una larga trayectoria en la industria. Todo este tiempo ha dado para mucho. Tras empezar en el mundo del firewall con su FortiGate, la empresa ha ido ampliando su oferta; en 2007 la compañía lanzaba su propuesta para la protección del correo electrónico. Dos años después le siguió el Web Application Firewall (WAF) y con el tiempo se han ido añadiendo más elementos al portfolio “pensando en cubrir todos los vectores de ataque y que se adapte a las necesidades del mercado”, dice José Luis Laguna, Director de Systems Engineering en Fortinet. La última evolución y lo que demandan los clientes, añade el directivo, no son sólo productos, sino también servicios, “y son los pasos que estamos dando”.

'LOS ATACANTES UTILIZAN TODO LO QUE ESTÁ A SU ALCANCE PARA SOFISTICAR SUS ATAQUES, Y SABEMOS QUE LA IA NO ES UNA EXCEPCIÓN' (FORTINET)

CLICAR PARA VER EL VÍDEO

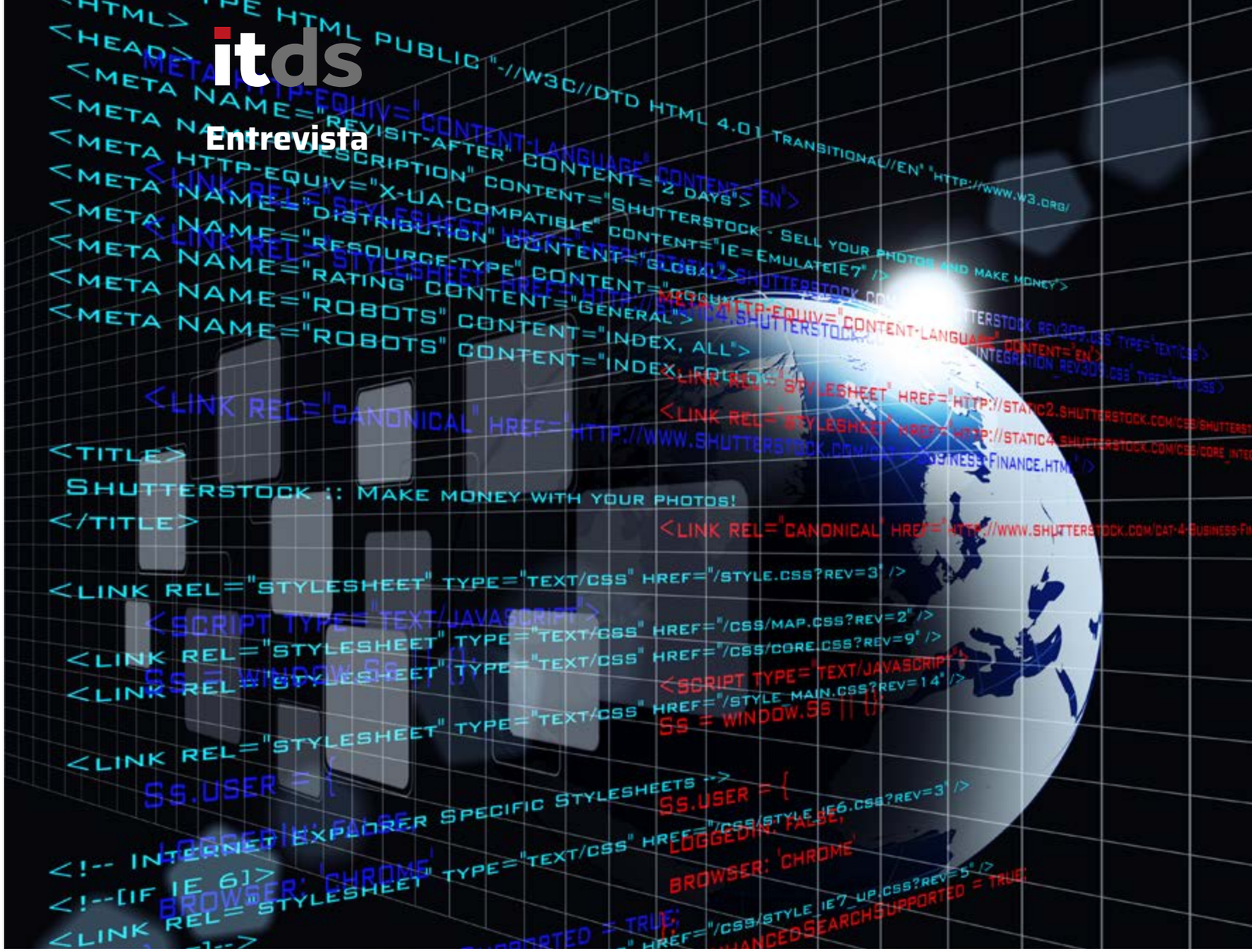
En abril de 2016, Fortinet presentó su Security Fabric, una propuesta que al principio costó entender y que se ha convertido en un elemento clave dentro de la oferta de la compañía. Para algunos era un nombre comercial, un producto de marketing, pero fue el germen de lo que después han hecho muchos de sus competidores. Nos explica José Luis Laguna que se iban incorporando elementos al portfolio y se vio la necesidad de trabajar con ellos de una manera conjunta, que si se recibe una amenaza por un vector, como el correo electrónico, y ya se ha identificado, ¿por qué no compartir esa inteligencia de amenazas, esos IoC de amenazas, con otros dispositivos de la red para hacer una protección más eficaz? Al compartir esa información "dotamos a la solución integral de mayor capacidad".

El lanzamiento de Fortinet Security Fabric llegó acompañado de un programa de partners, de alianzas, porque ya entonces tuvo claro Fortinet que la colaboración e integración entre fabricantes iba a ser necesaria para poder afrontar las amenazas, cada vez más numerosas y sofisticadas. "Y ese es el espíritu que hay detrás de ese programa de partnership, el mismo que hay detrás de la Cyber Threat Alliance (CTA)", uno de cuyos fundadores es, precisamente, Fortinet.

Inteligencia artificial en Seguridad

Tiene claro José Luis Laguna que "la inteligencia artificial hoy en día es imprescindible". Añade que no se puede proporcionar una solución eficaz si no es con la inteligencia artificial "porque es lo que están utilizando los atacantes". Insiste en que para sofisticar el malware y que tenga esa capacidad de mutación tan rápida de propagación y llegar a más tasas de infección, los ciberdelicuentes utilizan la inteligencia artificial "y nosotros tenemos que jugar en

"Yo quisiera para mí un buen partner que me ayudara a definir los puntos que hay que cubrir y, a partir de ahí, se busque la tecnología que mejor se pueda adaptar"



igualdad de condiciones. Si no lo haces, no puedes proteger de manera eficaz".

Reconoce al mismo tiempo el directivo de Fortinet que tanto se habla de ello, que muchos clientes acaban hartos de oír hablar de inteligencia artificial y machine learning. Y en parte tienen razón. Se habla de inteligencia artificial como si se pudiera ir a comprar al mercado, cuando en realidad es una tecnología que se está integrando en las soluciones, y no sólo de seguridad. Cada fabricante aplica sus propios algoritmos, más o menos buenos, y "sería prácticamente imposible" hacer una comparativa de la inteligencia artificial de los diferentes fabricantes para saber cuál es la mejor; claro que sí es cierto que al final la calidad de la inteligencia "está directamente relacionado con cuán eficaz es el producto".

