it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Enero 2020 - nº 26

La seguridad como servicio no cala en la administración pública

“Entrégame tu tráfico y yo me encargo de limpiártelo en la nube”

El Ransomware gana protagonismos gracias a GDPR

Especial IT Trends. 2020, nuevos pasos en el viaje digital

Samsung Knox, la seguridad de la movilidad a tu alcance

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

¿Qué preocupa a los CISO?

Indudables son las ventajas de la transformación digital, e indudable la complejidad que aporta a los entornos de TI. 2020 llega lleno de retos mientras los responsables de ciberseguridad de las empresas miran con preocupación la falta de personal. Una escasez que por el momento sólo puede afrontarse con automatización.

Decía un estudio reciente que los CISO están gastando la mayor parte de sus presupuestos en capital humano después de concluir que incluso las mejores herramientas aún no abordan suficientemente sus problemas más apremiantes de seguridad, especialmente cierto con las amenazas recientemente surgidas. Cuando se trata de la nube saber escoger las herramientas y socios adecuados para apoyar tanto la migración como la seguridad de la misma es vital. Les preocupa especialmente a los responsables de seguridad mantener la visibilidad de sus activos y evitar configuraciones erróneas que lleven a una brecha de seguridad.

Pero no es lo único que preocupa a los CISO, que quieren comprender los flujos de datos dentro de su organización y buscan las mejores herramientas de prevención de pérdida de datos (DLP) y de control de identidades y accesos colocando el centro de atención en el dato y quién accede a él, cuándo, desde dónde y desde qué dispositivos y con qué nivel de permiso.

Y es que mientras que los ciberdelincuentes persiguen los datos de las empresas con ahínco y perseverancia, comprendiendo la enorme importancia de los mismos, muchas empresas han tenido que hacer frente a la GDPR para darse cuenta de lo que los malos saben desde hace años. Los datos son el activo más importante de las empresas.

Este año estará de moda hablar de la seguridad de los contenedores, de los microservicios, del Edge o del cifrado cuántico mientras la mayoría de los CISO seguirán haciendo frente a aspectos mucho más básicos de la seguridad, como la gestión de las vulnerabilidades, cómo hacer que sus empleados no se empeñen en descargar malware, cómo mejorara sus capacidades de detección o cómo recuperarse de un incidente lo más rápidamente posible. La automatización será de gran ayuda.

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

itds

Sumario

En Portada

La seguridad como servicio no cala en la administración pública

Actualidad

Segmentación, clave para hacer frente a las brechas de seguridad

El ransomware: ese gran enemigo que ha ganado visibilidad con la Ley de Protección de Datos

No solo IT

Seguridad en movilidad, la gran olvidada

¿Por qué hay tantas organizaciones que siguen sin estar preparadas para IPv6?

Índice de anunciantes

Reportaje

Cuando son los empleados los que arriesgan **la seguridad empresarial**

Entrevista

"Entrégame tu tráfico y yo me encargo de limpiártelo en la nube" (Netskope)

Revista Especial

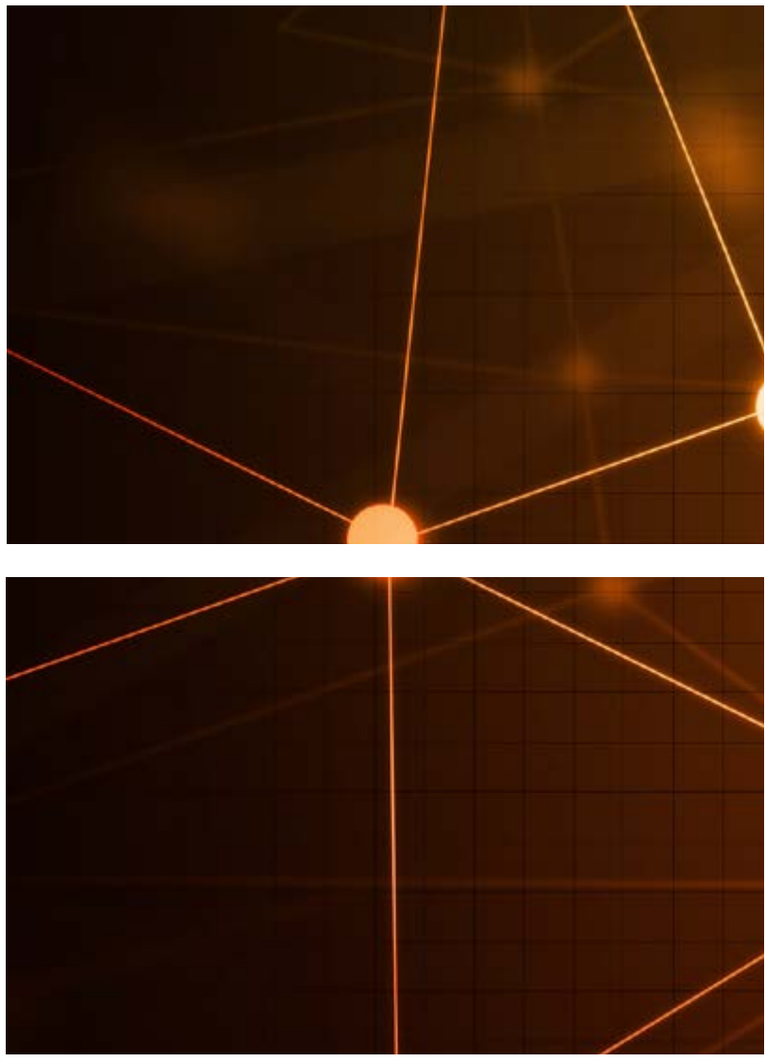
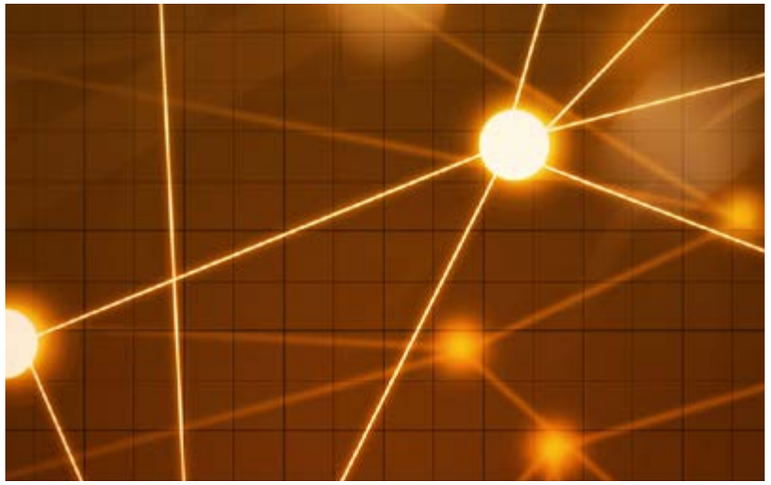
Samsung Knox, la seguridad de la movilidad a tu alcance

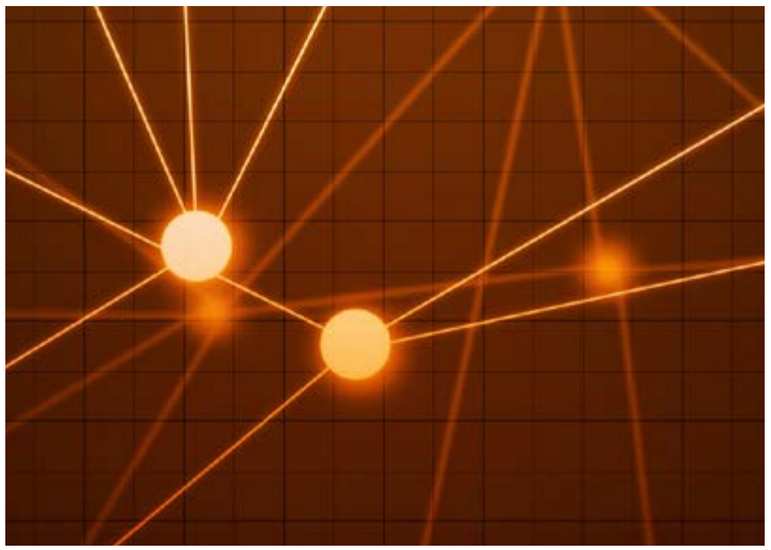
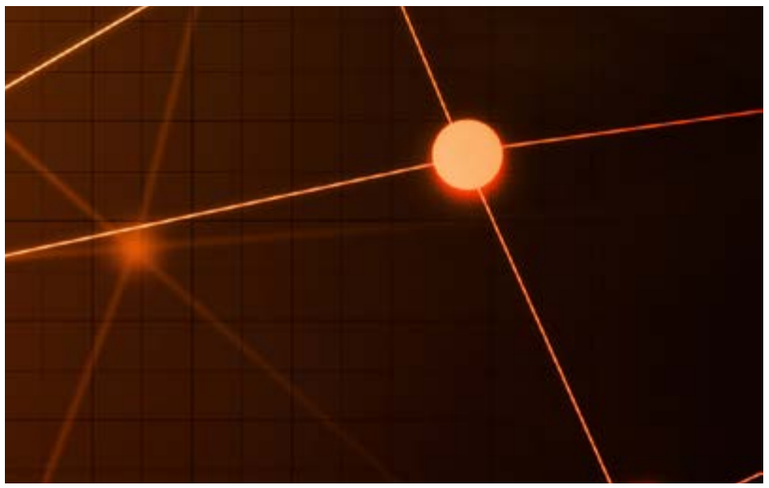
Especial IT Trends

2020, nuevos pasos en el viaje digital

Segmentación, clave para hacer frente a las brechas de seguridad

La segmentación de red no es nada nuevo. La complejidad de las redes es lo que ha cambiado. Tradicionalmente la segmentación se llevaba a cabo con listas de control de acceso en un firewall o un router, pero la pérdida de perímetro lo ha convertido en una tarea desalentadora. Es lo que parece confirmar un reciente estudio de la compañía Illumio enfocado en el estado de la segmentación como parte de una defensa en profundidad.

La segmentación limita la capacidad de los ataques de moverse lateralmente dentro de una organización al dividir las redes, creando subredes o subdivisiones de ésta con el objeto de controlar principalmente el acceso a recursos, así como el tráfico sin afectar su rendimiento. Además, en el caso de una intrusión, reducir la superficie del ataque gracias a la capacidad intrínseca de aislamiento de los activos críticos que provee la segmentación. La segmentación de red es reconocida como una práctica recomendada de ciberseguridad, aunque hoy en día está muy infrautilizada en las organizaciones.

Sólo el 19% de las empresas se protegen contra la propagación de una brecha con segmentación. Y aunque aproximadamente un 25% están planifican-

La segmentación limita la capacidad de los ataques de moverse lateralmente dentro de una organización al dividir las redes

Más de la mitad de las empresas no se está protegiendo con segmentación en absoluto, ni planea hacerlo en los próximos seis meses

do activamente un proyecto, más de la mitad no se está protegiendo con segmentación en absoluto ni planea hacerlo en los próximos seis meses.

Sobre los datos del estudio dice Matt Glenn, vicepresidente de gestión de productos de Illumio, que confirman lo que se sabe desde hace tiempo: a pesar de que las empresas se dan cuenta de que la probabilidad de un incidente de seguridad es alta "no aprovechan la segmentación porque es demasiado difícil y costoso de implementar, especialmente con firewalls, lo que impide una adopción más amplia".

Como elemento positivo, el estudio también recoge que el 45% de los encuestados planea comenzar un proyecto de segmentación en los próximos seis meses.

Tanto se esté de lleno en un proyecto como se esté planeando en el corto o medio plazo, es conveniente tener en cuenta las siguientes buenas prácticas.

1. Cuidado con la segmentación excesiva

Si bien aislar los activos individuales en una red es una excelente estrategia de ciberseguridad, cuando una red está demasiado segmentada, puede ser más difícil de administrar, e incluso afectar el rendimiento de la red, lo que afecta la productividad de los empleados.

Es necesario tener en cuenta la importancia de cada recurso que se está aislando, cuán sensibles son los datos y los sistemas y cuánto tráfico de red se espera que maneje ese recurso. Hacerlo puede ayudarlo a equilibrar el peso de la seguridad que aplica con el valor del recurso.

2. Realizar auditorías de red periódicas

No se puede aislar y proteger lo que no se puede ver. Realizar auditorías frecuentes de la red para identificar cualquier activo nuevo que se haya agregado a la red es una de las prácticas de seguridad de red más efectivas para cerrar las brechas de seguridad en su organización. Por lo tanto, hay que asegurarse de llevarlos a cabo con frecuencia.

3. Consolidar recursos similares en una base de datos

Al prepararse para implementar una estrategia de segmentación de red, puede ser útil no solo auditar

Enlaces de interés...

- Divide y vencerás: Segmentación al rescate
- Las oficinas inteligentes son altamente vulnerables frente a ciberataques
- Diez recomendaciones para securizar las máquinas virtuales

todos los datos en la red, sino consolidar recursos y datos similares en bases de datos individuales. Esto ayuda a promulgar una política de privilegios mínimos con mayor facilidad y a proteger la información extremadamente sensible más fácilmente.

Al definir qué recursos son “similares” para fines de consolidación, se ayuda a clasificar los datos tanto por tipo como por nivel de sensibilidad.

4. Crear y aislar portales de acceso para proveedores específicos

Si bien no todos los proveedores necesitan acceso al backend de una organización, algunos pueden necesitar acceder a sus sistemas para prestar servicios.

> El 45% de las empresas planea comenzar un proyecto de segmentación en los próximos seis meses

Al crear portales de acceso para proveedores externos en su red, es importante bloquearlos tanto como sea posible y sólo proporcionar acceso a los recursos que necesitan para cumplir su función en su organización. Esto ayuda a limitar el impacto potencial de una violación de seguridad en la organización del proveedor.

Compartir en RRSS

thalesgroup.com

THALES

¿Cuál es la estrategia de cifrado de su empresa?

Que sus datos estén en reposo, en movimiento o en uso, **puede confiar en Thales para proteger sus datos sensibles**

#EncryptEverything

Cuando son los empleados los que arriesgan la seguridad empresarial

En muchas ocasiones, los hackers pueden adentrarse en los equipos y documentos de una empresa gracias a los errores que comete el personal. El uso de dispositivos propios sin cifrar y una falta de formación y educación con respecto a los riesgos de seguridad son clave. Los CIO no deben perder de vista estos errores humanos si quieren preservar la seguridad empresarial.

Bárbara Bécares

Hay muchas formas a través de las cuales los empleados, de todos los niveles, de una empresa pueden facilitar el trabajo a cualquier hacker que quiera entrometerse en la empresa. La educación y formación de los trabajadores que dentro de una compañía utilicen sus sistemas informáticos, sea cual sea el sector de la firma, es esencial.

El factor humano todavía es uno de los de mayor riesgo en los procesos industriales, según ha vuelto a confirmar un estudio de Kaspersky. De hecho, los

FORMACIÓN Y CONCIENCIACIÓN PARA MEJORAR LA SEGURIDAD (DISPONIBLE BAJO DEMANDA)

CLICAR PARA VER EL VÍDEO

La falta de concienciación afecta a empleados de todos los niveles, incluido el propio equipo directivo

datos apuntan a que los errores de los empleados o sus acciones involuntarias estuvieron detrás del 52% de los incidentes que afectaron a las redes OT/ICS durante el año pasado.

En un webinar organizado por IT Digital Security sobre formación en la empresas se alertaba de que “es cinco veces más probable que un usuario pinche sobre un correo fraudulento que sobre uno real porque están pensados para que no te los leas, para que pinches, para que caigas”.

Hervé Lambert, Global Consumer Operations Manager de Panda Security; Pedro González, responsable de desarrollo de negocio de Kingston en España; Eusebio Nieva, director técnico de Check Point en España y Portugal y Luis Lubeck, investigador de seguridad en ESET Latinoamérica, nos acompañan en este reportaje que hará un repaso sobre diferentes asuntos que arriesgan la seguridad empresarial a causa de errores de quienes integran el equipo de trabajo.

Errores más comunes, inversión en educación de todas las personas que integran una compañía, diferencias o similitudes entre empresas pequeñas y grandes, lo que queda por mejorar y, cómo no, qué es lo que no debe perder de vista un CIO dentro de la compañía para asegurarse de que los empleados no facilitan el trabajo de los hackers.