Personas

Más del 60% del tráfico en internet es generado por bots, la mayoría de los datos se intercambian entre aplicaciones, ¿estamos demasiado preocupados de las personas y nos olvidamos de las máquinas? Responde José Luis Laguna diciendo que al final sabemos que el humano es el eslabón más débil en la cadena de la seguridad. Añade que por ese motivo se insiste tanto en las campañas de concienciación y de capacitación de ciberseguridad, "porque es necesario".

En todo caso y hablando de las redes de bots, dice también el directivo de Fortinet que es el comportamiento humano el que está íntimamente ligado con este problema, porque al final la botnet se compone de dispositivos que están utilizando los ciberdelincuentes para efectuar ataques, y esos dispositivos han sido capaces de tomar el control "porque quien los ha configurado, una persona, no tiene conocimiento o precauciones de lo que tenía que hacer". De forma que al final sí que vuelve a estar relacionado con el usuario, porque si no, una red de botnet no hubiera sido capaz de asumir el

"Esta crisis sanitaria ha puesto en evidencia la importancia de la digitalización de las empresas"

control de sus dispositivos para luego utilizarlo en ataques masivos. “Soy un creyente de que los planes de concienciación y capacitación en materia de ciberseguridad son imprescindibles”, asegura José Luis Laguna.

Del EPP al MDR

La mayoría, sino todos, los fabricantes originales de firewalls evolucionaron sus ofertas para llegar a securizar el endpoint. Y en el mundo del endpoint se ha pasado de las soluciones de EPP (Endpoint Protection Plataform) a los EDR (Endpoint Protection and Response) y, en la última etapa, a los MDR, o Managed Detection and Response, que añaden una capa de gestión a la detección y respuesta de amenazas. Esta capa de gestión, que ciertamente la están demandando los clientes, no es vista con buenos ojos por el canal de distribución, que mira con recelo cómo los fabricantes se quieren adentrar en lo que consideran su terreno.

“El mercado nos está demandando más servicios, más cosas as-a-service”, dice José Luis Laguna, añadiendo que “los que no seamos capaces de proporcionar este tipo de soluciones, no podremos atender las necesidades de todo este conjunto de clientes que cada vez es mayor”. Explica también el directivo que esta demanda no sólo procede de pequeñas empresas, sino de las grandes, y que la propuesta tradicional del Fortinet ha sido “la de favorecer a nuestro canal para que sean ellos los que ofrezcan servicios con nuestra tecnología. Nuestros modelos de facturación se han adaptado para que ellos puedan ser capaces de poner en marcha el servicio sin una inversión muy fuerte, y que pueden estar creciendo a medida que crecen servicios”.

Al mismo tiempo, apunta Laguna, hay empresas del canal que no pueden, no tienen capacidad, o

it whitepapers

ACCESO REMOTO SEGURO PARA SU FUERZA LABORAL A ESCALA

Las organizaciones se enfrentan a diferentes situaciones potenciales de emergencia como epidemias, inundaciones, huracanes y cortes de energía. La implementación de un plan de continuidad comercial es esencial para garantizar que la organización sea capaz de mantener la operación ante la adversidad y prepararse para posibles desastres.

"Soy un creyente de que los planes de concienciación y capacitación en materia de ciberseguridad son imprescindibles"

no tienen dimensión, para poder poner en marcha un servicio de esa magnitud, "con lo cual nos piden comercializar como servicio una propuesta, pero asumiendo nosotros esa parte del servicio también. Tenemos un modelo muy mixto".

Y con respecto a la evolución del EDR al MDR, ocurre lo mismo, "no todas las compañías del canal o del cliente final tienen un equipo de analistas especializado que esté disponible 24/7. Para muchas empresas es inviable y lo piden como servicio", dice José Luis Laguna.

Los mínimos

La respuesta no es fácil, reconoce Director de Systems Engineering en Fortinet cuando le preguntamos cuáles serían, en su opinión, los básicos que toda empresa debe tener y en qué tecnologías habría que apostar. Tira de su experiencia como CISO, que lo fue de Técnicas Reunidas durante más de diez años, para hablar de la concienciación del empleado como un must have, pero también piensa que es súper importante un buen análisis de riesgos; "esa es la recomendación que yo haría,

Es prácticamente imposible hacer una comparativa de la inteligencia artificial de los diferentes fabricantes para saber cuál es la mejor

porque es necesario poder tener una foto lo más precisa posible de en qué situación nos encontramos" para después, contando con los recursos y presupuesto que se tenga ver qué riesgos se pueden cubrir porque no es lo mismo una empresa que tenga servicios en la nube, otra que la ubicación de sus activos, esté dispersa…

"Tiene que ser un análisis de riesgo que sirva para preparar estratégicamente dónde tengo que invertir mi presupuesto para proteger de manera eficaz. Porque nos puede pasar que siguiendo la moda del mercado me compre un MDR y me haya dejado no sé cuántas otras cosas mucho más críticas sin protección".

Añade José Luis Laguna la importancia que en este punto tiene el canal: "Yo quisiera para mí un buen partner que me ayudara en esta parte de analizar el riesgo, que me ayudara a definir los puntos que hay que cubrir y a partir de ahí se busque la tecnología que mejor se pueda adaptar".

Que podemos aprender de 2020

Se va acabando a 2020, un año de pandemia de aceleración digital, de oportunidades, de cambios en la inversión. ¿Qué han aprendido las empresas de esta pandemia?

Tiene claras José Luis Laguna que durante este año hemos aprendido que "el teletrabajo está aquí para quedarse", porque nos hemos dado cuenta de que la tecnología, la capacidad de nuestras redes de telecomunicaciones "es tal que nos permite desarrollar nuestro trabajo en remoto sin ningún problema". Añade que el teletrabajo no sólo plantea mucho ahorro para las empresas, sino algunos retos.

"Aparte de esto del teletrabajo, para mí otra gran lección es que me ha quedado clarísimo que los ciber criminales no tienen ningún escrúpulo", dice Laguna recordando que durante la crisis hospitalaria han lanzado ataques que ha puesto vidas en peligro.

Por último, lo último que esta crisis sanitaria ha puesto en evidencia es "la importancia de la digitalización de las empresas"; aquellas que habían avanzado su proceso de transformación digital tuvieron menos impacto con el COVID-19 y han sido capaces de que les afecte menos, "porque la tecnología al final les ha ayudado en el negocio a salir a flote".

Añadir que la seguridad cobra un gran protagonismo gracias a una expansión digital que está en aumento.

Enlaces de interés…

- El mercado de dispositivos de seguridad registra un sólido crecimiento
- Schneider Electric y Fortinet se asocian para proteger entornos de OT

Compartir en RRSS

NUEVO INFORME

DOCUMENTO EJECUTIVO

Teletrabajo en 2020:
el futuro se hace presente

ELABORADO POR itResearch

Descarga este **documento ejecutivo** de itResearch

#ITWebinars

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Trabajo seguro desde cualquier lugar:

Adaptándonos a la "nueva normalidad"

Digital Security

Noviembre 2020

“Trabajo seguro en cualquier lugar significa pasar a políticas de seguridad centradas en las personas, de modo que la actividad empresarial pueda continuar independientemente de la ubicación”. Lo dice Jorge Ferrer Raventós, Ingeniero de soluciones OneTrust, en uno de nuestros #ITWebinars en el que no solo hemos analizado la situación del teletrabajo, sino cómo impacta en toda la empresa destacando la privacidad y monitorización de los empleados, que es el foco de OneTrust, una empresa con más de 5.000 clientes, tanto grandes cuentas como pymes, y con más de 1.500 empleados, de los que un 40% se dedican a la investigación y desarrollo.

Dice Jorge Ferrer que la pandemia global y los impactos derivados del COVID-19 sacudieron las operaciones en todo el mundo y que a medida que las organizaciones se han ido abriendo camino en los escenarios de regreso a la oficina muchas organizaciones están considerando la posibilidad de adoptar una política proactiva del trabajo seguro en cualquier lugar.

“OneTrust es la solución más utilizada para la gestión de la privacidad”, dice Jorge Ferrer, añadiendo que las organizaciones deben conocer los datos que se procesan en sus negocios, así como las leyes y reglamentos que se aplican a estos datos. Para la mayoría de las empresas hay tantos datos y tantas leyes que su gestión es difícil; OneTrust DataDiscovery y OneTrust DataGuidance son dos soluciones de la compañía que ayudan en estas tareas.

Explica el ejecutivo de OneTrust que la seguridad remota en el hogar es una extensión de las

"OneTrust es la solución más utilizada para la gestión de la privacidad"

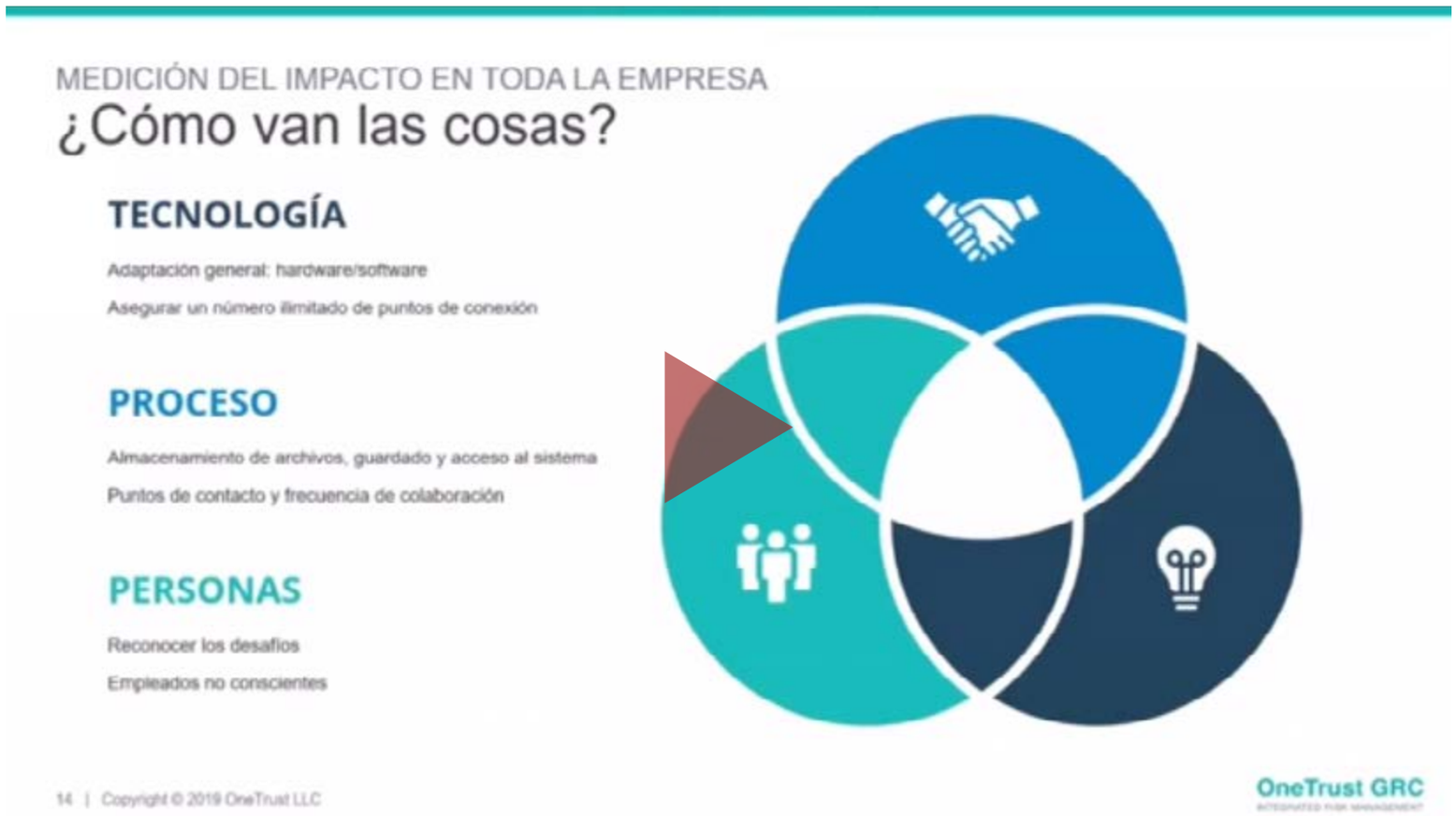
Jorge Ferrer Raventós,
Ingeniero de soluciones OneTrust

políticas de seguridad empresariales, con la diferencia de que “se tienen en cuenta todas las variables adicionales que una red doméstica añade la ecuación, como las conexiones a internet”.

Asegurando que las nuevas circunstancias en el teletrabajo deben permitir que la movilidad se adelante a la incertidumbre, asegura Jorge Ferrer durante este webinar que “el trabajo seguro en cualquier lugar consiste realmente en pasar a políticas de seguridad centradas en las personas, de modo que la actividad empresarial pueda continuar independientemente de la ubicación”.

La nueva realidad provoca que empleados y gerentes estén más abiertos a las oportunidades de trabajar desde casa, aunque hay algunas mejoras que realizar, como la gestión remota y las habilidades de colaboración. Hay tres elementos centrales que impactan en la gobernabilidad, la gestión y la seguridad en el teletrabajo, que el ejecutivo de OneTrust identifica como: la tecnología, el proceso y las personas.

En la parte de la tecnología se trata de cómo estamos habilitando a los interesados con el hardware y el software, para tener visibilidad y responder a las ciberamenazas. Hablar del proceso es hablar de los datos, del acceso, la disponibilidad, la colaboración… es decir, cuáles son los procesos, procedimientos y seguridades en torno al acceso de la información. Por último las personas, “a menudo el activo más valioso y la mayor vulnerabilidad cuando pensamos en asegurar el trabajo remoto”.



TRABAJO SEGURO DESDE CUALQUIER LUGAR **CLICAR PARA VER EL VÍDEO**

Exceso de trabajo, fatiga, incertidumbre o distracciones son algunas de las implicaciones negativas que acompañan al teletrabajo. En lo que respecta a la privacidad y monitorización de los empleados, hay empresas que lo llevan al extremo, instalado un software remoto que toma fotografías de lo que hacen los empleados cada 20 segundos, y otras que se han limitado a una videollamada diaria, o ni eso. “Para aquellos que han

Hay que tener en cuenta la ubicación de los datos, saber en todo momento qué empleados tienen acceso a qué información y desde dónde

itds
Webinar OneTrust

ONETRUST GRC, GESTIÓN INTEGRAL DE RIESGOS

OneTrust GRC (Governance, Risk and Compliance) es una plataforma de gestión integral de riegos que ofrece una visión completa y medible de los riesgos de la empresa, proporcionando una perspectiva clara a la dirección y agilizando la ejecución de las tareas rutinarias.

La seguridad remota en el hogar es una extensión de las políticas de seguridad empresariales

implementado medidas severas, tienen que pensar si realmente están cumpliendo con las leyes de privacidad", dice Jorge Ferrer añadiendo que hay que confiar en los empleados, que a menudo además están haciendo uso de sus dispositivos para hacer frente al teletrabajo.

Consideraciones

Algunos de los elementos a tener en cuenta en modelos de teletrabajo son: la seguridad de los dispositivos, gobernanza de tecnologías de la información, ubicación de los datos, herramientas de comunicación y formación para la concienciación.