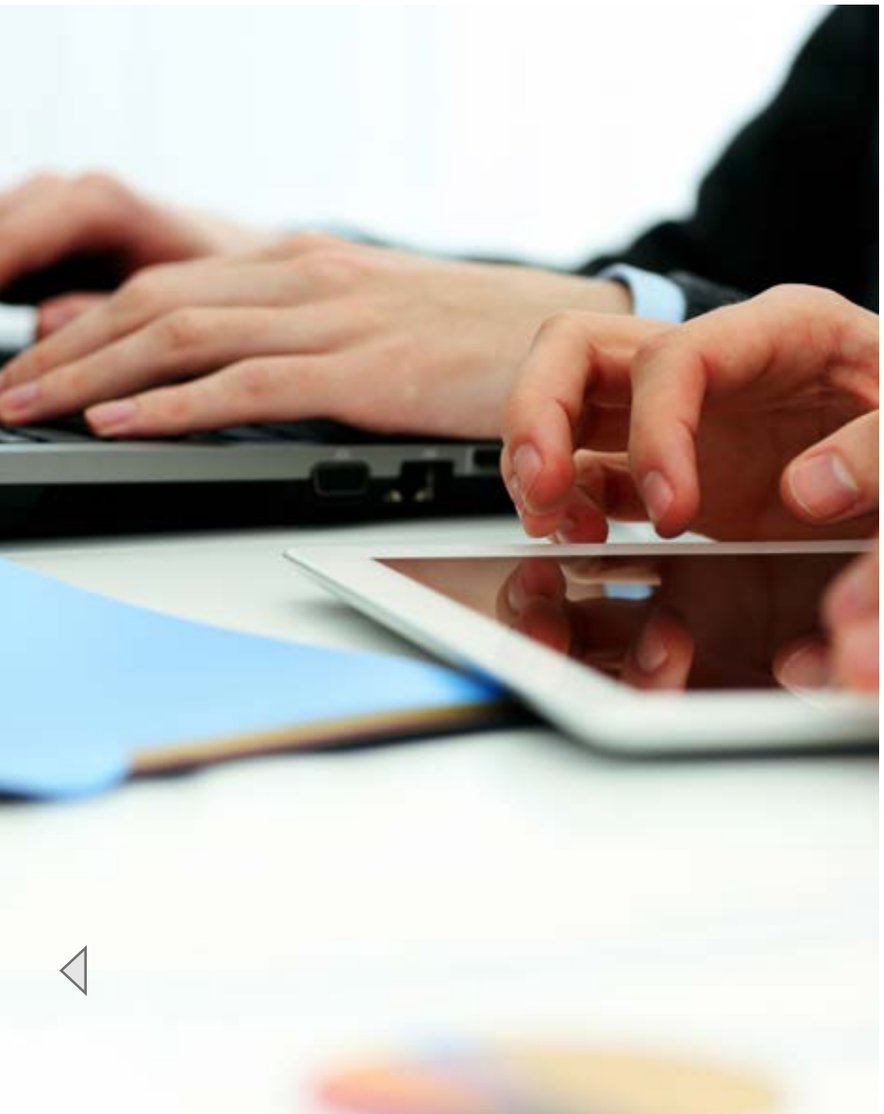
Los errores más comunes que cometen los empleados en cuanto a seguridad informática

Los errores pueden ser de varios tipos: por falta de atención o despiste, errores de percepción (pensar que un correo es legítimo cuando en realidad no lo es), errores en la decisión tomada o tener demasiada confianza en los programas informáticos que usamos en el día a día o en la seguridad de un dispositivo

“De estos tipos de errores, sin duda el que más crece, por la mejor ingeniería social utilizada por los

"En muchas ocasiones, por falta de información y educación, un trabajador de una empresa abre un correo malicioso pensando que es fiable"

Hervé Lambert, Global Consumer Operations Manager, Panda Security



atacantes, son los errores de percepción", concreta Hervé Lambert, desde Panda Security, que ha visto que, en muchas ocasiones, por falta de información y educación, un trabajador de una empresa abre un correo maliciosa pensando que es fiable. Eusebio Nieva, director técnico de Check Point en España y Portugal añade a este respecto que, a pesar de lo avanzados que están los ciberataques, muchos de los que entran en las empresas a causa de errores, son muy básicos: "abrir un correo que nos envía un destinatario desconocido, pinchar en un enlace dentro de este email o descargar archivos son las prácticas más comunes y, por tanto, las más peligrosas para la seguridad informática de una empresa" y, de hecho, como consecuencia de estas acciones, muchas veces se descargan virus como ransomware u otro tipo de amenazas.

Por otro lado, encontramos que otro uno de los principales riesgos para la seguridad informática es el robo o filtración de datos corporativos sensibles. Y la causa de esto, como explica Pedro González, responsable de desarrollo de negocio de Kingston en España es que "uno de los errores más comunes que cometen los empleados es el uso de dispositivos no cifrados y la falta de esta medida de seguridad hace que ante la pérdida de, por ejemplo, un USB, cualquiera pueda tener acceso a toda la información que almacena".

Si seguimos hablando de almacenamiento de archivos de una forma poco fiable, desde ESET Latinoamérica, Luis Lubeck comenta que "los casos más comunes que se pueden mencionar son los de utilizar servicios de nubes públicas para compartir archivos, envío de información comercial por direcciones de correo personales, y en cuanto al uso de los dispositivos de la empresa, no se ve una real conciencia de la protección de los mismos".

Inversión en educación y formación: necesita mejorar

La formación y concienciación a los empleados es una asignatura pendiente en las empresas que de-

berían potenciaar la cultura de ciberseguridad concienciando de forma continua a todo el personal, dándole los elementos oportunos para la gestión efectiva del riesgo.

Por su parte, desde Check Point. Eusebio Nieva afirma que “el balance entre el nivel de inversión que se realiza en la formación de sus trabajadores en el uso de herramientas TIC y las necesidades reales es claramente negativo”. A pesar de que “la gran mayoría de las empresas son conscientes de la importancia de llevar a cabo este tipo de actividades”, luego no todas lo consideren una prioridad dentro de su estrategia de protección, como aclara Nieva.

> Para casi el 60% de las empresas españolas, los programas de formación de empleados se sitúan en el último lugar de las prioridades para garantizar la seguridad de la información"
>
> Pedro González, responsable de desarrollo de negocio, Kingston

De hecho, Kingston cuenta con un estudio titulado “Estado actual de la protección de datos corporativos en España” que refleja que, para casi el 60% de las empresas españolas, los programas de formación de empleados se sitúan en el último lugar de las prioridades y acciones a llevar a cabo para garantizar la seguridad de la información”, según las palabras de Pedro González, desarrollador de negocio de esta firma. Si nos vamos al otro lado del Atlántico, a México, en el que muchas empresa españolas están instaladas, nos cuenta Luis Lubeck que “según el ESET Security Report solo el 39 % de las empresas situadas en México tienen políticas activas de concientización y el 19 % declaró no tener implementadas este tipo de actividades, con lo que es un punto donde hay que poner el foco”.

A este respecto, desde Panda Security, Hervé Lambert afirma que “la educación es necesaria pero no suficiente para evitar riesgos por ataques que explotan el factor humano”. De acuerdo con el directivo, “no solo hay que mirar al que ha cometido el error o su educación, sino a otros factores, incluso organizacionales, que hayan podido influir en la situación de riesgo o incidente”.

En otras industrias (en aviación, por ejemplo) se utiliza de hecho un marco de análisis de investigación del factor humano cuando hay incidentes (Human Factor Analysis and Classification System

- HFACS), que buscan las raíces de los problemas a todos los niveles. Este marco no se aplica todavía en ciberseguridad, pero pensamos que sería interesante hacerlo, según Lambert.

Las empresas pequeñas son más vulnerables

Como se menciona a menudo, las empresas pequeñas, igual que sucede con los usuarios individuales, tienden a pensar que no interesan a un hacker, en un panorama en el que están rodeadas por firmas gigantes con datos que podrían ser de más valor. “Lo que marca la diferencia es la cantidad de datos que almacena cada modelo de negocio, por lo que, como norma general, un hacker siempre tenderá a atacar a las empresas más grandes, ya que la recompensa es mayor”, aclara Eusebio Nieva desde Check Point.

Pero, una vez más, hay que recordar que una empresa pequeña o mediana también puede ser objeto de ataques. Y, además, al contar con menos recursos, en muchas ocasiones estas compañías no cuentan con una seguridad fuerte. Como explica Pedro González como portavoz de Kingston que “las compañías de menor tamaño suelen contar con menos recursos tanto técnicos (herramientas de ciberseguridad, departamento de protección de datos, etc.) como humanos (nadie de la plantilla es experto en temas de seguridad informática), por lo que son más susceptibles a ser víctimas de cualquier ataque o brecha de seguridad”.

Recuerda el portavoz de Panda Security que “obviamente las empresas con más recursos pueden hacer más, con personal especializado interno o externalizado. Las empresas más maduras en ciberseguridad suelen ser de tamaño grande, con más capacidad para mitigar riesgos que una pyme. No están en la misma situación y las Pymes son más vulnerables en este sentido”.

> "En cuanto al uso de los dispositivos de la empresa, no se ve una real conciencia de la protección de los mismos"
>
> Luis Lubeck, investigador de seguridad, ESET Latinoamérica

La responsabilidad del CIO

La falta de concienciación afecta a empleados de todos los niveles, incluido el propio equipo directivo. Hervé Lambert como portavoz de Panda Security se muestra contundente con esto: es erróneo pensar que “ponérselo fácil a los hackers” es un tema de los empleados. En realidad, es más bien lo opuesto. La empresa debe hacer una evaluación de riesgos y tomar medidas para, por ejemplo, arreglar las vulnerabilidades en los sistemas que utilicen los empleados. Las decisiones importantes sobre los riesgos y su mitigación se toman arriba, no por los empleados.

Así que es momento aquí de enfocarse en el CIO y ver qué medidas tiene que tomar un responsable del departamento de tecnología para que los erro-

"Es muy importante que (un CIO) tenga en cuenta el uso de dispositivos móviles y personales, ya que los empleados tienden a utilizar su propio móvil para funciones laborales"

Eusebio Nieva, director técnico, Check Point España y Portugal

res humanos no faciliten el trabajo a los hackers. Y aquí hay unos consejos para CIO dados por los expertos en tecnología que participan de este análisis:

- **Contar con tecnologías que impidan explotar programas de la empresa.** Si se cuenta con tecnologías y procesos eficientes que impidan la explotación de los programas más comúnmente utilizados por los trabajadores, el riesgo de ataque se puede minimizar, aunque el empleado pueda abrir un correo que no debe abrir.
- **Concienciación y formación de la plantilla de trabajo.** También se debe concienciar y formar para que quien integra la empresa utilice el sentido común, informe cuando reciba correos sospechosos y no los abra, etc. Disponer de planes de concienciación y formación en ciberseguridad de todo el personal, e ir actualizando a los trabajadores acerca de las nuevas tecnologías que se vayan implementando para proteger los equipos.
- **Implementar procesos de vigilancia.** Esto ayuda a un CIO a anticipar posibles ataques o fugas de información.
- **Seguir esquemas como ISO 27001 y 27002 o el Esquema Nacional de Seguridad.** Estas regulaciones establecen de forma sistemática qué es lo que hay que hacer para mejorar en la gestión de la ciberseguridad.
- **Prestar especial atención a la movilidad de los datos.** Desde hace años existe una tendencia generalizada a utilizar dispositivos BYOD (Bring Your Own Device), entre los que destacan los USBs. Este es uno de los principales peligros, ya que en el último año el 71,3% de los empleados ha perdido al menos una vez un USB con documentos de trabajo desprotegidos (según datos aportados por Kingston).
- **Evitar el uso de teléfonos personales para manejar información corporativa.** Además de los USBs, es muy importante tener en cuenta el uso de dispositivos móviles y personales como el teléfono móvil, ya que los empleados tienden a utilizar su propio móvil para funciones laborales. El malware móvil es una de las principales amenazas a las que hacen frente las empresas españolas.

FORMACIÓN Y CONCIENCIACIÓN PARA MEJORAR LA SEGURIDAD

Las ciberamenazas crecen y se multiplican. Las brechas de seguridad están a la orden del día, el phishing no deja de crecer y los ataques BEC (Business Email Compromise) son cada vez más habituales.

Cuando se habla de ciberseguridad se tiende a pensar que las amenazas vienen siempre de fuera, pero en realidad un gran porcentaje de los problemas se inician dentro, la mayoría de las veces por un error humano, pinchando un enlace malicioso, abriendo un adjunto que no es lo que parece, respondiendo un email que no es de quien dice ser...

El 75% de los ejecutivos citan el phishing como la mayor amenaza de ciberseguridad para su negocio. Por eso el poder identifica un email falso, Conocer y comprender el panorama actual al que nos enfrentamos, se puede convertir en la primera línea de defensa de las empresas.

Uno de los errores más comunes que cometen los empleados es el uso de dispositivos no cifrados

- **Uso de dispositivos seguros.** Implementar el cifrado de datos, tanto por hardware como por software. Asimismo, contar con copias de seguridad en dispositivos de almacenamiento externo y sin conexión a internet permite a las empresas hacer frente a ataques como ransomware.
- **Prestar atención al uso del correo electrónico.** Este es uno de los principales vías de acceso de virus al sistema informático de la empresa.
- **Priorizar la proactividad.** Es necesario que los responsables de seguridad de las compañías adopten un cambio de posición. Pasar a ser proactivos en lugar de ser reactivos. Esto quiere decir que basen su estrategia de ciberseguridad en un concepto básico como la prevención, ya que la forma de evitar ser víctima de ciberamenazas sencillas o incluso de mayor calado reside en adelantarse a ellas.
- **Mejorar el manejo de la información.** Implementar procesos de gestión en el manejo de la información y controles con los empleados para prepararse frente a posibles ataques.

Enlaces de interés...

- Formación y concienciación para mejorar la ciberseguridad
- El 52% de los incidentes de ciberseguridad en redes industriales están causados por el ser humano
- Saber dónde están los datos sensibles es la principal barrera de una estrategia de cifrado

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

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

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Samsung Knox, la seguridad de la movilidad a tu alcance

Samsung Knox ya no es un producto, es una plataforma. Lo que llegó al mercado en 2013 para que la incorporación de Android al mundo empresarial se hiciera con ciertas garantías de seguridad, ha evolucionado hasta ofrecer las mejores capacidades de seguridad, gestión de políticas y cumplimiento basadas en hardware de su clase más allá de las características estándar comunes en el mercado actual de dispositivos móviles.

SAMSUNG Knox

Samsung Knox, la seguridad de la movilidad a tu alcance

El dominio decreciente de los Blackberry y la presencia ascendente del iPhone de Apple como dispositivos estándar corporativos fue una de las razones que impulsó a Samsung a reforzar la seguridad del sistema operativo Android de manera específica para la empresa y los mercados B2B. Se sumaba lo que entonces se bautizaría como BYOD (Bring Your Own Device), que estaba llevando a que la plataforma de Google irrumpiera con fuerza en la empresa mientras los departamentos de TI luchaban para mantenerse al día.

Nace así la primera versión de Knox como parte de Samsung For Enterprise (SAFE), con el concepto de usar un enclave seguro, o un entorno de procesamiento separado dentro de la arquitectura de proceso ARM, llamada TrustZone, para incorporar capacidades de seguridad y autenticación de hardware y software en la plataforma Android. El lanzamiento inicial de Knox también introdujo el concepto de contenedorización para teléfonos Android desde la perspectiva OEM de un dispositivo nativo, lo que permite segmentar el trabajo y las aplicaciones personales y los datos en los dispositivos. En su lanzamiento Knox también trajo la verificación de arranque confiable y segura y la certificación remota, o la capacidad de verificar independientemente que un dispositivo esté en un “estado confiable” y que no haya sido alterado.

Desde aquellos primeros tiempos Samsung Knox se ha convertido en una plataforma que permite hacer muchas cosas, desde la personalización del dispositivo, a su gestión y añadiendo seguridad avanzada; una plataforma que permite dar respuesta a la necesaria estrategia de movilidad empresarial que debe adoptarse en un proceso de digitalización, o transformación digital; una plataforma basada en hardware que llega de fábrica en todos los dispositivos Samsung, tanto smartphones como tabletas.

Samsung Knox, la seguridad de la movilidad a tu alcance

“LA GESTIÓN DEL FIRMWARE EN DISPOSITIVOS MÓVILES ES ALGO EXCLUSIVO DE KNOX” (CÉSAR GARRO, SAMSUNG KNOX)

CLICAR PARA VER EL VÍDEO

Las empresas con decenas, cientos o miles de dispositivos móviles para empleados necesitan poder administrarlos de manera fácil, segura y eficiente

La movilidad empresarial se ha convertido en el gran habilitador del trabajo, que ha dejado de estar asociado a un lugar o ubicación física, ni siquiera a un horario. Cada vez más, el trabajo se ha convertido en una actividad que se puede realizar desde cualquier lugar, dispositivo y momento. De hecho, según datos de IDC, el porcentaje de trabajadores móviles respecto a la población activa en Europa Occidental será del 61% a finales de 2019 y alcanzará el 66% en 2023.