Enlaces de interés...

- INCIBE y Google forman a las empresas sobre cómo implementar el teletrabajo sin riesgos
- Más del 90% de las empresas aumentará sus inversiones para proteger el trabajo a distancia
- Consejos para evitar las ciberamenazas ligadas al teletrabajo

Respecto a la seguridad de los dispositivos, se deben tener en cuenta cuáles son las configuraciones de hardware y el uso de los dispositivos en teletrabajo, definiendo políticas de seguridad. Hay que tener en cuenta la ubicación de los datos, saber en todo momento qué empleados tienen acceso a qué información y desde dónde. En lo relativo a las herramientas de comunicación, ¿sabemos cuántas se están utilizando en la organización? ¿sabemos a ciencia cierta que los datos están seguros en esas herramientas de videoconferencia? Y finalmente, la parte formación para la concienciación: ¿cómo se está educando a la fuerza laboral frente a estos cambios? Hay que estar seguros, dice Jorge Ferrer, que se dispone de mecanismos para rastrear a quienes no han completado los cursos de concienciación.

La solución OneTrust GRC (Governance, Risk and Compliance) es una suite de gestión de riesgos que permite a las empresas identificar, mitigar, monitorizar e informar de los riegos empresariales a través de diferentes herramientas con las que las empresas pueden analizar el riesgo, reforzar la gobernanza, mejorar la visibilidad y escalar el cumplimiento normativo.

Compartir en RRSS

it User
TECH & BUSINESS

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

El reto de compartir archivos de forma segura

Mucho se ha hablado de la conectividad y seguridad de los accesos como algunos de los principales retos que ha generado un teletrabajo adoptado casi de manera generalizada en apenas unas semanas fruto de la pandemia sanitaria. De las seis etapas del ciclo de vida de los datos (creación, almacenamiento, uso, intercambio, archivo y eliminación), la compartición de los mismos se ha acelerado con la adopción del cloud y, posteriormente, la adopción masiva del teletrabajo.

Saber quién se conecta a qué y desde dónde se ha convertido en una necesidad que ha impulsado modelos como el de Zero Trust, no confiar en nada ni en nadie. El uso compartido de archivos empezó a aumentar a medida que las empresas adoptaban la nube y se ha acelerado con el trabajo remoto. Los servicios de intercambio de archivos basados en la nube proporcionan un acceso fácil y conveniente a la información en cualquier momento y desde cualquier lugar, pero las empresas que tarden en adoptar políticas de intercambio de archivos pueden encontrarse con que sus empleados podrían hacer uso de cuentas personales y servicios gratuitos que, diseñados para el mercado de consumo, podrían poner a su empresa en alto riesgo de una violación de seguridad.

Actualmente el 39% de los datos empresariales que se suben a la nube se utilizan en servicios de intercambio de archivos, según datos de Varonis, que apunta además que una empresa promedio comparte archivos con más de 800 dominios online diferentes, incluyendo socios y proveedores. Por otra parte, aproximadamente el 70% de los archivos compartidos se distribuyen solo a los usuarios internos de una organización y, curiosamente, cerca del 60% de los archivos cargados en un servicio de intercambio de archivos nunca se comparten con otras personas sino que se utilizan como copia de seguridad.

> Para lograr la máxima productividad, las personas deben poder acceder y compartir archivos sin tener que preocuparse por dónde residen

Las organizaciones invierten cada vez más recurso en ciberseguridad, sin embargo, las brechas de datos y otros incidentes de seguridad continúan aumentando tanto en número como en tamaño. Sin las medidas de seguridad adecuadas, los beneficios de compartir archivos pueden verse

Los responsables de TI se enfrentan a la necesidad de recuperar la visibilidad y el control sobre cómo y dónde se accede y comparten los datos empresarial, y por quién

superados significativamente por la posibilidad de exponer los datos confidenciales de su empresa a nuevas amenazas de seguridad.

Saber qué datos se tienen, cómo son de sensibles, dónde se almacenan y quién tiene acceso a ellos es fundamental. Diferentes estudios apuntan a que la etapa de almacenamiento de datos resultó ser la más desafiante para garantizar la protección de los mismos. De hecho, un 24% de las empresas descubren datos fuera de ubicaciones seguras. Un informe de la compañía Netwrix recoge que el 54% de las organizaciones no siguen las mejores prácticas de seguridad a la hora de revisar los derechos de acceso de los usuarios a los datos de forma regular; un 30% de los administradores de sistemas han otorgado acceso directo a datos sensibles y regulados basándose únicamente en una solicitud del usuario; el 46% de las organizaciones que tuvieron un incidente de intercambio de datos no autorizado están sujetas al GDPR, sin embargo, un 38% de ellos confía en que los empleados no evitan los controles de TI para compartir datos; el 7% de las organizaciones tuvieron incidentes de seguridad durante la etapa de archivo de datos, pero el 58% de ellos notaron que los datos estaban comprometidos.

De manera más específica, cuando se trata de compartir datos o archivos, el estudio de Netwrix dice que el 54% de las organizaciones confían en que sus empleados no comparten datos mediante ningún medio de comunicación desconocido para el equipo de TI. Desafortunadamente, la mayoría de ellos no puede probarlo, ya que un 29% no rastrea el intercambio de datos de los empleados, y otro 25% solo tiene procesos manuales, propensos a generar errores en el rastreo. A pesar de que las regulaciones de privacidad modernas requieren que las empresas rastreen la huella de los datos personales que recopilan, el 33% de las organizaciones sujetas al GDPR no hacen un seguimiento del intercambio de datos.

Otro estudio, en esta ocasión de Elastica, que analizó 100 millones de archivos compartidos en las principales aplicaciones de nube pública, mostró que “los datos empresariales confidenciales están abandonando las redes de la empresa

it whitepapers

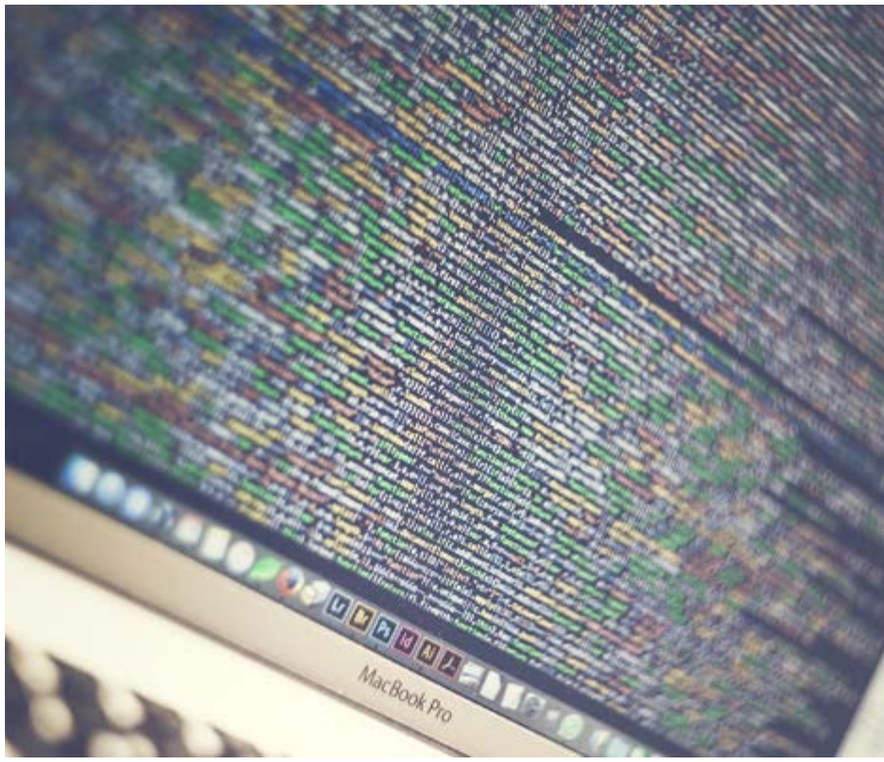
PRINCIPALES REQUISITOS PARA EL INTERCAMBIO SEGURO DE ARCHIVOS EMPRESARIALES

Los empleados dependen de los datos para ser productivos. Descubre en este documento qué necesitas para permitir el acceso a la información desde cualquier lugar y dispositivo sin exponer a su organización a riesgos.

Hay que encontrar un equilibrio para mantener los datos lo más seguros posible donde sea y como sea que se utilicen, y garantizar la mayor libertad permitida para cada usuario en cada escenario

a través de servicios de intercambio de archivos basados en la web a un ritmo asombroso", dice el informe. Según Elastica, los empleados almacenan un promedio de 2.037 archivos en la nube. El 20% de esos archivos que fueron "ampliamente compartidos" a través de servicios de intercambio de archivos incluían algún tipo de dato regulado.

Según la encuesta de Elastica, el 80% de los incidentes de riesgo por compartir archivos fueron accidentales, es decir, los empleados que compartieron archivos de manera inadecuada lo hicieron sin ninguna intención maliciosa. Sí que se detectó una actividad malintencionada en el 12% de los incidentes. En todo caso, y según concluía Elastica en su informe, ya sean malintencionados o involuntarios, los riesgos planteados por cualquiera de estos incidentes de intercambio de archivos tienen consecuencias potencialmente catastróficas para las empresas, en particular aquellas que manejan grandes cantidades de datos sensibles o aquellas sujetas a regulaciones de seguridad de datos.



Principal preocupación de seguridad SaaS

Un informe publicado a mediados de este año por Enea y Cybersecurity Insiders ponía de manifiesto que los servicios de transferencia y almacenamiento de archivos se han convertido en la princi-

pal preocupación de seguridad de SaaS entre los profesionales de la seguridad. Como decíamos, la cantidad de empleados que trabajan desde casa u otras ubicaciones remotas se ha disparado y este cambio masivo ha llevado a un aumento en el uso de aplicaciones y servicios cloud, así como comportamientos más arriesgados.

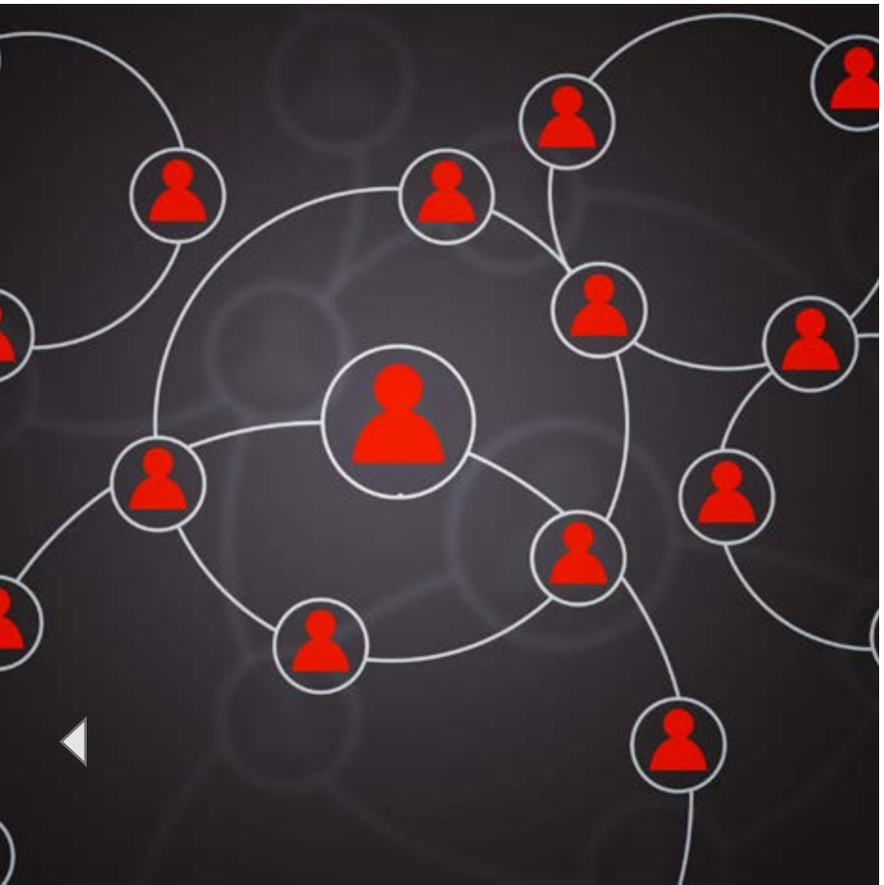
Según el informe, el 72% de los responsables de seguridad encuestados mencionaron las aplicaciones de transferencia y alojamiento de archivos como una de las principales preocupaciones, seguidos del correo electrónico en la nube, la mensajería instantánea, la comunicación y la colaboración, las videoconferencias y la gestión de proyectos.

Riesgos relacionados con el intercambio de archivos

• Liberación de datos sensibles. Uno de los riesgos más graves del software de intercambio de archivos es que los datos confidenciales pueden quedar expuestos, ya sea de forma intencionada o no, si los empleados no son cuidadosos y no se aplican las políticas adecuadas. Una vez que una parte no autorizada obtiene acceso a su servicio de intercambio de archivos, es difícil discernir a qué accedió y qué tan lejos se ha extendido su información privada.

• Cibertaques. En ocasiones los programas de intercambio de archivos requieren que se omita el firewalls para cargar o descargar archivos, lo que puede ser aprovechado por los atacantes para realizar denegaciones de servicio distribuidas, ataques man-in-the-middle y otros contra el sistema.

Instalación de software malicioso. Si un empleado abre un archivo de riesgo que se colocó en su servicio de intercambio de archivos, puede descargar e introducir malware sin darse cuenta, como virus, software espía, gusanos o caballos de Troya, comprometiendo no solo su equipo, sino toda la red.



Intercambiar archivos a través de cuentas de correo personal o servicios pensados para los consumidores no cumplen con los estándares de seguridad

En términos de amenazas relacionadas con SaaS, el 77% de las empresas están preocupadas por la infección de malware de los dispositivos conectados, así como por la pérdida y el robo de datos, el robo de credenciales y el compromiso de la cuenta, las violaciones de datos en la nube de terceros y las violaciones de las redes empresariales a través de la nube.

Intercambio, una necesidad

Por más que genere un riesgo, lo cierto es que el intercambio de archivos es una necesidad para las empresas. Los empleados y socios comerciales se vuelven cada vez más globalizados y requieren acceso a documentos electrónicos para aumentar la productividad y la colaboración. Lo que queda es tomar las medidas adecuadas para lograr la segu-

ridad del intercambio de archivos, empezando por la formación y concienciación de los empleados sobre el riesgo de compartir archivos, sobre todo a espaldas de los responsables de IT. Intercambiar archivos a través de cuentas de correo personal o servicios pensados para los consumidores no cumplen con los estándares de seguridad y pueden estar fuera de los controles de seguridad existentes de la empresa.