Vivimos en un mundo centrado en el móvil y las empresas se enfrentan a la compleja tarea de gestionar, aprovisionar y proteger los dispositivos móviles en las empresas, y Samsung Knox es la plataforma que proporciona el ecosistema de productos y servicios para asegurar y facilitar esa gestión de la movilidad. La plataforma Knox defiende contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware. Y lo hace a través de una suite de productos que, por un lado permiten el despliegue de los terminales, por otro la gestión de los mismos y además añadir seguridad a los dispositivos, la información que almacenan, e incluso las comunicaciones que establecen.

Seguridad por encima de todo

Asegurar y facilitar la gestión de los dispositivos móviles es una de las acciones que se pueden

Samsung Knox, la seguridad de la movilidad a tu alcance

llevar a cabo con Samsung Knox, que defiende contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware.

Ese entorno confiable permite separar el código crítico de seguridad del resto del sistema operativo, garantizando que sólo los procesos confiables que estén aislados y protegidos de ataques y exploits puedan realizar operaciones confidenciales, como el cifrado y descifrado de datos. Los entornos de confianza realizan verificaciones de integridad antes de ejecutar cualquier software, lo que les permite detectar intentos maliciosos de modificar el entorno de confianza y el software que se ejecuta en el dispositivo.

Y decíamos que es un entorno confiable que está respaldado por hardware porque es el hardware el que aísla el entorno del resto del sistema en ejecución, lo que garantiza que las vulnerabilidades en el sistema operativo principal no afecten directamente a la seguridad de dicho entorno confiable.

Por otra parte, Knox proporciona varias formas de aislamiento de aplicaciones para crear un espacio contenedor de aplicaciones protegidas en dispositivos Samsung sin olvidarnos de su capacidad para proteger los datos personales y profesionales mediante la autenticación de usuarios, de manera tan sencilla como introduciendo un PIN, o tan compleja como a través de autenticación biométrica; el cifra-

Samsung Knox, una historia de éxito

A lo largo de su historia, Samsung ha establecido asociaciones clave con más de 15 proveedores de soluciones de gestión de movilidad empresarial y dispositivos móviles para permitir la activación y el control de las funciones integradas de Knox.

Tener una estrategia de soporte lo más amplia posible con los diferentes EMM (Enterprise Mobile Management) ha sido una de las calves para que Samsung adoptara y activara los dispositivos habilitados para Knox. El éxito de esta estrategia se refleja en un fuerte crecimiento en las activaciones de Knox en los últimos años. Según los datos de la compañía más de 40 millones de trabajadores móviles empresariales usaron Knox en 2018, un número que se ha más que duplicado año tras año desde 2013. Samsung pronostica que este mismo crecimiento para el uso de Knox continuará hasta 2020.

Samsung Knox, la seguridad de la movilidad a tu alcance

Terminales Samsung para el mercado profesional

Entre su amplia oferta de productos, Samsung cuenta con ediciones pensadas especialmente para empresas y entornos profesionales que requieren de unas especificaciones específicas en términos de seguridad, personalización según las necesidades de cada negocio, y soporte técnico de calidad. Algunos de estos modelos son:

- **Samsung Galaxy Note 10,** una potencia nunca antes vista

- **Samsung Galaxy Tab Active Pro,** una Tablet robusta para llevar su negocio a todas partes)

- **Samsung Galaxy Xcover 4S,** ideado para trabajar al aire libre

- **Samsung Galaxy Tab S6,** Portátil y con el rendimiento de un PC

- **Samsung Galaxy S10,** un teléfono de nueva generación para la nueva generación

do de los datos del dispositivo, que garantiza que los datos se descifren sólo en el dispositivo donde están almacenados, y sólo por el propietario del dispositivo; el cifrado de los datos de red mediante la más amplia selección de características avanzadas de VPN; y la capacidad de localizar, bloquear y borrar el dispositivo de forma remota en casa de que sea robado o salga de un perímetro geográfico especificado.

Con respecto a la opción de VPNs, destacar VPN Chaining, que permite el uso de dos túneles VPN para cifrar doblemente el tráfico, mejorar el anonimato y evitar que un solo error de seguridad en una capa VPN comprometa el cifrado de la red.

Gestión del dispositivo

Las empresas con decenas, cientos o miles de dispositivos móviles para empleados necesitan poder

Samsung Knox, la seguridad de la movilidad a tu alcance

administrarlos de manera fácil, segura y eficiente. Los administradores de TI pueden controlar los dispositivos Samsung Knox de manera integral, administrando las funciones del dispositivo con facilidad.

En cuanto al despliegue, se cuenta con Knox Mobile Enrollment, un servicio gratuito para terminales empresariales que hace que, una vez encendido, el terminal se ponga en contacto con la herramienta de gestión que tenga el cliente, y se quedará bloqueado hasta que el usuario introduzca sus credenciales corporativas

Es decir que con Knox Mobile Enrollment las empresas pueden automatizar la inscripción de dispositivos, ya sea individualmente o en masa. Después de que un administrador de TI registra un dispositivo con este servicio, el usuario del dispositivo simplemente lo enciende y lo conecta a una red Wi-Fi o 3G / 4G para inscribirlo en un sistema EMM. No hay inscripción manual de dispositivos individuales, y no hay necesidad de gestión y verificación de IMEI, todas tareas onerosas que requieren mucho tiempo y son propensas a errores.

Una vez dado este paso, se puede aplicar una personalización de los dispositivos, permitiendo o restringiendo casi todos los aspectos de la configuración del dispositivo y la experiencia de usuario, incluidas las animaciones de arranque que incorporan logotipos empresariales personalizados, configuraciones de pantalla, fondos de pantalla, configuraciones de red, quitar aplicaciones del sistema que no se requieran en el terminal, o poner aplicaciones que sí se quiere poner.

Un aspecto muy interesante son las 1.200 API con las que cuenta Samsung para la gestión granular y flexible del dispositivo, que se incluyen dentro de lo que se conoce como Samsung Knox SDK, y que permite a los administradores de TI empresariales implementar políticas de TI para administrar y proteger todos los aspectos de los dispositivos Knox

Uno de los avances importantes que ha hecho Samsung dentro de la parte de gestión es la posibilidad de gestionar el firmware de los dispositivos. ¿Qué pasa cuando el terminal ya se ha desplegado y lo tienen los usuarios? Que se pierde parte del control, sobre todo a la hora de gestionar el firmware de ese dispositivo, algo que puede ser funda-

> Samsung Knox defiende los dispositivos móviles contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware

Samsung Knox, la seguridad de la movilidad a tu alcance

Knox E-FOTA (Enterprise Firmware Over The Air) permite que sean las empresas quienes puedan decidir cuándo quieren actualizar los smartphones o tabletas y cómo se va a hacer exactamente

Enlaces de interés...

- Samsung Knox
- Samsung Knox Security Solution
- Samsung Knox Manage
- 'Knox es la solución integrada de seguridad endpoint de Samsung'

mental en caso de querer solucionar una vulnerabilidad.

En el mundo de los dispositivos móviles, la única manera de actualizar el firmaware era contar con el usuario, que al fin y al cabo tenía que hacer una acción indispensable: aceptar de forma proactiva la actualización. Y en Samsung pensaron que eso no tenía sentido desde el punto de vista de la seguridad, que es la prioridad de Knox; no tiene sentido teniendo en cuenta que esto es algo que se lleva haciendo mucho tiempo en el mundo del PC, y no tiene sentido teniendo en cuenta que hoy en día los terminales móviles son un vector de ataque importantísimo en el que cada vez tenemos más información, y en los que cada vez delegamos más acciones.

Samsung lo ha resuelto con Knox E-FOTA, un acrónimo de Enterprise Firmware Over The Air, que permite que sean las empresas quienes puedan decidir cuándo quieren actualizar los smartphones o tabletas y cómo se va a hacer exactamente: que se descargue por ejemplo el día 1 en toda la flota de terminales, y que además se descargue siempre que tenga conectividad WiFi, y que una vez que esté descargada se instale entre las 2 y las 3 de la mañana. Y cuando se cumplen esas condiciones, la instalación se hará de forma automatizada y de forma transparente para el usuario. En definitiva, lo que se ha diseñado es una forma en que las empresas pueden controlar desde un punto de vista de seguridad y de gestión cómo quieren que se comporten sus terminales.

Compartir en RRSS

#ExpectTheUnexpected

RECONOCER**RIESGOS**

aunque aún sean desconocidos

Os presentamos la nueva protección para los E-Mails comerciales.
Descubra ahora la **Secure Email Platform** de Retarus: www.retarus.es/secure-email-platform

retarus

“Entrégame tu tráfico y yo me encargo de limpiártelo en la nube”

(Netskope)

Netskope nació para proteger el SaaS, pasó al IaaS y la navegación web y apunta ahora hacia las aplicaciones legacy. Reconocida en el cuadrante de Gartner en la categoría de Cloud Access Security Brokers, o CASB, Netskope quiere ir un paso más allá. “Queremos posicionarnos como un proveedor de seguridad en la nube que pueda absorber la carga de tráfico de los clientes, ya sea web, SaaS, o IaaS y aplicar políticas de control de una forma unificada”; lo dice Alain Karioty, Regional Sales director de Netskope, primer responsable de la compañía en España hasta el nombramiento de Samuel Bonete como director de Netskope para la región de Iberia.

CASB es un tecnología que nació ante la necesidad de proteger los servicios en la nube y el acceso a ellos por parte de los usuarios dentro y fuera del perímetro. Los CASB proporcionan una ubicación central para la política y la gobernanza al mismo tiempo en múltiples servicios en la nube tanto para usuarios como para dispositivos, además de visibilidad granular y control sobre las actividades del usuario y los datos confidenciales. Fundada en 2012, Netskope ha sido, desde sus comienzos, un jugador importante de este mercado. Durante estos años ha visto cómo algunos de sus principales competidores eran adquiridos por grandes empresas: Adallom

era comprado por Microsoft, CloudLock por Cisco, Palerra por Oracle, Elastica por BlueCoat, FireLayers por Proofpoint o Skyhigh Networks por McAfee; durante estos años, Netskope se ha mantenido como una compañía independiente, y privada; durante estos años, la empresa ha conseguido más de 400 millones de dólares en sucesivas rondas de financiación, la última en noviembre de 2018 por valor de 168,7 millones de dólares. También ha comprado una empresa, Sift Security para avanzar en la seguridad cloud de próxima generación. Porque la compañía quiere ir más allá del CASB, quiere convertirse en un proveedor de seguridad cloud con una propuesta diferencial que no sólo tiene en cuenta en Saas, el IaaS y la navegación web, sino las aplicaciones legacy y avances como el Edge o la 5G.

"Lo que no han entendido otros competidores, que se van al cloud público porque es más barato, es cuán importante es la latencia hoy en día"

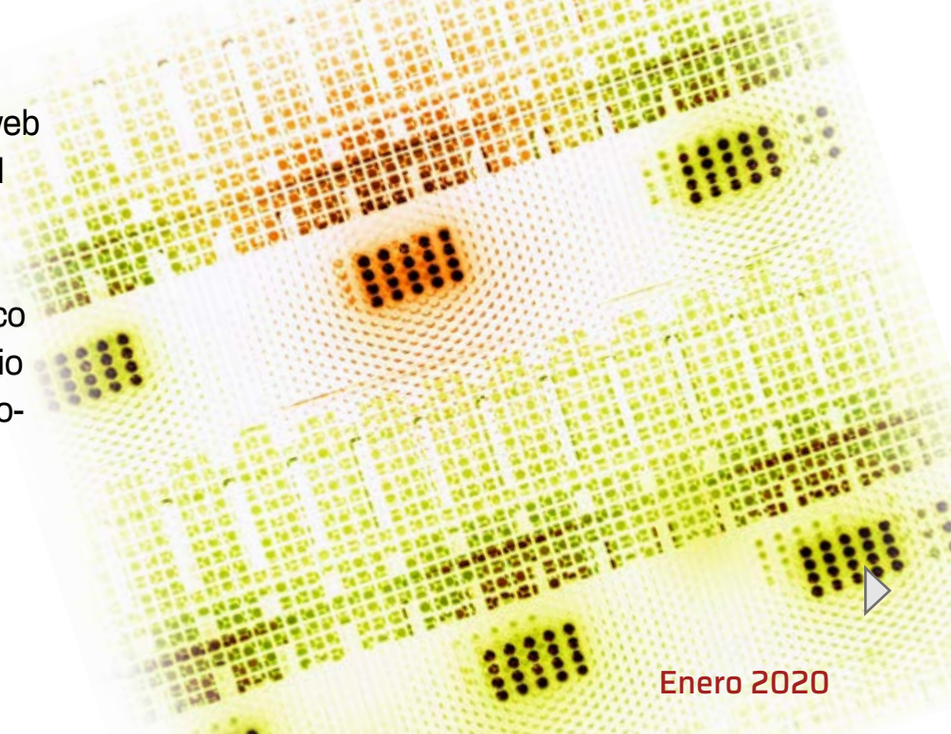
La cuestión, explica Alain Karioty, es cómo ha ido evolucionando la adopción de la tecnología por parte de los clientes junto con la evolución del tráfico de internet en las empresas; "el tráfico pasa de ser un 30% generado por las aplicaciones

"Si la realidad es que del total de tráfico empresarial un 8% es web, un 85% es de aplicaciones cloud, y un 7% es IaaS, ¿para qué sigues invirtiendo en perímetro?"

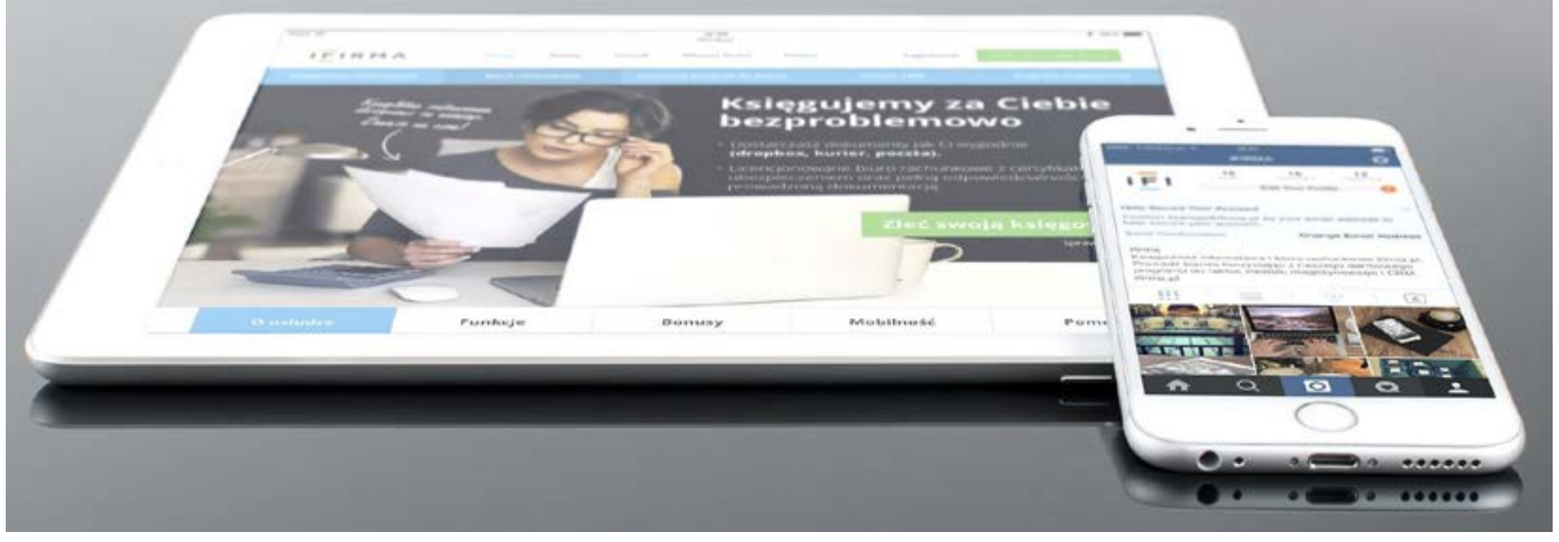
cloud versus un 70% tráfico web, para ser un 85% de cloud SaaS, un 7% de cloud IaaS y un 8% tráfico web". Este cambio hace que los clientes, con las tecnologías que tienen, no tengan visibilidad de ese tráfico.