Como hemos visto, esa formación y concienciación pueden verse superadas por accidentes y conductas malintencionadas, por lo tanto se hace necesaria la implementación de una política formal de intercambio de archivos que sea específica sobre el uso de todos los métodos de intercambio de archivos, incluidos los que están basados en la nube y entre las aplicaciones de sincronización y uso compartido de archivos. Fundamental es que el departamento de TI tenga una visibilidad completa de todas las aplicaciones que utilizan sus empleados para compartir archivos así como el poder administrar y controlar el acceso de los usuarios a los datos confidenciales de la empresa.

> Los servicios de transferencia y almacenamiento de archivos se han convertido en la principal preocupación de seguridad de SaaS entre los profesionales de la seguridad

Beneficios y áreas de actuación

La seguridad del intercambio de archivos requiere invertir en una solución de protección de datos que proteja contra la pérdida y el robo de datos

Cómo compartir archivos de forma segura

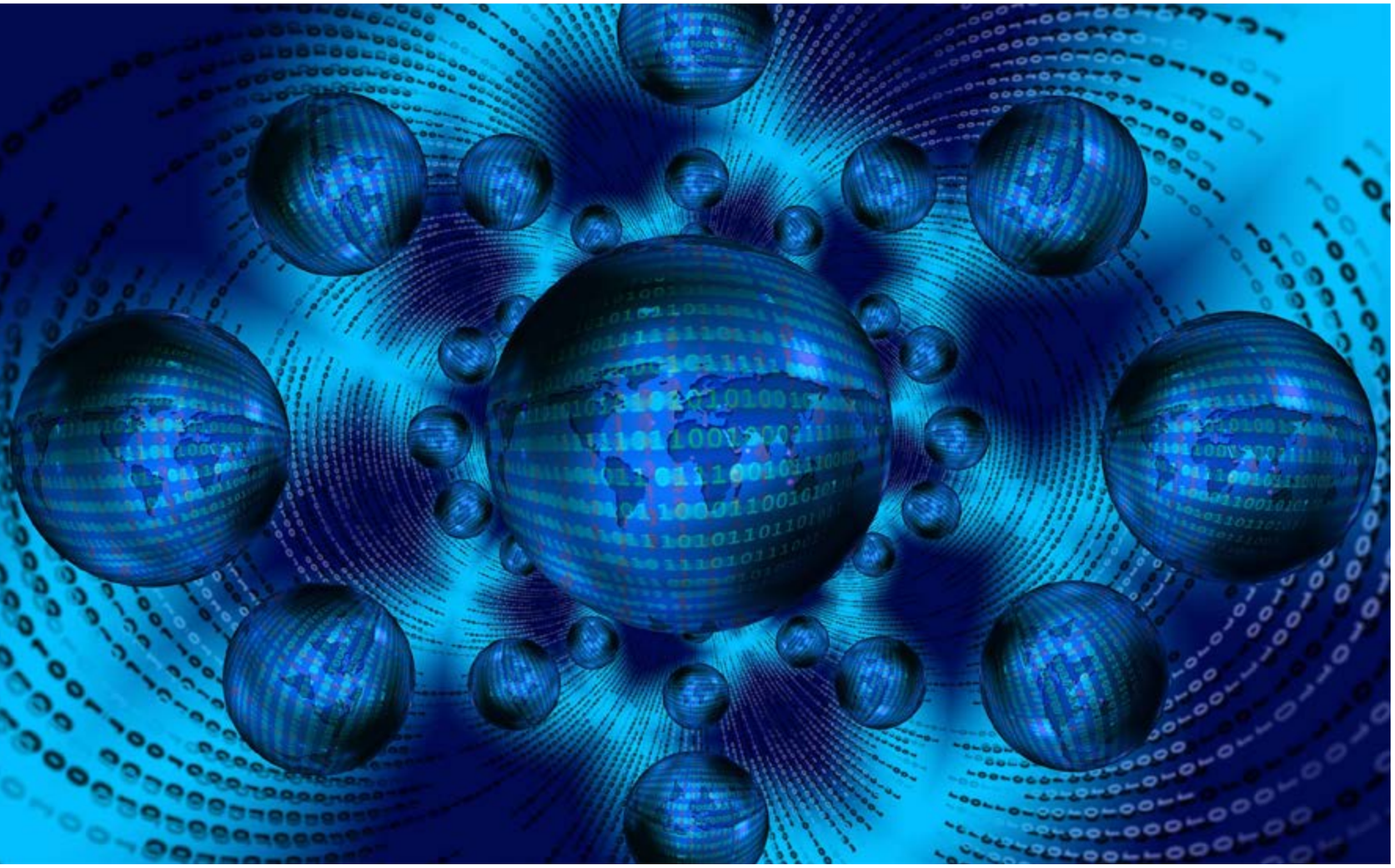
Algunos consejos para el necesario intercambio de activo que requieren los negocios de hoy pero con la seguridad en mente:

- **No ignore el problema.** En lugar de ignorar la protección de datos, conviértalo en una prioridad y busque un servicio que permita a los usuarios enviar y recibir archivos, de manera segura y controlada.
- **Escoja un sistema de nivel empresarial.** Los servicios de intercambio de archivos pensados para el mercado de consumo pueden exponerle a fugas de datos y otras amenazas de seguridad, además de dificultar tareas de cumplimiento. Se hace necesario un servicio que ofrezca visibilidad y controles de seguridad adecuados.
- **Formación y concienciación.** Los empleados deben comprender la sensibilidad de los diferentes tipos de información y los riesgos asociados con el mal manejo de datos confidenciales. Deben tener una comprensión clara de lo que no pueden compartir fuera del negocio y que deben utilizar el servicio que ha contratado.
- **Facilidad de uso.** Escoger una solución o servicio fácil de utilizar e intuitivo garantiza su uso por parte de los empleados.

como consecuencia de ese intercambio de archivos mediante una combinación de control de acceso, control de aplicaciones, control de terminales, dispositivos de seguridad de red y otras medidas proactivas que evitan de manera efectiva el intercambio de información confidencial de la empresa con aplicaciones, terminales y terminales no autorizados.

Los beneficios de adoptar una solución para la seguridad del intercambio de archivos incluyen: Supervisión y visibilidad continua de todas las interacciones de datos con aplicaciones de almacenamiento web y en la nube; control granular de movimiento de archivos basado en eventos del navegador y del sistema operativo que involucran aplicaciones web como SharePoint, Dropbox y Google Apps; Clasificación automática y protección basada en políticas de los datos descargados de aplicaciones web; Registros de eventos forenses para generar alertas, informes y creación de políticas de manera efectiva; Cifrado automático de datos sensibles antes de la salida

Las áreas de actuación que deben abordarse para satisfacer al mismo tiempo las necesidades de colaboración e intercambio de archivos con los requisitos de seguridad y control de TI pasan por la autenticación, control de acceso y seguridad de dispositivos, así como por contemplar diferentes opciones de almacenamiento para satisfacer diversas necesidades de soberanía de datos, cumplimiento, rendimiento y coste. No hay que olvidar



El 80% de los incidentes de riesgo por compartir archivos fueron accidentales, es decir, los empleados que compartieron archivos de manera inadecuada lo hicieron sin ninguna intención maliciosa

la integración con la infraestructura existente así como el soporte para espacios de trabajo de próxima generación para que las personas puedan trabajar y colaborar de manera productiva.

La movilidad y el cloud fueron el principio del fin de un perímetro de seguridad que se desdibuja a pasos agigantados. Los responsables de TI se enfrentan a la necesidad de recuperar la visibilidad y el control sobre cómo y dónde se accede y comparten los datos empresariales, y por quién. Y al hacerlo, no deben limitar la productividad, por lo que deben lograr el equilibrio adecuado de mantener los datos lo más seguros posible donde sea y como sea que se utilicen, al tiempo que garantiza la mayor libertad permitida para cada usuario en cada escenario.