Con las tecnologías tradicionales, explica Alain Karioty, se va a poder controlar el 8% de tráfico web haciendo filtrado de navegación, haciendo control de amenazas, etc., pero, lógicamente, eso no resuelve el problema porque lo que se necesita es controlar el 100% de ese tráfico. "Los clientes poco a poco se están dando cuenta, y eso es un cambio que ya estamos viendo", dice el responsable regional para Latinoamérica de Netskope.

Con un firewall y un proxy una compañía puede detectar, y bloquear, una página con contenido inapropiado, infectada por malware, pero cuando llegamos al tráfico SaaS, al mundo IaaS, no puede diferenciar si un Gmail es corporativo o personal, no pueden saber si los atacantes están aprovechándose de una vulnerabilidad y están creando una



En julio de 2018 Netskope compró Sift Security, una startup creada en 2014 que ayudaba a asegurar servicios de infrestructuras cloud como Amazon, Microsoft y Google utilizando Machine learning



cuenta falsa modificando una letra del apellido de un empleado; el 99% de la gente ve un documento que envía un colega de la misma empresa, y pincha y abre el documento, e inicia una infección. “Son ataques muy dirigidos, complejos, pero lo que ve el firewall es Office 365, y el firewall lo que sabe es que Office 365 está permitido, y como Office 365 genera una cantidad enorme de sesiones, y los proxy no están preparados para eso, se opta por un bypass y se deja pasar ese tráfico sin revisar”, dice Karioty.

Preguntado si las empresas empiezan a entender la nueva situación, si entienden que tienen un parte de responsabilidad de la seguridad en el mundo de la nube, dice Alain Karoity que algunas sí, pero a otras todavía les cuesta entender el modelo de responsabilidad compartido; “no saben que en SaaS tú eres el responsable de los datos”.

Entrégame tu tráfico

Si la realidad es que del total de tráfico empresarial un 8% es web, un 85% es de aplicaciones cloud, y un 7% es generado por las propias infraestructuras cloud, “¿para qué sigues invirtiendo en perímetro?”, pregunta Alain Karioty. La propuesta de Netskope, sigue diciendo el directivo, es: “entrégame tu tráfico y yo me encargo de limpiártelo en la nube”.

Es ir más allá de CASB, porque bajo este concepto se resolvía el problema de “voy a ir a Office 365 y quiero estar seguro, pero hoy el problema es diferente, el problema es que con mi proxy no tengo visibilidad de a dónde navegan mis usuarios; ni si las instancias son corporativas o personales; no puedo hacer control de malware en instancias que no son corporativas; tengo un problema con el tráfico SSL… Tengo muchos problemas y lo solucionamos de una manera simple: redirecciónname tu tráfico y yo me encargo, sea del tipo que sea, incluso del tráfico cifrado SSL”.

Al margen de otras empresas que se mueven en el segmento del CASB, Netskope tiene como rivales a fabricantes de seguridad bien asentados en el

mercado. La mayoría de los fabricantes de firewall, por ejemplo, están avanzando su estrategia hacia la seguridad del cloud, mientras que los proveedores de nube avanzan sus propios servicios de seguridad.

¿Cómo se posiciona Netskope? Dice Alain Karioty que los fabricantes de seguridad perimetral vienen del mundo del appliance y algunos han comprado tecnologías que les permiten controlar ciertas partes del cloud, pero la propuesta de Netskope es diferencial y única: reenvíanos tu tráfico más allá de tu perímetro corporativo, hacia la nube, sabiendo que estés donde estés te voy a aplicar control; hoy por hoy no lo ofrecen; no pueden procesar en línea cerca de los usuarios el tráfico SaaS, web, IaaS y hacer los controles que hacemos, no son capaces.

Inversión en centros de datos y acuerdos de peering

Pedir a las empresas que les entreguen su tráfico no es asunto baladí. Netskope lleva tiempo preparándose para ello. Durante el primer trimestre la compañía abrirá un datacenter en Madrid, pero además se están montando 50 puntos de presencia “de forma que la seguridad esté lo más cerca del usuario”.

Lo que no han entendido otros competidores, que se van al cloud público porque es más barato, es cuán importante es la latencia hoy en día, explica Alain Karioty. Dice el directivo que cuando se trabaja con un proveedor de cloud pública este proveedor te da el espacio y la conectividad, “y tú no puedes escoger las rutas” por las que pasa tu tráfico; “esa conectividad preselecciona las rutas más baratas, y hace peering con los proveedores de acceso menos costosos”.

Añade Karioty que la aproximación de Netskope es ir a cloud privado “y nosotros mismos cerrar acuerdos de peering con los proveedores de acceso local de forma de que en cuanto salgas a Internet ya estés directamente conectada con nosotros, estés en la red corporativa o en 4G, y luego hacemos también conexión directa con los tres principales proveedores de cloud. Eso no lo puedes hacer cuando estás en Amazon porque no controlas esa parte de ese tramo”.

Evolucionando hacia el legacy

Después de proteger el SaaS, el IaaS y la Web, ¿cuál es el siguiente paso? “El siguiente paso son

Después de proteger el SaaS, el IaaS y la Web, el siguiente paso para Netskope es la protección de las aplicaciones legacy privadas

"Lo que vamos a lanzar en este primer trimestre se llama Netskope Private Access, que está basado en el modelo Zero Trust del que se habla tanto"

Enlaces de interés...

- ¿Caminando o arrastrando los talonmes?
- Cyber Kill Chain para explotar los servicios cloud
- Netskope lanza su nueva infraestructura de protección cloud y web
- 'Seguridad endpoint, autenticación, CASB y correlación de eventos son el futuro de la seguridad' (Netskope)

las aplicaciones legacy privadas, que son client server y que estén tanto en un datacenter tradicional o un datacenter en nube", dice Alain Karioty. Explica el directivo que lo habitual es acceder a esas aplicaciones a través de VPN, pero que el problema de la VPN es que cuando le das acceso a un usuario, puede ser un usuario interno, o un colaborador externo; y cuando ese colaborar externo está dentro, no se sabe en realidad lo que está haciendo. "Y lo que vamos a lanzar en este primer trimestre se llama Netskope Private Access (Acceso privado seguro), que está basado en el modelo Zero Trust del que se habla tanto".

El modelo Zero Trust se basa en dar acceso a un usuario solamente a lo que tiene que tener acceso, solamente en la franja horaria que tiene que tener acceso, para hacer lo que tiene que hacer y desde el dispositivo que tienes que usar exactamente. Este modelo de confianza cero sustituye esa VPN estableciendo una capa intermedia, Netskope Cloud, que es donde el usuario se conecta para acceder al recursos que tenga que acceder, que puede estar en un datacenter privado o en un nube pública, y bajo unas condiciones establecidas.

"Al final el motor es el mismo, lo que hemos hecho es ir ampliando el destino", dice el responsable de Netskope para Latinoamérica. Y es que, si inicialmente el destino era solamente SaaS, y luego se evolucionó hacia el IaaS, para ampliarse posteriormente a la navegación web, "ahora lo vamos a ampliar en aplicaciones privadas eliminado las VPN, que es también una tecnología legacy, evitando el tener que darte una IP privada sobre la que no tengo control".

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.

it TRENDS

ENERO 2020

2020: nuevos pasos en el viaje digital

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

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

2020,
en busca de las tecnologías estratégicas para el negocio

Los responsables empresariales, cada vez más caracterizados por un perfil tecnológico e innovador, se enfrentan hoy a un entorno marcado por los cambios, las tendencias tech, la competencia, la incertidumbre y la oportunidad. Arranca 2020, un nuevo año que será para unos el comienzo de una nueva década, con nuevos planes estratégicos a corto, medio y largo plazo, y para otros, el final de un decenio en el que cumplir las metas propuestas ejercicios atrás. Independientemente de cómo lo considere cada uno, los próximos doce meses serán clave para todas -y son muchas- las organizaciones inmersas en procesos de transformación digital. Será, además, un año que constate el ritmo cada vez mayor al que evolucionan las tecnologías.

En IT Trends hemos analizado ese futuro de las tendencias tecnológicas en este número, junto a destacados protagonistas tecnológicos del mercado. Tanto en nuestro Encuentro "Tendencias TI 2020, visionando el futuro", como en nuestros Diálogos IT Trends, HPE, Sothis, ESET, GMV, F5 Networks, Micro Focus y Nutanix, nos han proporcionado las pautas de este entorno tecnológico en el que hoy se mueven las empresas y cómo éstas pueden resolver algunos de los retos a los que tienen que hacer frente en ese movimiento digital. Asimismo, uno de estos desafíos, el de la ciberseguridad, será analizado en el próximo Encuentro IT Trends "Ciberseguridad en 2020, qué debemos esperar", que se emitirá a finales de enero.

Además de agradecer a todos los patrocinadores su participación en estas actividades, también queremos hacer partícipes de este agradecimiento a todos aquellos profesionales empresariales y de TI que han colaborado con nosotros en la elaboración del **Informe IT Trends 2020, el año de la consolidación**, que puedes descargar aquí. En este documento se recoge el estado de las iniciativas tecnológicas en las empresas españolas durante 2019, y sus perspectivas de inversión y proyectos TI en 2020.

A todos ellos y a ti, lector de este número de IT Trends, feliz 2020 innovador y digital. ■

Arancha Asenjo
Directora de IT Televisión
y Lead Gen Programs

Hewlett Packard
Enterprise

ALMACENAMIENTO HPE 3PAR

Basado en memoria Flash. Hasta un 50 % más rápido*

→ Descubre cómo en

www.hpe.com/es/es/storage/hpe-memory-driven-flash

* Basado en pruebas internas de HPE 3PAR comparado con valores de latencia publicados de Dell PowerMax a 26 de noviembre de 2018.

IT Trends 2020, el año de la consolidación digital

Muchas organizaciones y administraciones públicas se marcaron 2020 como el año para conseguir sus objetivos de transformación digital. Muchas lo han conseguido, pero es cierto que, en el transcurso del desarrollo de dichos planes, han ido surgiendo y cogiendo fuerza nuevas tecnologías y planteamientos.

Con el objetivo de continuar analizando la realidad digital de la empresa española, IT Research llevó a cabo un nuevo estudio entre los lectores de las publicaciones de IT Digital Media Group, para conocer el estado de esas iniciativas digitales y sus planes de implantación de TI para 2020.

El informe **IT Trends 2020, el año de la consolidación digital**, que puede descargarse aquí, constata que la nube puede considerarse ya como la plataforma sobre la que se sustentan la mayor parte de las iniciativas tecnológicas de las empresas, tales como alojamiento de datos, desarrollo de aplicaciones o almacenamiento, convirtiendo así al cloud en un elemento imprescindible en cualquier estrategia de TI, con un modelo híbrido como el preferido por los equipos de IT. Además, muestra que la seguridad seguirá siendo prioritaria en este año en muy diferentes ámbitos (cloud, redes, entorno de trabajo...) y apunta que la Inteligencia Artificial supondrá el gran paso que muchas organizaciones den para innovar en sus diferentes áreas de actuación.

Para complementar esta perspectiva de la realidad digital, hemos elaborado un documento con los principales pronósticos tecnológicos realizados por las consultoras de aquí a unos pocos años, relativos a cinco ámbitos de la TI empresarial: cloud, Edge/IoT, Inteligencia Artificial, seguridad y transformación digital, que reflejan de qué manera la propia evolución de estos segmentos dará lugar a nuevos productos y servicios para el consumidor final, sea éste el ciudadano de a pie o la propia empresa, así como nuevos modelos de negocios que potencien el mercado de TI. Lee aquí Preparándonos para el futuro. ¿Cómo están cambiando las TI empresariales? ■

10 tecnologías de transformación digital para 2020

Este 2020, el panorama de la transformación digital va a sufrir cambios, y las tendencias que han guiado las iniciativas de digitalización de las organizaciones van a salirse de lo que ya se puede considerar tradicional.

La nube, la computación perimetral, Internet of Things y otras tecnologías hasta ahora emergentes comenzarán a establecerse, dejando paso a nuevas innovaciones que impactarán en los siguientes episodios de la era digital.

En el último año las organizaciones han dado grandes pasos en su camino hacia la digitalización y, a lo largo de 2019, conceptos que eran disruptivos hasta ahora, como la nube, la computación perimetral o la automatización se han convertido en algo relativamente habitual. Gran parte de las organizaciones ya han implementado muchas de estas tecnologías o están en proceso de hacerlo, lanzando proyectos piloto en distintas áreas, y su impacto ya se siente y se está asimilando en gran parte de su estructura, con mejores o peores resultados.

Esto ha cambiado completamente la forma de entender los negocios y el papel que tiene la tecnología que hay detrás de todas estas innovaciones. Las mejoras que proporcionan comienzan a notarse y se están asimilando como una realidad inamovible. Todavía quedan por superar problemas como la resistencia al cambio por parte de los trabajadores, especialmente en ciertos sectores, pero se está implantando una mayor conciencia de que el cambio hacia la era de los datos es imparable, y hay que adaptarse a ello para seguir avanzando hacia el futuro.

En este contexto, lo que anteriormente se consideraban tendencias están pasando a ser la tónica habitual del trabajo, a pesar de que quedan retos por afrontar para superar los problemas de trabajar bajo las condiciones de un nuevo paradigma digital. Pero el avance no frena, y las siguientes fases de la transformación digital estarán impulsadas por nuevas tendencias que las empresas comienzan a vislumbrar.

En un reciente artículo publicado por Futurum Research, se analiza en profundidad cómo está cambiando el panorama de las tendencias que mueven los procesos de digitalización en las empresas más avanzadas en este campo, y destacan 10 tendencias que van más allá de las que han dominado estas iniciativas hasta ahora.

No significa que la nube, la IA o las nuevas arquitecturas de datos y computación no vayan a seguir afectando a la forma en que las empresas operan y hacen sus negocios, pero la punta de lanza del cambio y la innovación se va a trasladar a nuevas áreas y tecnologías que los líderes de las empresas deben tener muy presentes si

Cinco tendencias tecnológicas emergentes con un impacto transformador

quieren estar preparados para lo que vendrá a partir de este 2020. Algunas, como 5G, la analítica avanzada de datos o la inteligencia artificial llevan tiempo acaparando titulares, pero todavía tienen mucho recorrido por delante en las próximas etapas de la transformación digital de las organizaciones. Las 10 tendencias que identifican desde Futurum son las siguientes:

1 5G everywhere. Hace tiempo que las redes celulares de comunicaciones están sufriendo problemas de saturación. En los países desarrollados el uso de 4G es masivo y en los que están en vías de desarrollo todavía se usa 3G, con resultados similares. Y las empresas no pueden depender mucho de estas tecnologías para sus operaciones ni para dotar de herramientas a sus trabajadores. Pero 5G promete superar las expectativas de consumidores y organizaciones en capacidad de conexión, ancho de banda, mínima latencia, etc.

Aunque las promesas puedan parecer tan vacías como en las generaciones anteriores, la realidad es que los proveedores de infraestructura para telecomunicaciones están apostando fuerte por llevar 5G a todos los ámbitos de la conectividad global. Las aplicaciones comerciales para las redes móviles están viéndose reforzadas por un gran número de casos de uso empresariales e industriales, que impulsarán el despliegue de esta tecnología en nuevos ámbitos, sustituyendo a las tecnologías actuales, y en muchos casos abriendo nuevos campos para los dispositivos conectados de uso profesional.

Ejemplos de ello se están viendo en las grandes inversiones de firmas de primera línea, como Nokia, Qualcomm, Verizon, AT&T o Huawei que van a ser los principales responsables del despliegue de la tecnología 5G en todo el mundo. Incluso a pesar de los esfuerzos de EEUU por desbancar al gigante chino Huawei, muchos países están decididos a implementar sus tecnologías para lograr un despliegue rápido y efectivo de las nuevas redes. Porque la industria no puede esperar a la resolución de conflictos comerciales con intereses alejados de los suyos, y demanda soluciones ya.

Se tiende a pensar que esto impulsará las ventas de móviles 5G como principal núcleo de negocio, pero las cifras de los principales analistas indican que la penetración de esta nueva generación de smartphones podría ser más lenta de lo esperado. No será así con las aplicaciones en las industrias de fabricación, salud o en los proyectos de SmartCity, que aprovecharán al máximo las nuevas posibilidades para dar conectividad a las tecnologías IoT, una de las innovaciones que más impactarán en sus respectivos ámbitos.

2 Una nueva generación de conexiones WiFi. Al mismo tiempo que las redes celulares están a punto de dar un gran salto evolutivo, lo mismo está sucediendo con las clásicas redes WiFi. La llegada del nuevo estándar WiFi 6, aunque no acapara tantos titulares de prensa como 5G, va a tener un impacto significativo en numerosos ámbitos. Estas redes se usan más en entornos domésticos y de oficina, pero con el gran aumento de velocidad que traerá el nuevo estándar, sus casos de uso industriales podrían multiplicarse rápidamente.

Se espera que las primeras soluciones lleguen al mercado a lo largo de 2020, y los expertos creen que la mayor baza de esta tecnología es que encontrará una gran sinergia con 5G, complemen-

tando la conectividad externa de esta tecnología celular con un mejor desempeño en interiores. Esto permitiría ofrecer soluciones completas que abarquen todas las necesidades de transmisión inalámbrica de datos, de extremo a extremo.

La velocidad de descarga tres veces más rápida es un gran avance, pero la fuerza de WiFi 6 estará más en su mayor capacidad para proporcionar conexión eficiente a un número muy superior de dispositivos de forma simultánea. Esto es una clave importante, ya que se espera que el volumen de dispositivos conectados en las empresas aumentará de un promedio del 10% al 50%, lo que requerirá más eficiencia, rapidez, ancho de banda y una administración más inteligente de todas esas conexiones.

Además, los expertos creen que en los próximos años el impulso de la tecnología WiFi vendrá dado en gran medida por la necesidad de actualizar los sistemas actuales. Hoy en día, el estándar de WiFi vigente experimenta dificultades para gestionar el creciente volumen de dispositivos conectados, algo que WiFi 6 solventará, independientemente de que la base de dispositivos existentes no cuente con esta tecnología.

3 Analítica para obtener ventajas competitivas. La analítica de datos se está convirtiendo en una herramienta fundamental para campos como la inteligencia de negocio, la experiencia del cliente y otras áreas que se están potenciando con la transformación digital. Según opinan desde Futurum, las empresas que no hayan invertido en analítica para 2020 probablemente tampoco lo harán partir de 2021. Y probablemente estará abocadas a la desaparición, en favor de quienes sí han apostado por aprovechar el valor encerrado en los datos, algo vital para ganar competitividad en la era digital.

Porque la cantidad de datos útiles que generan los clientes y usuarios no para de crecer, y para aprovecharlos es necesario invertir en las tecnologías necesarias para recopilarlos, almacenarlos y procesarlos en el contexto adecuado. Las viejas estrategias comerciales, basadas en el instinto, ahora se demuestran ineficaces frente al poder de las sofisticadas herramientas actuales de analítica. Estas permiten identificar fácilmente tendencias y posibles problemas, lo que lleva a actuar con más agilidad para aprovechar las oportunidades.

Y, tras un tiempo de uso de estas herramientas se está detectando una consolidación de

Se espera que el volumen de dispositivos conectados en las empresas aumentará de un promedio del 10% al 50%

las capacidades de analítica en el ámbito de las empresas tecnológicas, donde las grandes firmas están adquiriendo a pequeños innovadores en estas tecnologías con el fin de dotar de nuevas capacidades a sus soluciones tradicionales. Esta tendencia continuará en los próximos años, ya que los gigantes tecnológicos han descubierto el potencial que tiene la analítica en tiempo real, y hay muchas empresas emergentes especializadas en este campo.

4 IA y machine learning para potenciar la analítica. Todo el avance actual de la analítica de datos se fundamenta en las capacidades mejoradas que aportan la inteligencia artificial y el aprendizaje automático. Estas dos tecnologías, principalmente, son las responsables de llevar la analítica al siguiente nivel, aportando tres valores principales, que en opinión de los expertos son la velocidad, la escala y la conveniencia.

La velocidad y la escala se refieren a la capacidad que aportan la IA y el ML para automatizar el análisis de grandes conjuntos de datos, haciendo que ya no sea necesario asignar grupos enteros de analistas a estos trabajos. Con estos sistemas es posible reducir enormemente los tiempos necesarios para analizar la información, reduciendo a una mera fracción el tiempo invertido en tareas que podrían durar hasta varios años. Todo gracias a los potentes algoritmos actuales, que no solo son más rápidos, sino que se pueden escalar a los enormes volúmenes de información que se manejan en la nube.

Además, la evolución de estas herramientas de analítica se está desarrollando a una velocidad tremenda, y se espera que en los próximos años se acelere aún más, dando como resultado toda una nueva generación de capacidades para el software de analítica potenciado con inteligencia artificial y aprendizaje automático.

5 Blockchain saldrá finalmente del ámbito de las criptomonedas. A pesar de que se están explorando numerosas posibilidades para la tecnología de cadenas de bloques, ésta todavía tiene una fuerte vinculación con el ámbito de la minería de criptodivisas. Pero en los próximos años se verá una importante expansión a otros tipos de transacciones y comunicaciones electrónicas, ya que sus ventajas en materia de

9 tendencias de experiencia digital para 2020

seguridad atraen a nuevos sectores, como las finanzas o las administraciones públicas.

Empresas como Amazon están invirtiendo en democratizar el uso de blockchain mediante modelos de suscripción, y muchas empresas líderes en el ámbito de la tecnología están mirando con interés las posibilidades que podría ofrecerles. Por ejemplo, Samsung, IBM, Microsoft o Alibaba, que están explorando los posibles casos de uso más allá de los pagos y las criptomonedas.

Ejemplos de aplicación exitosa de blockchain se encuentran en la trazabilidad dentro de la industria alimentaria, en el campo de la propiedad intelectual o en la administración de bienes raíces y activos, campos en los que 2020 será un año clave para la implementación de blockchain.

6 Nueva etapa para las soluciones RPA. La automatización robótica de procesos (RPA) está evolucionando gracias a las nuevas tecnologías, y para muchos es la rama más popular de la inteligencia artificial. Su evolución está permitiendo a las organizaciones nuevos niveles de automatización de tareas, agilizando procesos cada vez más complejos y ahorrando mayores costes. Por ello, los expertos creen que 2020 será un buen año para el mercado de soluciones RPA, tanto por el crecimiento de las ventas como por la evolución que están realizando los proveedores más importantes.

2020 será un buen año para el mercado de soluciones RPA, tanto por el crecimiento de las ventas como por la evolución que están realizando los proveedores más importantes

Una de las vías de desarrollo que está cobrando fuerza es la utilización de RPA no para sustituir puestos de trabajo, sino para complementar a los trabajadores para aumentar el valor de la fuerza laboral. Esto no significa que no se destruyan puestos de trabajo al introducir esta fórmula de automatización, pero el objetivo es que la pérdida de empleos sea mínima, y que la automatización robótica de procesos sirva para potenciar las capacidades de los trabajadores restantes.

7 La IA conversacional se convertirá en una interfaz sólida. Aunque se está dando mucho bombo a los asistentes virtuales por voz, la realidad es que todavía no se ha desarrollado un ecosistema lo suficientemente diverso como para poder utilizar esta tecnología como interfaz principal para interactuar con las aplicaciones de negocio. De hecho, muchos se quejan de la dificultad de escribir un simple mensaje sin tener que corregirlo a cada paso. Pero los expertos creen que a partir de 2020 se podrán ver interfaces conversacionales basadas en IA verdaderamente útiles.

En este sentido, destacan los avances que introducirán proyectos como Microsoft Conversational AI, que pretenden crear plataformas con un reconocimiento de voz mucho más preciso, y sobre todo que permita entablar conversaciones complejas, en las que la máquina sea capaz de comprender matices emocionales que creen un contexto básico para la comunicación de los humanos.

Además, en el ámbito del hardware se está avanzando poco a poco en la creación de chips y SOC específicos para los dispositivos inteligentes empleados como interfaz para los asistentes virtuales. Aquí se distingue entre procesadores de lenguaje natural por hardware y dispositivos de captación de sonido especializados, capaces de reconocer la voz en ambientes ruidosos. Los expertos no creen que en 2020 se vean lanzamientos destacables, pero el avance de estas tecnologías continuará de forma discreta, sentando las bases de productos disruptivos que llegarán en unos años.

8 La tecnología de los PCs siempre conectados se convertirá en el estándar. El trabajo en movilidad depende cada vez más de la capacidad de los ordenadores de mantener una buena conexión a las redes, estén donde estén. En este sentido, ha nacido el concepto de ACPC (Always Connected Personal Computer), que pretende establecer como estándar básico uns serie de tecnologías que proporcionen conectividad permanente a los usuarios en movilidad.

Esto supone incorporar chips de comunicaciones LTE (o 5G), que ya existen, pero también avanzar en ciertas tecnologías que faciliten esta conectividad permanente. El principal problema es el consumo de batería, algo muy limitante sobre todo en equipos portátiles de alta potencia, con chips como Intel Core i7 y similares. En este sentido, fabricantes como Qualcomm o Lenovo está trabajando intensamente para diseñar chips de comunicaciones, procesadores y SOC de ultra bajo consumo. Aunque hay otras tecnologías que serán habilitadoras del concepto de ACPC, como nuevas baterías que proporcionen más autonomía en el mismo espacio, y que se puedan cargar rápidamente, como ya sucede con los smartphones y tablets. En opinión de Futurum, en el próximo año podrían llegar tecnologías de batería que ofrecerían autonomías nunca vistas, de incluso varios días. Esto materializaría por primera vez el concepto de ordenador portátil con el que la gente lleva soñando décadas, y supondría un cambio verdaderamente disruptivo en el trabajo en movilidad.

Aunque parece un cambio demasiado radical en una tecnología que avanza muy despacio desde hace muchos años, la de las baterías, y seguramente solo se podrá lograr esto si se mejoran también los consumos de los componentes integrados en estos equipos. Si se logra, habrá que

tener en cuenta que el rango de precios de estos equipos también supondrá una barrera importante para la adopción masiva en las empresas.

9 Normalización de los vehículos conectados y las ciudades inteligentes. Con la llegada de tecnologías como 5G y la computación en el extremo, que lograrán expandirse mucho durante 2020, por fin cobrarán vida ideas que hasta ahora han acaparado muchos titulares, pero que no están dando los resultados esperados. Dos de las más importantes y disruptivas para las personas quizá sean los vehículos conectados y las ciudades inteligentes. Por mucho bombo que se les haya dado, las iniciativas de los gobiernos locales para crear Smart Cities se han limitado a automatizar algunos procesos y a monitorizar mejor ciertas infraestructuras dentro de las ciudades, como puede ser el transporte o los suministros básicos gestionados por la administración.

Algo parecido sucede con los vehículos conectados, que sí generan muchos datos, pero estos no están repercutiendo como deberían en los servicios al conductor. En estos dos campos, la llegada de 5G y de la nueva idea de computación perimetral van a sentar las bases de nuevos niveles de automatización, inteligencia aplicada a los datos y servicios al consumidor y las empresas. Y será a partir de 2020 cuando esto podrá hacerse realidad, aunque dependerá del ritmo de implantación de las redes 5G y de cuánto inviertan las autoridades en infraestructuras en el extremo para hacerse cargo de los datos generados por IoT en Smart Cities y por los vehículos conectados.

La mayoría de los proveedores están transformando el modelo de negocio de TI, tanto local como alojado en instalaciones de terceros y en la nube

Mención aparte merecen los vehículos autónomos, un campo en el que el avance tecnológico de cada fabricante de automóviles está siendo muy dispar. El líder indiscutible es Tesla y, aunque otras marcas están apostando fuerte por construir su ecosistema de coches sin conductor, aún parece que se encuentran muy lejos del nivel alcanzado por la firma de Elon Musk.

10 Tendencias subyacentes que moverán el avance digital. Más allá de las tecnologías puntuales o interrelacionadas que evolucionarán y serán más o menos disruptivas en los próximos años, hay ciertas tendencias generales que se encuentran detrás de la mayoría de cambios a nivel tecnológico, tanto para las empresas como para los gobiernos y los consumidores. Se trata de conceptos que están cambiando la forma de entender el consumo, los negocios y el poder de los datos en la era digital. Desde Futurum distinguen tres tendencias principales:

❖ **Cambio hacia un modelo de "todo como servicio (XaaS)":** esto supone que los proveedores de tecnología, ya sea software, infraestructura o servicios en la nube, van a cambiar su modelo para ofrecer sus soluciones como servicio. Un claro ejemplo de la fuerza que está cobrando esta tendencia es la decisión adoptada por HPE, que ofrecerá toda su cartera de soluciones como servicio para el año 2022, revolucionando el mercado de infraestructura en el que es uno de los líderes mundiales. Y los expertos afirman que la mayoría de los proveedores se están dirigiendo hacia el mismo camino, transformando el modelo de negocio de TI, tanto local como alojado en instalaciones de terceros y en la nube. A esto se acompañará toda una batería de servicios de big data, analítica o blockchain entregados como servicio, facilitando a las empresas la adopción de nuevas tecnologías con un coste más contenido que si lo hiciesen todo por sí mismas.

❖ **Cambio de enfoque hacia la experiencia del usuario/cliente:** este es un campo del que se habla desde hace mucho tiempo, pero que solo ha cobrado verdadera importancia a la luz

del éxito que están cosechando los pioneros en invertir "de verdad" en mejorar su UX/CX para convertir al cliente en el centro de las estrategias comerciales. Con el establecimiento de los modelos de negocio digitales, basados en los datos, muchas organizaciones no se han dado cuenta de que la experiencia de usuario es un factor decisivo para impulsar los negocios, la innovación y la subsistencia, sobre todo en mercados de alta competencia. Pero, a partir de este año, se espera que las organizaciones adopten un enfoque más centrado en el cliente, buscando formas innovadoras de mejorar su experiencia para capturar y retener su interés, y generan una mayor vinculación con la marca. Y esta tendencia impactará directamente en ciertas tecnologías emergentes de diversos campos. Por un lado, en las comunicaciones inalámbricas 5G y WiFi 6 y, por otro, en la mejora de las capacidades de computación necesarias para aplicar la inteligencia artificial, la analítica en tiempo real, el aprendizaje automático y la nube. Pero también en la automatización inteligente y las nuevas interfaces de usuario como la realidad virtual y aumentada y las interfaces conversacionales basadas en IA.

❖ **Privacidad digital:** Con la llegada de nuevas y más restrictivas leyes de protección de datos personales, y con el empoderamiento de los ciudadanos en materia digital, las organizaciones van a llevar a cabo grandes cambios en casi todos los niveles de sus negocios, cada vez más movidos por los datos. Por una parte, ya están invirtiendo en las tecnologías necesarias para mantener la seguridad y la privacidad de los datos de sus clientes, socios y empleados. Por otra, están reconfigurando sus modelos de negocio para mejorar la transparencia, un factor cada vez más importante para generar confianza en los clientes. Además, se está instalando una corriente que pretende aportar beneficios a los clientes que cedan sus datos para fines comerciales o de mejora de servicios, algo que muchos ciudadanos ven con buenos ojos, ahora que saben más acerca de cómo las empresas utilizan su información para ganar dinero de forma directa o indirecta.

Aunque las grandes tecnológicas como Amazon o Google están en posesión de ingentes cantidades de datos de las personas y comercian con ellos, los gobiernos les están presionando con fuerza para que abandonen las clásicas formas de recopilar y utilizar la información, a través de leyes mucho más restrictivas. Esto supone cambiar sus políticas, pero también garantizar la privacidad y seguridad de los datos confidenciales a nivel tecnológico. Esto está ejerciendo mucha influencia en los propios fabricantes de infraestructuras TI y en los prestadores de servicios tecnológicos, que ya están implementando tecnologías para garantizar este nivel de protección, ofreciéndoselas a sus clientes, entre ellos los proveedores de la nube y de redes sociales. ■

MÁS INFORMACIÓN

- Futurum Research
- 10 tendencias tecnológicas para 2020 (TrendForce)
- Tendencias en infraestructura digital para 2020 (Uptime Institute)
- Cinco tendencias tecnológicas emergentes con un impacto transformador (Gartner)
- 10 predicciones tecnológicas para 2020 (IDC)
- 5 tendencias que revolucionarán los medios de pago en 2020
- 9 tendencias de experiencia digital para 2020
- Future Disrupted: 2020 (Predicciones de disrupción en el futuro para 2020)

Si te ha gustado este artículo, compártelo

TENDENCIAS QUE NO VERÁN LA LUZ EN 2020

Durante 2019 se habló mucho de ciertas tecnologías emergentes que en los próximos años mostrarán un gran potencial disruptivo, generando grandes cambios en la sociedad y en los negocios. Ejemplos de estas tendencias tan atractivas, pero no tan cercanas son los ordenadores cuánticos comerciales, los wearables 5G aplicados al ocio, el deporte o la medicina, o los vehículos autónomos para transporte de personas y mercancías.