Dado que más personas acceden a la información empresarial desde cualquier lugar y desde cualquier dispositivo, la autenticación y la autorización se vuelven más críticas, lo que significa que TI debe poder definir políticas sólidas de autenticación y autorización sobre quién puede acceder a qué y en qué escenarios. Este “quién” no sólo debe contemplar a los empleados, sino a los socios, proveedores, contratistas…, lo que significa contar con un servicio completo de intercambio y sincronización de archivos para la empresa que contemple

Cerca del 60% de los archivos cargados en un servicio de intercambio de archivos nunca se comparten con otras personas, sino que se utilizan como copia de seguridad

Enlaces de interés...

- El 37% de los teletrabajadores no tiene restricciones de seguridad
- Mapeo y gestión de riesgos de terceros

la capacidad de acceder y compartir archivos de forma segura con cualquier persona y en cualquier lugar mediante políticas granulares y capacidades que permitan restringir el número de descargas o el acceso según la ubicación de la red.

La necesidad de visibilidad completa del acceso a archivos, la sincronización y la actividad de uso compartido también es necesaria para mantener el compliance, por lo que una solución o servicio de intercambio de archivos debe contar con capacidades de rastrear, registrar e informar sobre el acceso a archivos de los usuarios, sincronizar y compartir la actividad, incluida la fecha, tipo, lugar y dirección de red de cada evento de usuario.

Además de la falta de seguridad, otro inconveniente de las cuentas personales para compartir archivos a través de internet es su incapacidad para acceder a los datos o integrarse con los servicios e infraestructura de backend, como los recursos compartidos de red existentes, Microsoft SharePoint, SharePoint Online, OneDrive para empresas o sistemas de administración de contenido empresarial (ECM). Para lograr la máxima productividad, las personas deben poder acceder y compartir archivos sin tener que preocuparse por dónde residen.

Como decíamos, sin la experiencia intuitiva que ofrecen los servicios personales de intercambio de archivos, es probable que los empleados no adopten la opción empresarial a pesar de tener requisitos que van mucho más allá del alcance de una simple cuenta de consumidor, como la capacidad de acceder y compartir archivos que residen en cualquier lugar del entorno empresarial, colaborar a través de redes corporativas y mejorar la productividad. Por ejemplo, un editor de contenido integrado permite a las personas crear, revisar y editar documentos de Microsoft Office y realizar anotaciones en archivos PDF de Adobe.

Contar con un servicio o solución de intercambio y sincronización de archivos diseñada para la empresa, simple de utilizar garantiza

La adopción de una alternativa empresarial autorizada, segura y fácil de utilizar, que permita un control de acceso granular, limita el riesgo del intercambio de archivos, algo por otra parte cada vez más necesario en un mundo descentralizado, de trabajo remoto y basado en cloud.

Compartir en RRSS

it Reseller
TECH&CONSULTING
nº 61
NOVIEMBRE 2020
El segmento enterprise agita el negocio TI
it Reseller
TECH&CONSULTING
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 Ejecutivo en la Nueva Sociedad Digital: ¿evoluciona o no?

Compartir en RRSS

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

Como hemos venido diciendo, y 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 18 que nos ha dado ya dos siglos y medio de un gran avance de la humanidad.

Al Poder Ejecutivo se le asigna, como su nombre indica la ejecución y desarrollo de un programa de Gobierno del Estado durante un período, el más común 4 años en la mayoría de las democracias, que conforme al Programa de Gobierno sometido a votación por los ganadores de las elecciones de las llamadas elecciones generales.

El Poder Ejecutivo es el único que concentra el poder prácticamente en una persona, que tiene la potestad de nombrar libremente a sus colaboradores, llámense ministros, Directores Generales, consejeros, asesores… que disponen para desarrollar sus funciones del ejército de funcionarios públicos, personal profesional y no políticos, que sin violar la leyes vigentes deben cumplir las órdenes del Poder Ejecutivo Político.

En algunos estados descentralizados, sean con modelos federales u otros modelos regionales, una limitada y pequeña parte del Poder Ejecutivo se comparten con los gobiernos regionales que ejecutan y desarrollan un programa de gobierno en el ámbito de su región y con las limitaciones establecidas en su Constitución.

El Sistema de Gobierno Municipal, también podemos considerarlo como parte del Poder Ejecutivo, puesto que su función es ejecutar y desarrollar el

Está claro que el Poder Ejecutivo necesita evolucionar digitalmente con urgencia, no solo en estos aspectos sino en muchos otros más que no son menos importantes

programa municipal en un ámbito más pequeño y cercano a los ciudadanos.

Vamos a empezar por este último, el Gobierno Municipal ¿ha evolucionado con el avance tecnológico y digital para realizar sus tareas de manera más acorde a las necesidades de los Ciudadanos Digitales?

En algunos aspectos sí que hemos visto avances como el mal llamada Atención Digital Municipal al ciudadano que se ha concentrado en facilitar el cobro de impuestos por vía digital, facilitar la obtención de algún certificado o documentos por vía digital y poco más. Todo esto con tecnología de principios del siglo XXI y con una sensación de que se ha creado una nueva barrera, esta vez al Ciudadano Digital, con servicios que se han quedado obsoletos a la misma velocidad que la digitalización ha avanzado en la sociedad.

De facilitar la participación de los Ciudadanos Digitales en la decisiones de los procesos de gestión en el ámbito municipal, nada de nada

En el ámbito Municipal no se han aprovechado las facilidades que han traído las nuevas tecnologías digitales para facilitar al Ciudadano Digital una información transparente y en tiempo real del funcionamiento, gestión y utilización de los recursos por parte de los gestores del poder ejecutivo municipal.

Existen algunos sitios web obsoletos ya, que contienen algo de la información, de difícil uso y aún mayor complejidad de acceso. Parecería que más que facilitar están hechos para entorpecer y disuadir al Ciudadano Digital y mantenerlo en el mismo estado de desinformación previo a la era de la Sociedad Digital.

El Ciudadano Digital de la tercera década del siglo XXI tiene derecho a recibir toda esta información en cualquier tipo de dispositivo digital, de manera simple y clara durante las 24 horas de cada día. Cualquier situación inferior a esta es absolutamente insuficiente.

De facilitar la participación de los Ciudadanos Digitales en la decisiones de los procesos de gestión en el ámbito municipal, nada de nada. Si no se facilita información, cómo podemos pedir los Ciudadanos Digitales que como mínimo tengan a bien los electos compartir su poder con ciudadanos modernos.

En los Estados descentralizados, sean de modelos regionales, autonómicos, federales, plurinacionales o variaciones de estos, nos encontramos con un nivel intermedio de gobierno con su correspondiente poder ejecutivo.

La situación respecto a la evolución digital del poder ejecutivo en este nivel intermedio de gobier-

nos, con sus limitaciones correspondientes, es muy similar, si no igual, o, incluso peor, que las que nos estamos encontrando en los gobiernos municipales.

Aquí, además, no podemos aceptar la excusa de que estos gobiernos son mucho más grandes y más complejo, excusa utilizada en los siglos pasados para una mayor opacidad, falta de comunicación y participación de los ciudadanos.

Esta excusa es inaceptable para los Ciudadanos Digitales que saben que las nuevas tecnologías hacen que los procesos sean mucho menos sensibles al tamaño de datos a manejar y gestionar, que precisamente el tamaño de los datos es proporcionalmente inverso a los recursos digitales necesarios para su proceso.