Estos se incluyen en el último informe que acaba de publicar la firma ABI Research, en el que aparecen las 54 tendencias tecnológica a tener en cuenta para 2020, entre las que se incluyen 19 que, casi con total seguridad, no verán la luz el año que viene. Todo este avance de tecnologías generará nuevos desafíos para las organizaciones, que deberán racionalizar y enfocar bien sus esfuerzos para sacar partido de las nuevas tecnologías.

En opinión de Stuart Carlaw, director de investigación de ABI Research, "Después de un tumultuoso 2019 que estuvo plagado de muchos desafíos, tanto integrales a los mercados tecnológicos como derivados de la dinámica del mercado global, 2020 parece ser igualmente desafiante". Por ello, afirma que "triunfar en tecnología en el próximo año es importante para los usuarios finales, implementadores y proveedores, para lo que deberán gestionar adecuadamente sus inversiones o enfocar sus estrategias".

Entre las tendencias tecnológicas que probablemente no se materializarán el año que viene destacan la llegada de los wearables 5G, la computación cuántica comercial, los televisores 8K o los camiones autónomos, y otros factores como la consolidación del mercado de IoT o que la computación Edge logre superar a la nube. En cuanto a dispositivos 5G, el año que viene sí se comenzarán a expandir los terminales móviles con esta tecnología de comunicaciones, pero no así otras categorías de dispositivos como los wearables de consumo y para aplicaciones profesionales. Según los expertos, esto no se producirá hasta más o menos el año 2024.

Por su parte, la computación cuántica también está llenando muchos titulares, pero más allá de algunos avances en procesadores y equipos de ciertos proveedores como IBM o Google (y unos pocos más), las tecnologías de computación cuántica solo estarán al alcance de muy pocos durante el año que viene, y por supuesto la informática cuántica comercial no llegará hasta dentro de unos años. En el ámbito del transporte autónomo, por mucho que los fabricantes y las empresas de sectores como la logística se afanen en fomentar la idea de que esta tecnología ya está aquí, la realidad es que aún falta tiempo para que se puedan ver camiones o autobuses autónomos circulando por las carreteras y las ciudades.

El resto de las tendencias tecnológicas que los expertos de ABI Research han descartado de cara al año que viene, como la consolidación del mercado de plataformas IoT o la supremacía de la computación perimetral frente a la nube, podrían o no materializarse, pero desde luego no el año que viene. La gran diversificación de proveedores y servicios en ambos campos dificulta por ahora el proceso, y de momento los analistas no logran estimar con más precisión cómo se desarrollarán las cosas en el futuro cercano.

MÁS INFORMACIÓN

ABI Research

Cuando la empresa se extiende,
los riesgos de seguridad también.

Si tus socios no tienen
la protección adecuada
y tu sistema sigue vigilando
los puntos vulnerables de siempre,
el objetivo del ataque será
el que menos esperas.

SAP Gold Partner

SAPSecure

Aumenta la protección de tu empresa,
protegiendo el centro de tus procesos
de negocio: el ERP.

Sothis

www.sothis.tech

Tendencias TI 2020, visionando el futuro

¿Qué tendencias tecnológicas serán imprescindibles en el nuevo año? ¿Cuáles de ellas tendrán un mayor impacto en nuestros negocios? ¿Qué retos traen consigo? ¿Qué beneficios? Para arrojar luz sobre estas cuestiones, Micro Focus, GMV, Sothis y F5 Networks participaron en un debate, retransmitido online, sobre esas tendencias tecnológicas que están dirigiendo el día a día de los negocios. Las estrategias de cloud híbrida se posicionaron como el sustento de la TI empresarial; la ciberseguridad se reveló como hilo conductor de toda estrategia tecnológica; y la Inteligencia Artificial resultó ser el gran paso que dar, si no en este 2020, en los próximos años.

Luis Colino, Director de Preventa para España y Portugal de Micro Focus; Juan Rodríguez, Director General de F5 Networks; Ángel Gavín, Business Partner en GMV; y Catalina Jiménez, directora general de la Unidad de Negocio de Consultoría y Sistemas de Información en Sothis, se reunieron bajo el título de la mesa redonda "Tendencias TI 2020, visionando el futuro", para analizar el estado de las estrategias digitales en las empresas españolas y avanzar cómo se están desarrollando los diferentes planteamientos a nivel tecnología (y negocio) que se están asentando en el mercado.

Situémonos, para empezar, en el punto de partida: 2020, año que será, a priori, definitivo para muchas empresas en su camino a la digitalización. En este contexto, la pregunta surge casi de forma automática: ¿se ha acelerado en los últimos meses la transformación? Luis Colino abrió fuego: "Desde Micro Focus sí creemos que todas las empresas han empezado el proceso. Al menos eso dicen, si bien luego no es tan

ENCUENTRO IT TRENDS: TENDENCIAS TI 2020

"Las tecnologías de IA y machine learning empiezan a ayudar a automatizar todos los procesos de monitorización y gestión, pero recordemos que estos dispositivos abren nuestras organizaciones a nuevos ataques"

Luis Colino, Micro Focus

sencillo. Pero ahora mismo es natural hablar de DevOps, de agilidad, de IoT o de Inteligencia Artificial, lo que indica que la tendencia es clara y que la gente no quiere perder ese tren".

Juan Rodríguez opinó igualmente, aunque recalcó que "aún estamos empezando". "El cambio al digital no es sólo tecnológico, sino operacional y de talento. Cada empresa empieza por donde ve más conveniente", razonó. Una cuestión que Ángel Gavín denominó "cultura de la organización", y que relacionó estrechamente con "las infraestructuras actuales".

Catalina Jiménez se mostró muy de acuerdo con sus compañeros en lo tocante a esta primera pregunta. Para ella, "la transformación digital no es un hito, sino un proceso en el que las empresas entienden que una vez iniciado no hay vuelta atrás, por lo que vas a estar forzado a una constante actualización". Y señaló al tejido empresarial como punta de lanza del cambio: "La Administración aún sufre los coletazos de la crisis, pero la empresa sí ha comenzado a moverse, algo que se nota en el mercado".

Un ritmo algo desigual en una agenda digital, sin embargo, continua e inevitable para todos, que tiene a la nube como el pilar sobre el que se van a sustentar las nuevas tecnologías, pues, como afirmó Juan Rodríguez, "la situación del Cloud es real". "Hoy la tendencia es un entorno híbrido, de modo que podemos ir a muchos entornos cloud dependiendo del modelo de negocio", aseguró.

Este panorama "múltiple" genera interesantes retos. El representante de F5 Networks señaló dos. Por un lado, la dificultad para dar pasos atrás después de marchar a Cloud, ya que muchas veces "hay multitud de herramientas para migrar cargas de trabajo a la nube, pero no hay posibilidad de retorno". Por otro, la visibilidad de la gestión, ya que "cuando uno lee la letra pequeña de los contratos, ve que el tema de la seguridad y la gestión es compartida". "Uno cree que cuando migra a la nube se lo van a hacer todo, y no es así. Estás obligado a compartir riesgos", adujo.

A estos dos factores, Ángel Gavín añadió la ciberseguridad: "Cuando te mueves a entornos nuevos y cambias de proveedor se revela un nuevo componente, que es transversal. Por eso, antes de movernos debemos preguntarnos qué vulnerabilidades podemos tener". Una tesitura que llevó a Catalina Jiménez a defender como fundamental la estrategia: "Es esencial para los clientes tener claro el camino multicloud que van a transitar, porque tratamos con varios proveedores, pero actualmente no tenemos todas las herramientas que podrían permitirnos la versatilidad necesaria en ese proceso", dijo.

UN EXTREMO GENERADOR DE DATOS QUE GANA PROTAGONISMO EN LA TI EMPRESARIAL

Aclarados los puntos más candentes del centro, pasamos al extremo, pues se estima que para

2023 habrá 44.000 millones de dispositivos conectados a Internet. ¿Cómo va a impactar IoT en el resto de las infraestructuras de TI? Ángel Gavín fue el encargado de empezar la ronda de respuestas. Según el Business Partner de GMV, "lo importante son los datos". "Hay que entender cuáles son beneficiosos para nuestro negocio y cuáles no, pues no se trata de acumular información por acumular", aseveró.

Catalina Jiménez, puso el acento en "una capacidad cada vez mayor de almacenamiento y de cómputo que nos obliga a saber qué dispositivo tenemos, qué dato vamos a tener y en qué parte de la cadena lo voy a gestionar". Además, trajo a colación el 5G, pues, según la representante de Sothis, "si son fundamentales las comunicaciones, también lo es que sea viable que esa multitud de dispositivos conectados puedan transmitir información a la vez".

Luis Colino, a la importancia del dato, le sumó la de las operaciones y la seguridad. "Creo que TI tiene un reto importante, y las tecnologías de IA y machine learning, que empiezan a ayudar a automatizar todos los procesos de monitorización y gestión, son claves, pero recordemos que estos dispositivos abren nuestras organizaciones a nuevos ataques", argumentó.

"Nosotros, desde F5, vemos dos vertientes", comentó Juan Rodríguez. "Una es la infraestructura pura, como 5G o los CPDs, que van a ser llevados al extremo con todos sus datos. Otra es la parte de los dispositivos, donde vemos dos grandes diferencias. La primera está relacionada con industria, que se está consumiendo en modo servicio. La otra es la parte del consumidor, que cada vez va a tener más elementos inteligentes a su disposición. Será fundamental proteger estos dispositivos en un futuro", sentenció.

Un cambio de paradigma que repercutirá, obviamente, en los negocios; contexto en el que vuelve a destacar, cómo no, la seguridad. Así lo explica Catalina Jiménez: "Nosotros, en Sothis, tenemos una concienciación muy grande con la gestión de los datos y la información. Para que ésta sea efectiva es vital garantizar la seguridad. La información la clasificamos en base a su criticidad, lo que genera un mapa que nos ayuda a saber cómo almacenar la información de la mejor manera. Algo especialmente importante en un ámbito multicloud".

Luis Colino, por su parte, explicó que, para su compañía, el ciclo de vida del dato es un todo. "Desde su captura, que nos permite inocular información en nuestra base de datos, al tratado y securización, todo debe formar parte de la cadena, y va incluido en nuestras soluciones. A lo que hay que sumar la parte de la que nadie habla: disaster recovery. ¿Qué hacemos cuando realmente nos han atacado? Hay que garantizar el backup lo más rápido posible", aseveró.

"Hace años algunos se veía IA como un lujo, pero hoy es una necesidad. O estás ahí, o vas a desaparecer en cuestión de nada, casi por puro darwinismo"

Ángel Gavín, GMV

“Una capacidad cada vez mayor de almacenamiento y de cómputo nos obliga a saber qué dispositivo tenemos, qué dato vamos a tener y en qué parte de la cadena lo voy a gestionar”

Catalina Jiménez, Sothis

En este contexto, Juan Rodríguez recordó que “los dos principales assets son la aplicación y el dato. Sin embargo, el panorama está cambiando: ya no tenemos únicamente aplicaciones monolíticas. Están en diversos ámbitos y no sabemos qué es lo que hace cada una. Lo que nosotros proponemos es hacer visible la trazabilidad de esas aplicaciones. La posibilidad de que tu aplicación escale, la tengas securizada en cualquier lugar y puedas cambiar desde el código tradicional monolítico a un entorno de veinte líneas que puedes compartir entre diferentes departamentos nos parece el gran reto”, expuso.

Ángel Gavín coincidió con todas estas opiniones, pero subrayó la importancia de la moral: “Yo creo que hacia la ética también nos vamos a mover. No todo es posible. Si vamos a usar un software o una aplicación para contratación de personal, es importante que no haya un sesgo en los datos. En GMV tenemos experiencia en datos médicos, que son muy sensibles. Ese dato pasa por un gabinete deontológico que señala si lo que se quiere hacer sobre esa información es o no factible”.

Un futuro disruptivo en el ámbito de las aplicaciones que precisa de un componente moral acaso peleado con la velocidad a la que todo se va a producir si nos atenemos a la opinión de Catalina Jiménez, quien aseguró que “la gran ruptura en el desarrollo de software vendrá dada por la velocidad para cerrar el ciclo del dato”. “El futuro va a ser muy disruptivo en el desarrollo de aplicaciones. Pasaremos de procesos manuales a otros mucho más automáticos donde va a ser esencial la interacción del desarrollador con el usuario final para que los tiempos de producción se vuelvan muy cortos”, explicó la portavoz de Sothis.

Al hilo de esta reflexión, Rodríguez, de F5, agregó que “en dos o tres años los datos de nuestras aplicaciones dependerán de terceras empresas, lo que implica un grado de seguridad muy alto que no todas las compañías aún entienden”. Mientras que Luis Colino, de Micro Focus, sostuvo que “el problema principal de las organizaciones es la escalabilidad, ya que la mayoría de los negocios tienen un background que no es fácil de agilizar”.

OBJETIVO: INTELIGENCIA ARTIFICIAL

Entonces, ¿cómo abrazar una IA que, para 2022, se postula como la principal iniciativa de transformación de IT? ¿Hay razones para que las organizaciones estén preocupadas ante la llegada de la automatización de los procesos? Colino se muestra tajante: “El tema no es si están o no preocupadas, es que lo necesitan. Hoy ya hablamos de tendencias que hacen imposible el trabajo manual tradicional. ¡Hasta la seguridad de la empresa pasa por la Inteligencia Artificial!”.

“La posibilidad de que tu aplicación escale, la tengas securizada en cualquier lugar y puedas cambiar desde el código tradicional monolítico a un entorno de veinte líneas que puedes compartir entre diferentes departamentos, es el gran reto”

Juan Rodríguez, F5 Networks

En esa misma línea se movió Gavín, de GMV, cuando aseguró que “hace años algunos se veía IA como un lujo, pero hoy es una necesidad”. “O estás ahí, o vas a desaparecer en cuestión de nada, casi por puro darwinismo. Hoy es ridículo hacer trabajos que una máquina hace mejor que un hombre. Ese capital humano se puede invertir en otras labores”.

Por último, ¿qué tendencias marcarán definitivamente 2020? Según Catalina Jiménez, “la movilidad en el trabajo, que hará al empleado más eficiente, la IA, la gobernanza del dato, la seguridad y el desarrollo de aplicaciones orientadas al entorno multicloud”. Para Luis Colino y Ángel Gavín la clave será IA, si bien el primero también menciona la robotización y el segundo apuesta por Everything as a Service. Y Juan Rodríguez, por su parte, afirma que veremos cómo “el departamento IT se va a acercar al negocio, incluso tomando decisiones que afectan a la empresa”.

Accede aquí a la grabación de este debate, y escucha cómo ven el futuro tecnológico Micro Focus, GMV, Sothis y F5 Networks. ■

MÁS INFORMACIÓN

- Tendencias TI 2020, visionando el futuro
- Informe IT Trends 2020

INFORME IT TRENDS 2020, EL AÑO DE LA CONSOLIDACIÓN DIGITAL

2020 se presenta como el año de consolidación para muchas de las estrategias de digitalización puestas en marcha por las organizaciones. Esta nueva edición del Informe IT Trends muestra la realidad digital de la empresa y sus planes de inversión y despliegue tecnológico en 2020. Según esta encuesta, seguridad y cloud serán las principales áreas de inversión en TI durante 2020Descubre otros datos en el informe.

Si te ha gustado este artículo, compártelo

IMPULSANDO LA INDUSTRIA 4.0
NUEVOS RETOS, NUEVAS SOLUCIONES

Fabricación Aditiva

Big Data

INDUSTRIA 4.0

Cloud Computing

Sistemas Ciber-físicos

CIBERSEGURIDAD

AUTOMATIZACIÓN

DIGITALIZACIÓN

Ciberseguridad

Visión Artificial

Internet of Things

Robótica

Simulación

www.gmv.es

gmv®
INNOVATING SOLUTIONS

Diálogos it TRENDS

"Apostamos por el modo híbrido: conocer la mejor arquitectura para cada carga de trabajo", Jorge Lorenzo, HPE

"Las tendencias tecnológicas en 2020 vendrán marcadas por la necesidad de ser más eficientes y productivos", Catalina Jiménez, Sothis

"Cada vez funcionan mejor las amenazas híbridas" , Josep Albors, ESET

"Homogeneizar y simplificar son las claves para aprovechar la nube pública", Alejandro Solana, Nutanix

Automatizar. Hoy mejor que mañana…

José Antonio Fernández,
Responsable de servicios Hybrid IT de HPE Pointnext Services

Si yo fuera el CIO de una compañía donde las infraestructuras y los recursos de IT estuvieran medianamente consolidados, y me preguntaran: ¿Cuál es tu propuesta de prioridades de inversión en IT para el año que viene? Mi respuesta sería rápida y contundente: Automatización, sin lugar a dudas. Y como CIO, no solo lo diría yo, lo dicen las grandes consultoras del sector. Así, Gartner, vaticina en su informe de predicción de 2019 que para el año que viene, más del 50% de las tareas manuales en los servicios gestionados de infraestructura, serán reemplazados por servicios automatizados. Igualmente, Forrester en otro estudio reciente, indica que en casos reales de implantación agresiva de automatización, el ROI obtenido fue superior al 140%, siendo su periodo de retorno menor a 3 meses. Es decir, ya sea porque es el área donde mejor rentabilizar las inversiones de IT, ya sea porque es una "oleada tecnológica" inminente, en la que hay que estar preparados, o sea simplemente por usar todas las funcionalidades que nos ofrecen las nuevas tecnologías en hardware y software que adquirimos, la automatización es la apuesta ganadora.

Ahora bien, automatizar está bien, pero y ¿Orquestar? Porque orquestar es otro nivel. Pasamos de las tareas, las acciones, los scripts, los ficheros de comandos a los procesos, a la toma de decisiones, a la coordinación, a los flujos, y eso es harina de otro costal. Pero está claro que, acciones de este tipo a mayor nivel, conllevan mayores beneficios a medio y largo plazo.

Y una vez que nos decidimos por automatizar (y también orquestar), viene el siguiente dilema: ¿Cuánto control quiero tener sobre todo ello? O dicho de otra manera, ¿Cuánto control sobre mi IT estoy dispuesto a perder en aras de conseguir automatización y orquestación de manera rápida? Si no me preocupa y tengo suficientes grados de libertad (es decir, puedo cambiar o adaptar parte de mis flujos y procesos internos), ahí tenemos

“¿Cuánto control sobre mi IT estoy dispuesto a perder en aras de conseguir automatización y orquestación de manera rápida?”

la oferta de Cloud Pública, el “pack” de automatización, a diferentes niveles y en diferentes áreas. Dependiendo del tipo de servicio consumido, deberemos integrar y orquestar esta parte externa, con el resto de mi IT, también de forma automática.

Pero si esto no es así, si los procesos o “workflows” de mi compañía son un activo de valor, sobre los que debe haber un control integral, tendremos que empezar a pensar en automatizar y orquestar de otra forma, de manera interna. Y aquí entran en juego conceptos fundamentales a tener en cuenta desde el mismo comienzo de la iniciativa de automatización: Estrategia, Metodología, Roadmap, Esponsorización, Herramientas, Industrialización, Cultura de automatización, Gestión del cambio, Monitorización y KPIs,...y si todo esto se complementa con un compañero de viaje con experiencia y conocimiento real en la materia (lo que se denomina “socio tecnológico”), el camino será más fácil. Y eso es lo que ofrecemos desde HPE Pointnext Services. Una aproximación holística e integral para automatizar.

Si quieres o necesitas empezar en la automatización: Hoy mejor que mañana. ■

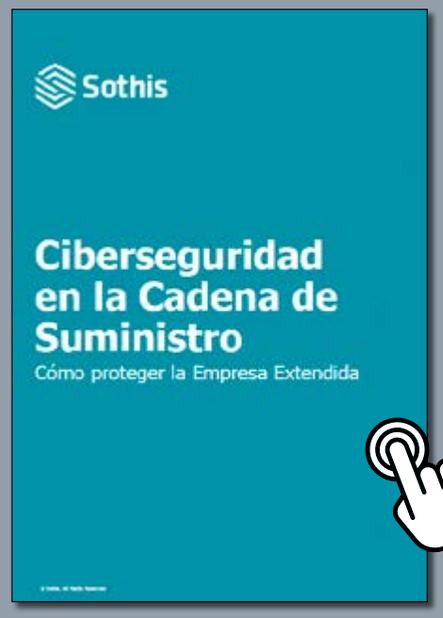
GESTIÓN DE DATOS PARA LA EMPRESA INTELIGENTE

CIBERSEGURIDAD Y PYMES: EL NUEVO ESCENARIO

10 BENEFICIOS DEL ESCRITORIO COMO SERVICIO (DAAS)

CAPACITAR A LOS USUARIOS FINALES Y OFRECERLES MEJORES EXPERIENCIAS

CONVIERTE LOS DATOS EN OPORTUNIDADES DE NEGOCIO CON UNA PLATAFORMA DE DATOS INTELIGENTE



CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO: CÓMO PROTEGER LA EMPRESA EXTENDIDA

it whitepapers

it TRENDS

2020, el origen de la década inteligente

Emilio Castellote,
analista Senior,
IDC España

Comienza el 2020 y con él una nueva década; es momento de reflexionar y preguntarnos cómo van a ser esos cambios, cómo hemos llegado hasta ellos y a qué velocidad. Sin duda alguna, esas tres preguntas cuentan con el denominador común de la tecnología. En las últimas dos décadas, la irrupción de la tecnología en nuestras vidas ha modificado todo tipo de hábitos que van desde la forma en la que accedemos a la información, pasando por la forma en la que nos relacionamos y la manera en la que consumimos.

Todo ello ha motivado unos cambios muy significativos en los modelos de negocio de cualquier empresa, independientemente del sector al que se dedicase. Cambios que nos han llevado a acometer planes de transformación digital desde finales de esta última década 201x para afrontar el 2020 y la nueva década desde una parrilla de salida muy globalizada, con enfoque en la explotación del dato, priorizando las necesidades particulares de cualquier cliente y entregando valor a través de unos servicios que deben ser, ante todo, inmediatos y personalizables.

Quizás antes de abordar ese pistoletazo de salida de la nueva era digital es importante reflexionar sobre la velocidad de esos cambios que hemos vivido en las dos últimas décadas. Y es que, a veces, tirar de recuerdos nos hace tomar conciencia de situaciones pasadas para aprender de lo que nos viene en este futuro hiperconectado inmediato.

Recordemos que la década de los 90 debía ser aquella que alumbraría el acceso a Internet, recordemos los primeros buscadores exitosos como Yahoo! que aparecieron sobre 1994 (quizás un ejemplo de reflexión sobre la transformación digital que estamos viviendo ahora mismo) e incluso el famoso Internet Explorer de Microsoft que nacía embebido en Windows 95 (y que ha visto su fin de vida recientemente en 2015), recordemos cómo a finales de esa década de los 90 llegaban a España las primeras tarifas planas y acceso a Internet a través de ADSL a velocidades “vertiginosas de la época” de apenas 512kps. Sí, podemos afirmar que la década de los 90 fue la década de la aparición de Internet y el detonante del cambio social e industrial que se nos venía encima.

Debimos todavía superar el catastrófico efecto 2000 (que quedó afortunadamente en miedo

“Tirar de recuerdos nos hace tomar conciencia de situaciones pasadas para aprender de lo que nos viene en este futuro hiperconectado inmediato”

mediático) para entrar en una nueva década que supondría la aparición de redes sociales de todo tipo que modificarían la forma de comunicarnos y relacionarnos. Y es que hay que recordar que el ahora omnipresente Facebook nacía en 2004, y que deberíamos esperar a finales de esta década para ver el nacimiento de Instagram o WhatsApp. Si algo hemos de recordar de esta década de los 2000 es que el modelo de comunicación se elevaba al plano online y la comunicación con el usuario se convertía en un modelo síncrono y con necesidad de respuesta inmediata, al tiempo que el Cloud empezaba a consolidarse como la plataforma de alojamiento de aquellos primeros servicios web que poco a poco irían transformando el escenario corporativo.

Y por fin llegó la década del 2010 que acabamos de terminar donde, si hay algo que marcó la diferencia, fue la optimización de la red móvil y sus capacidades de transmisión de datos. Esta ha sido la década de la movilidad con la llegada del 3G, pasando al 4G y llegando al nacimiento del 5G.

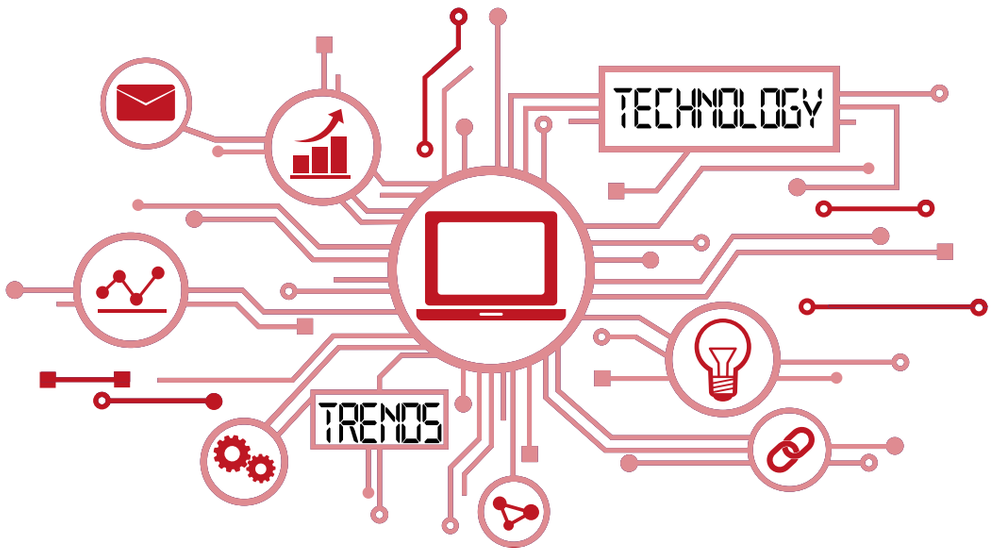
La movilidad ha supuesto el catalizador de los nuevos modelos de negocio digitales, de la hiper-conectividad entre usuarios y empresas y la consolidación de un modelo de relación vinculado al concepto de experiencia de usuario que tanto se afanan organizaciones de todo tipo por optimizar y consolidar antes de la llegada de la nueva década que comienza en 2020. Sin duda alguna acabamos ésta con todos los ingredientes necesarios para dar lugar a una verdadera revolución industrial y social.

¿Y qué nos depararán entonces el 2020 y los años venideros? Estamos ante el comienzo de una nueva década que seguramente recordaremos dentro de 10 años como la de la inteligencia artificial. Una década que debe transformar el modelo industrial hacia un modelo de servicios personalizables a demanda, donde los modelos tradicionales B2B (Business to business) y B2C (Business to customer) deberán converger y transformarse en B2Me (business to me). Esta será la década que probablemente recordaremos como de mayor impacto en el tejido empresarial (rememoramos a todos aquellos que ya han desparecido en los últimos años por no ver el cambio que se les venía encima) y todo ello nos conducirá a un nuevo mercado donde más del 50% de las nuevas profesiones de esta nueva década están todavía por crearse.

Pensemos por lo tanto en cuánto hemos vivido en las dos últimas décadas y cómo la tecnología aceleró esos cambios, y decidamos cómo queremos transformarnos nosotros mismos para la década inteligente que está a punto de comenzar. ■

Encuentros IT Trends

Las tendencias TIC para
la empresa digital de la mano
de los líderes del sector



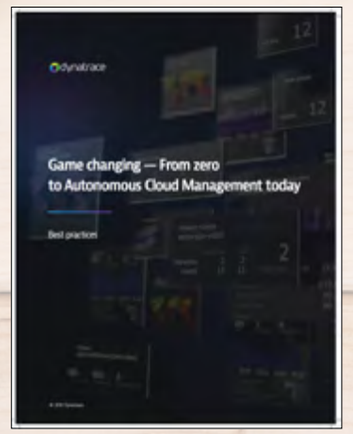
Reducir las vulnerabilidades, mejorar la seguridad de la red, hacer uso de automatización y otros procesos que mejoren la eficiencia, o aumentar la privacidad y el cumplimiento de los datos son algunos de los objetivos que las empresas deberían marcarse de cara al próximo año para mejorar la seguridad.

Estos objetivos deberían hacer frente a tendencias como el ransomware, el mayor uso de los móviles como vector de ataque, nuevas regulaciones, el creciente impacto de la Inteligencia Artificial y el Machine Learning o las amenazas contra las infraestructuras críticas.

Únete a nosotros en este **Encuentros IT Trends sobre Ciberseguridad en 2020** 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 2020. **29 de enero · 11:00 AM**

¡Regístrate ya!

La documentación TIC, a un solo clic

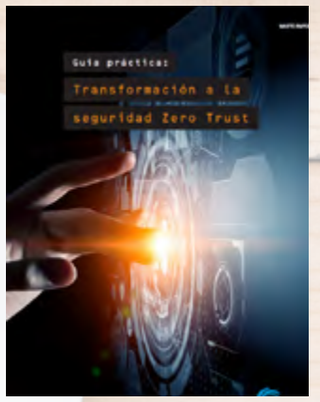


Cambio de juego: cómo lograr una gestión autónoma de la nube

En el mundo digital actual casi todas las empresas son compañías de software, y la mayoría de las organizaciones buscan formas innovadoras de crear nuevos productos o identificar modernas maneras de operar para ser más competitivos. Dynatrace es una firma que vio el cambio digital desde el principio y pasó de entregar software a través de un modelo tradicional on premise, al innovador modelo híbrido-SaaS.

Caso de uso:
Codere ahorra un 27% de su gasto en Azure con Cloud Economics de Crayon

La compañía energética CenterPoint Energy está aprovechando la innovación, incluyendo cosas como contadores y redes inteligentes, para mejorar la calidad de sus servicios de energía. Sin embargo, los sistemas IoT y las transacciones complejas con los clientes generan cantidades enormes de datos, parte central de su estrategia, operaciones e, incluso, identidad.



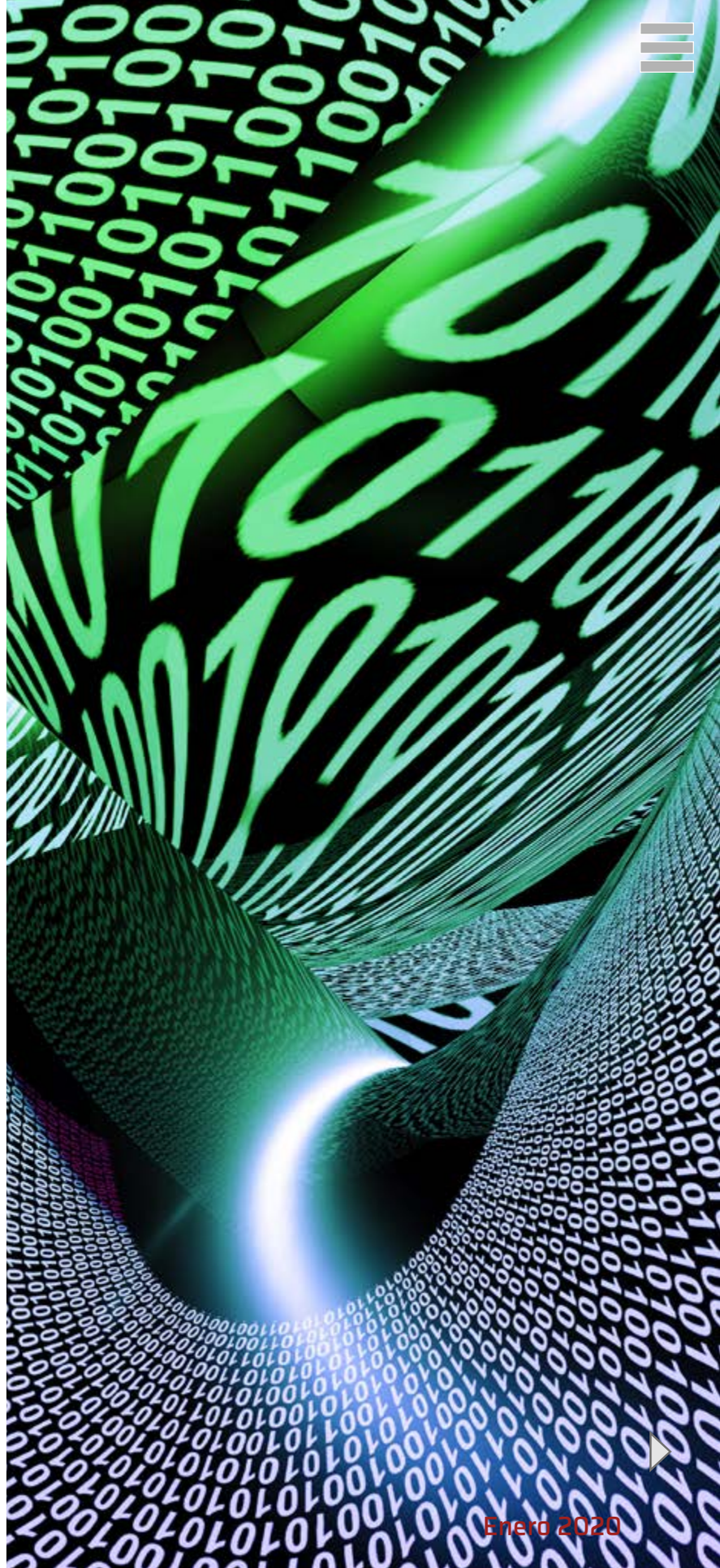
Transformación a la seguridad Zero Trust

La noción de un perímetro de red, en el que todo el que está fuera de la zona de control de la empresa es malicioso y todo el que se encuentra dentro es honesto y bienintencionado, no es algo en lo que se pueda confiar en el panorama empresarial actual. La amplia adopción de aplicaciones SaaS, la migración a arquitecturas basadas en la nube, un número creciente de usuarios remotos y un flujo cada vez mayor de dispositivos BYOD han convertido la seguridad perimetral en irrelevante.