No hemos visto señales iniciales de evolución digital del Poder Ejecutivo. Ni información, ni comunicación ni participación digital son elementos que al final de esta segunda década del siglo XXI tengan en cuenta las necesidades de los Ciudadanos Digitales

En vez de poner inconvenientes y perder el tiempo en mantener modelos obsoletos cada vez más ineficaces, estos gobiernos medianos con limitación de funciones y mayor cercanía a los ciudadanos podría ser el entorno ideal para desarrollar un nuevo modelo de poder ejecutivo digital más transparente, efectivo, eficaz y eficiente aprovechando los grandes avances de las tecnologías digitales de información y participación disponibles ya. Con visión, futro de que estas tecnologías avanzan cada vez más de prisa, hay que proyectar para el futuro y no solo para el presente.

Enlaces de interés...

- Separación de Poderes en los sistemas democráticos modernos
- Poder Ejecutivo en España

Pero claro, es el Poder Ejecutivo del Estado el que encarna este pilar fundamental del sistema democrático desde hace ya varios siglos, responsable de la gestión de todos los recursos, bienes, ciudadanos, que guía el devenir de la Nación de acuerdo a la voluntad expresada en la elecciones generales que normalmente se realizan cada 4, 5 o incluso más años en diferentes países.

No hemos visto ni siquiera señales iniciales de evolución digital del Poder Ejecutivo. Ni información, ni comunicación ni participación digital son elementos que al final de esta segunda década del siglo XXI tengan en cuenta las necesidades de los Ciudadanos Digitales, y llevamos perdido ya el 20% de este siglo.

La circunstancia de que el poder Ejecutivo es el único de los 3 que recae en una única persona, el Presidente, podría hacernos pensar que hacer evolucionar digitalmente al poder ejecutivo podría ser más fácil, ya que las decisiones para avanzar en ese sentido recaen conceptualmente en una sola persona, que se supone que es la más apta en todo el Estado para ejercer este poder, no solo en la gestión del presente, sino, más importante aún, para decidir sobre el camino que habrá que seguir para tener un futuro más acorde a la realidad de los cambios tecnológicos que ocurren a la velocidad de la luz.

Lamentablemente al final de la segunda década del siglo XXI el poder ejecutivo en la mayoría de naciones con sistema democrático moderno está enfrascado en discusiones obsoletas del siglo XX o, peor aún, del siglo XIX, sin entender o sin querer entender que la civilización humana ya ha dado un salto tecnológico en la que los grandes problemas existenciales de los siglos anteriores ya no tienen sentido.

Está claro que el Poder Ejecutivo necesita evolucionar digitalmente con urgencia, no solo en estos 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.

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos itUser

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓNDigital

Con la colaboración de: brother LRS OUTPUT MANAGEMENT

MÀRIUS ALBERT GÓMEZ

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

Digitalización, **datos,** algoritmos **y otras hierbas**

Hace ya unos años, en un evento del sector TIC en Madrid, regalé un libro de D. Hoftatder (Gödel-Escher-Bach) después de mi ponencia al asistente que descubrió que estaba jugando recursivamente con los títulos de las slides de la presentación y de forma implícita… detalle imperceptible por un asistente en modo "escucha pasiva". Ese día, recuerdo que cuando me paré con el taxi en una librería para comprarlo, el taxista me preguntó muy educadamente respecto lo que me proponía hacer. Mi respuesta fue que participar en un evento de Digitalización (DES) y dar una pequeña ponencia. Su respuesta, para mi asombro, fue que él entendía pues que me dedicaba a cómo mejorar la sociedad con la tecnología. Qué mejor entendimiento mutuo, ¿no?

Compartir en RRSS

Avancemos, pues el espacio y el tiempo de esta columna teóricamente podría ser infinitamente indivisible, de forma que no alcanzaríamos nunca el final. En torno a la digitalización, leía recientemente en la prestigiosa HBR (Harvard Business Review) varios artículos respecto a cómo la IA está dando forma a nuestro futuro, así como opiniones concretas al respecto de OpenAI en las también prestigiosas Wired o Bloomberg. Más allá del debate creciente en torno la IA, resulta innegable reconocer que dos de los ingredientes básicos que forman parte de la receta de la Transformación Digital que estamos impulsando son datos y algoritmos (algoritmos avanzados de IA).

Unos algoritmos que actualmente ya pueden superar al humano en el tratamiento masivo de un volumen de datos que como sociedad generamos rondando probablemente decenas de Zettabytes (estructurados y no estructurados, en las redes y en los sistemas de información), y todo ello para una pretendida generación de nueva información y conocimiento en el contexto de Digitalización.

Este hecho me hizo recordar la tesis de L. Floridi, según la cual, los algoritmos podrían ser entendidos en este sentido como los auténticos nativos digitales, así como nosotros entendidos como organismos informacionales que se relacionan de forma creciente en la infoesfera. En este rol, actuamos de forma intensiva en la creación de nuevos esquemas interpretativos, sin pretender sustituir la acción computacional de algoritmo y dato masivo. En este entendimiento, nuestra contribución resulta clave pues en la aplicación de los criterios del diseño y evaluación de la actuación, y si no nos la cuestionamos, podríamos llegar a ser parte del

Debemos recordar que digitalizar comporta intrínsecamente un objetivo concreto de negocio o de impacto sobre la economía productiva, social y cómo no, intelectual

propio sistema axiomático de Gödel substituible a su vez por un Algoritmo(¿?).

Pero digitalizar comporta comprender y aceptar que todos los esquemas que diseñamos con el uso de la tecnología, afectan la infoesfera y la propia bioesfera que conceptualmente incluye la misma. Que dichos esquemas, sus decisiones y resultados, afectan finalmente la vida de las personas, y que por tanto resulta imprescindible e inherente contemplar una visión ética y humanista aplicada en la tecnología. Pero no sólo eso, a su vez debemos recordar que digitalizar comporta intrínsecamente un objetivo concreto de negocio o de impacto sobre la economía productiva, social y cómo no, intelectual. ¿Qué otras hierbas requerimos pues en dicho proceso para superar el reto que se plantea?

Al igual que Gödel parece que usó matemáticas para probar que las matemáticas no podían probar todas las matemáticas, extienda el lector dicha comprensión a la tecnología. Aceptar este hecho dentro de un pretendido sistema deductivo, comporta aceptar los límites de la computación/tecnológicos y superarlos siendo capaz de integrar pragmáticamente nuevos puntos de vista. Así mi respuesta al señor taxista fue que me dedico a intentar entender la digitalización desde la tecnología, pero pretendiendo nuevas perspectivas que acojo desde la ética y el humanismo, desde la ciencia y lo social, desde la lógica y la creatividad…y, por qué no, desde la música y el arte, y todo ello siempre con humildad profesional y organizativa (Management: The Human Dimension, Global Peter Drucker Forum).

Para terminar, un reto. El primer lector que me envié un mensaje de correo a mi cuenta de LinkedIn identificando una de las varias famosas paradojas matemáticas implícitas en las columnas que he escrito hasta la fecha, recibirá un ejemplar del libro “El mito del algoritmo: Cuentos y cuentas de la Inteligencia Artificial” de Richard Benjamins e Idoia Salazar García. Y que conste que no tengo derechos de autor ni de colaboración de ningún tipo, pero sí curiosidad por conocer lectores “de escucha no pasiva” de artículos.

Enlaces de interés...

- Luciano Floridi
- OdiseIA

Debemos recordar que digitalizar comporta intrínsecamente un objetivo concreto de negocio o de impacto sobre la economía productiva, social y cómo no, intelectual

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el Centro de Recursos itUser

Tecnología para tu Empresa

Con la colaboración de:

NFON Cloud Telephone System