Cómo el análisis de datos incrementa el valor del negocio y aporta ventajas competitivas

Todas las empresas se encuentran inmersas en procesos de transformación digital, y la red es un elemento fundamental para el éxito. Las organizaciones modernas exigen agilidad y conectividad ininterrumpida, y la red es hoy día el facilitador de cualquier iniciativa digital donde el análisis de datos se ha convertido en un componente absolutamente crítico. Este documento expone cómo las organizaciones que incorporan análisis de datos en su actividad consiguen mejores resultados; con ejemplos prácticos de los sectores de educación, retail, entretenimiento y sanidad.

El ransomware: ese gran enemigo que ha ganado visibilidad con la Ley de Protección de Datos



El ransomware es un malware que puede causar un gran perjuicio económico a una empresa y, sobre todo, puede arruinar su reputación. Con la normativa europea de protección de datos o RGPD, las compañías están obligadas a hacer públicos estos ataques por lo que ahora se sabe más de ellos. Y aquellas firmas que sean víctimas, también se enfrentan a grandes multas.

Bárbara Bécares

Se habla más del ransomware que nunca antes en la historia. Por un lado, el ataque WannaCry, la mayor brecha conocida dentro de este segmento y del que se conoció por primera vez en mayo de 2017, le dio visibilidad. Y por otro lado, el Reglamento General de Protección de Datos (RGPD), la legislación europea que busca proteger las informaciones de los ciudadanos por diversos frentes, ha hecho el ransomware más visible que nunca antes.

Recuerda la Agencia Española de la Protección de Datos que una de las medidas en las que se materializa el principio de responsabilidad activa del RGPD es en la obligación de notificar las brechas de seguridad a la autoridad de control, a menos que sea improbable que la quiebra suponga un riesgo para los derechos y libertades de los afectados, dentro de las 72 horas siguientes a que el responsable sea consciente de que el hecho se ha producido.

Además, en los casos en que sea probable un alto riesgo para los derechos o libertades de los afectados, también se les deberá comunicar la brecha a estos. El objetivo de la comunicación a los afectados es permitir que puedan tomar medidas para protegerse de las consecuencias. Destaca que un 10% de las notificaciones de brechas de seguridad recibidas en la AEPD durante 2018 desde el 25 de mayo de 2018 (fecha de aplicación del RGPD) indican que el motivo de la brecha es el cifrado de equipos mediante algún tipo de ransomware, y en ocasiones el vector de ataque es el acceso mediante servicios de escritorio remoto.

En las siguientes líneas, con Eusebio Nieva, director técnico de Check Point en España y Portugal; Alexis de Pablos, director técnico de Veeam para Iberia; Guillermo Fernández, senior sales engineer Southern Europe de WatchGuard Technologies; y José de la Cruz, director técnico de Trend Micro

RANSOMWARE, ¿SABES LO QUE ES? **CLICAR PARA VER EL VÍDEO**

Los ataques de ransomware han pasado a formar parte de uno de los principales riesgos que cualquier ciudadano o empresa confronta

Iberia tiene la oportunidad de aprender más sobre ransomware poder hacerle frente.

¿Cómo ataca el ransomware?

Para empezar, recuerda Alexis de Pablos desde Veeam que “un ataque de ransomware es normalmente un intento de extorsionar a una organización al negarle el acceso a sus datos. Ransomware es un subconjunto de malware, un término colectivo para todas las formas de código malicioso, incluidos virus informáticos y gusanos”. Y Eusebio Nieva, director técnico de Check Point en España y Portugal añade que, para conseguir su objetivo, que suele ser pedir un rescate por una información secuestrada, “esta variante de virus informático se instala de forma silenciosa en dispositivos móviles, y ordenadores de todo tipo, y una vez se pone en acción cifra o encripta todos los datos para bloquear el acceso a ellos sin la contraseña que permite descifrarlos”.

"Al daño para la imagen de la empresa y su reputación, y al coste que tiene para la empresa interrumpir su actividad, se suma el hecho de que quizás, si no cuentan con un plan de contingencia la compañía puede incluso verse obligada a cerrar por un ataque de este tipo"

Guillermo Fernández, senior sales engineer Southern Europe, WatchGuard Technologies

Tras aclarar algo tan básico, lo primero para cualquier responsable de TI es saber por dónde llegan estas temidas amenazas. Así será más fácil tener en cuenta qué no perder nunca de vista. “Según los datos de nuestro último Índice Global de Amenazas de septiembre de 2019, el ransomware que más estaba afectando a las empresas en nuestro país era DarkGate, una amenaza compleja que se instala de forma silenciosa. Este troyano, que ha afectado a más del 8% de las empresas españolas, provoca problemas operativos e incapacidad para ejecutar ciertos servicios o aplicaciones”, explica Eusebio Nieva desde CheckPoint España.

Por su parte, Guillermo Fernández de WatchGuard advierte que, de momento, “la fórmula más extendida de ataque de ransomware es a través de los correos electrónicos de phishing”. Por lo general, siempre hay un usuario que recibe un correo con un enlace al que el usuario accede, y es precisamente ese enlace el que produce la infección, advierte el experto.

Y añade este directivo que “otra variante empleada en los ataques de ransomware consiste en utilizar vulnerabilidades ya descubiertas, y que por tanto deberían estar ya parcheadas en los sistemas, por ejemplo un servidor web que tiene una vulnerabilidad y la gente se conecta a ese servidor web, o bien casos en los que los usuarios tienen servidores terminal server y los tienen publicados en Internet –cuando esto nunca deberían hacerlo sin protegerse antes detrás de una VPN- y son víctimas de un ataque de fuerza bruta para descubrir

"Es esencial cambiar el enfoque en materia de protección, dejando atrás una actitud reactiva para pasar a implementar un enfoque mucho más proactivo"

Eusebio Nieva, director técnico, Check Point España

la contraseña del administrador y como tengan una contraseña fácil, entran y ejecutan el ransomware y cifran ese servidor entero".

Además de esto, José de la Cruz anima a los responsables de TI a no confiarse. Y advierte que realmente no existe un único método de ataque. "Precisamente los atacantes intentan diversificar tanto en los vectores de ataque utilizados (correo, red, dispositivos locales, etc.) como en los métodos empleados (ataques a vulnerabilidades, phising, troyanos, etc.)". A día de hoy, el ataque a vulnerabilidades es un factor importante de riesgo (como único método de ataque o parte del proceso de un ataque global) y parece que, a futuro, esto no va a cambiar demasiado, especifica el directivo de Trend Micro.

¿Qué quiere el ransomware?

Desafortunadamente estos ataques ya han pasado a formar parte de uno de los principales riesgos que cualquier ciudadano o empresa confronta. Ahora bien, cabe tener en mente qué es lo que persiguen. "Persigue un claro objetivo económico, pues el fin del rescate es ese, pagar una cantidad para recuperar los datos", explica Guillermo Fernández, senior sales engineer Southern Europe para WatchGuard Technologies. Y si un ransomware asusta es porque, precisamente, el ciberdelincuente busca causar mucho daño para forzar así a que la otra parte pague el rescate para restablecer la situación.

De hecho, desde la Agencia Española de Protección de Datos explican que en los últimos años han cobrado una especial importancia los ataques de tipo ransomware en los que se busca cifrar información para posteriormente solicitar un rescate por la contraseña de descifrado. "Aunque parezca una actividad en descenso, sigue siendo una gran amenaza a tener en cuenta especialmente en el caso de las pymes, uno de sus grandes objetivos", de acuerdo con un informe del mencionado organismo público.

¿Por qué el ransomware es tan temible?

Es muy importante tener en cuenta que, además del riesgo que puede suponer para una empresa y para cada uno de sus clientes, que un delincuente cibernético se haga con las informaciones privadas, un caso de ransomware puede arruinar todo el prestigio de cualquier marca. Años de trabajo y esfuerzo en publicidad y en buenas prácticas pueden irse por la borda en los minutos en los que un ataque entra en los sistemas de una compañía.

Además de esto, “al daño para la imagen de la empresa y su reputación, y al coste que tiene para la empresa interrumpir su actividad, se suma el hecho de que quizás, si no cuentan con un plan de contingencia la compañía puede incluso verse obligada a cerrar por un ataque de este tipo”, tal y como añade Guillermo Fernández, senior sales engineer Southern Europe para WatchGuard Technologies.

De hecho, quiere hacer énfasis el portavoz de Veeam en que “las empresas que han pensado que su única opción era pagar a los ciberdelincuentes para recuperar sus archivos, no solo han puesto en riesgo su dinero (dado que no hay garantía ninguna de que les devuelvan los datos), sino que además han permitido que se ponga en tela de juicio su reputación (ya que otros delincuentes pueden considerarles un objetivo potencial fácil)”.

Y por si todo esto fuera poco, un ataque de ransomware puede derivar en el incumplimiento de normativas como GDPR y, por tanto, suponer una fuerte sanción para una empresa, como recuerda José de la Cruz desde Trend Micro.

> "El ataque a vulnerabilidades es un factor importante de riesgo (como único método de ataque o parte del proceso de un ataque global) y parece que, a futuro, esto no va a cambiar demasiado"
>
> José de la Cruz, director técnico, Trend Micro Iberia

Ejemplos de casos de ransomware

El ransomware más famoso es Wannacry. Causó muchos problemas y fue el ataque más grande de la historia. Además de que hacerle frente es una tarea muy complicada. De hecho en agosto de este 2019, la telemetría de la firma de seguridad de Sophos detectó 4,3 millones de casos de WannaCry, y el número de variantes observadas fue de 6.963, de las que un 80% eran archivos nuevos. Y además de Wannacry, estos ciberdelitos son frecuentes, no son casos aislados. Recuerda el portavoz de Watchguard Technologies el “reciente caso de ransomware que ha tenido lugar en el Ayuntamiento de Jerez, el cual ha quedado paralizado y ha devuelto literalmente al papel al consistorio”.

Fue a comienzos de octubre cuando el ataque conocido como Ryuk llegó a la ciudad gaditana camuflado a través de un correo electrónico con un adjunto que alguien abrió sin saber que desencadenaría el caos, impidiendo el acceso a archivos alojados en más de 50 servidores y cuyo acceso quedó cifrado. Pero Jerez no fue el único ayuntamiento afectado recientemente. El pasado mes en Euskadi se registraron al menos cuatro denuncias por presuntos delitos de ciberseguridad. Se alertó de una campaña de envíos masivos de correos electrónicos con malware adjuntos en la región, que llevó al Basque Cybersecurity Centre (BCSC) a activar un protocolo de actuación.

Además, en agosto de este año, un informe de Bitdefender concluía que GermanWiper, malware wiper que hacía creer a las víctimas que era un ransomware, tenía una amplia presencia en España. Más recientemente

¿Cómo hacerle frente al ransomware?

Advierte Alexis de Pablos desde Veeam que "no existe la fórmula milagrosa cuando hablamos de protección contra ciberamenazas como ransomware y, por desgracia, en los últimos años las empresas han conocido el impacto de estos ataques. Los ciberdelincuentes saben perfectamente cómo aprovechar las debilidades de los sistemas TI de las empresas, puesto que tan solo hace falta un pequeño agujero en el casco para hundir el barco, un punto de entrada vulnerable puede dejar expuesta a la empresa a ciberataques que la dejen completamente paralizada".

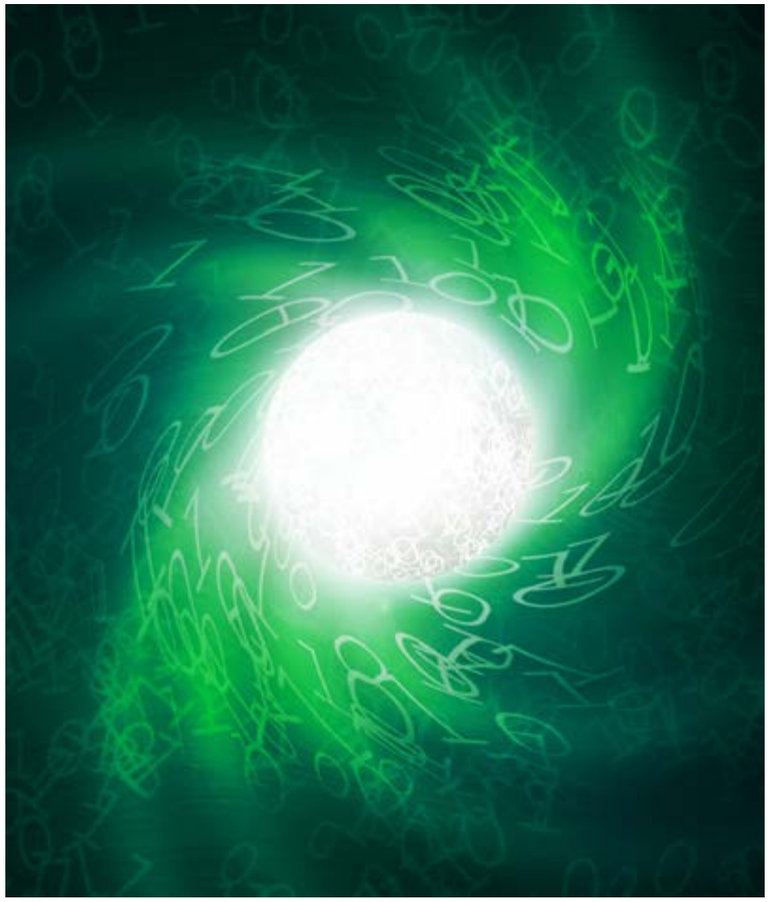
En cuanto a qué decisiones debe tomar un CIO para hacer frente al ransomware, sin duda es clave tener los equipos parcheados, no tener servicios expuestos en Internet innecesariamente y concienciar y formar adecuadamente a todos los usuarios para que sepan actuar de forma correcta y estar educados ante el phishing y, por supuesto, estar preparado actuar ante el peor escenario

"Las empresas que han pensado que su única opción era pagar a los ciberdelincuentes para recuperar sus archivos, no solo han puesto en riesgo su dinero, sino que además han permitido que se ponga en tela de juicio su reputación"

Alexis de Pablos, director técnico, Veeam Iberia

Enlaces de interés...

- Wannacry sigue activo con millones de intentos de infección al mes
- Detectado un repunte del ransomware en el segundo trimestre
- Las mejores configuraciones de firewall para bloquear el ransomware



Es clave tener los equipos parcheados, no tener servicios expuestos en Internet innecesariamente y concienciar y formar adecuadamente a todos los usuarios

y tener un plan de actuación, de acuerdo con las palabras del portavoz de WatchGuard Technologies.

Para el experto de CheckPoint “lo más destacado sería la incapacidad de detectar una amenaza de este tipo y, por tanto, evitar las consecuencias que tiene el convertirse en una nueva víctima de este tipo de ataque. Por tanto, la decisión fundamental que un CIO debe tomar se centra en el modelo de ciberseguridad a implantar en la empresa”. La firma considera esencial que los CIO y responsables de ciberseguridad en general tengan conciencia sobre “la necesidad de cambiar el enfoque en materia de protección, dejando atrás una actitud reactiva para pasar a implementar un enfoque mucho más proactivo, que permita identificar, adelantarse y prevenir las amenazas antes de que estas puedan tener efecto”.

Desde Veeam piden que se les preste especial atención a las copias de seguridad. “La mejor solución ante los ataques que vulneran la seguridad de los datos es la prevención”, dice Alexis de Pablos. “Hay muchas formas de hacer una copia de seguridad externa de los datos, desde discos del sistema y discos duros extraíbles, hasta dispositivos de cinta offline y backups en la nube”. Veeam recomienda su regla 3-2-1: crear tres copias de los archivos más importantes, usar al menos dos medios diferentes y asegurarse de que una copia se almacene siempre fuera de las instalaciones.

Compartir en RRSS

it User
TECH & BUSINESS

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

La seguridad como servicio no cala en la administración pública

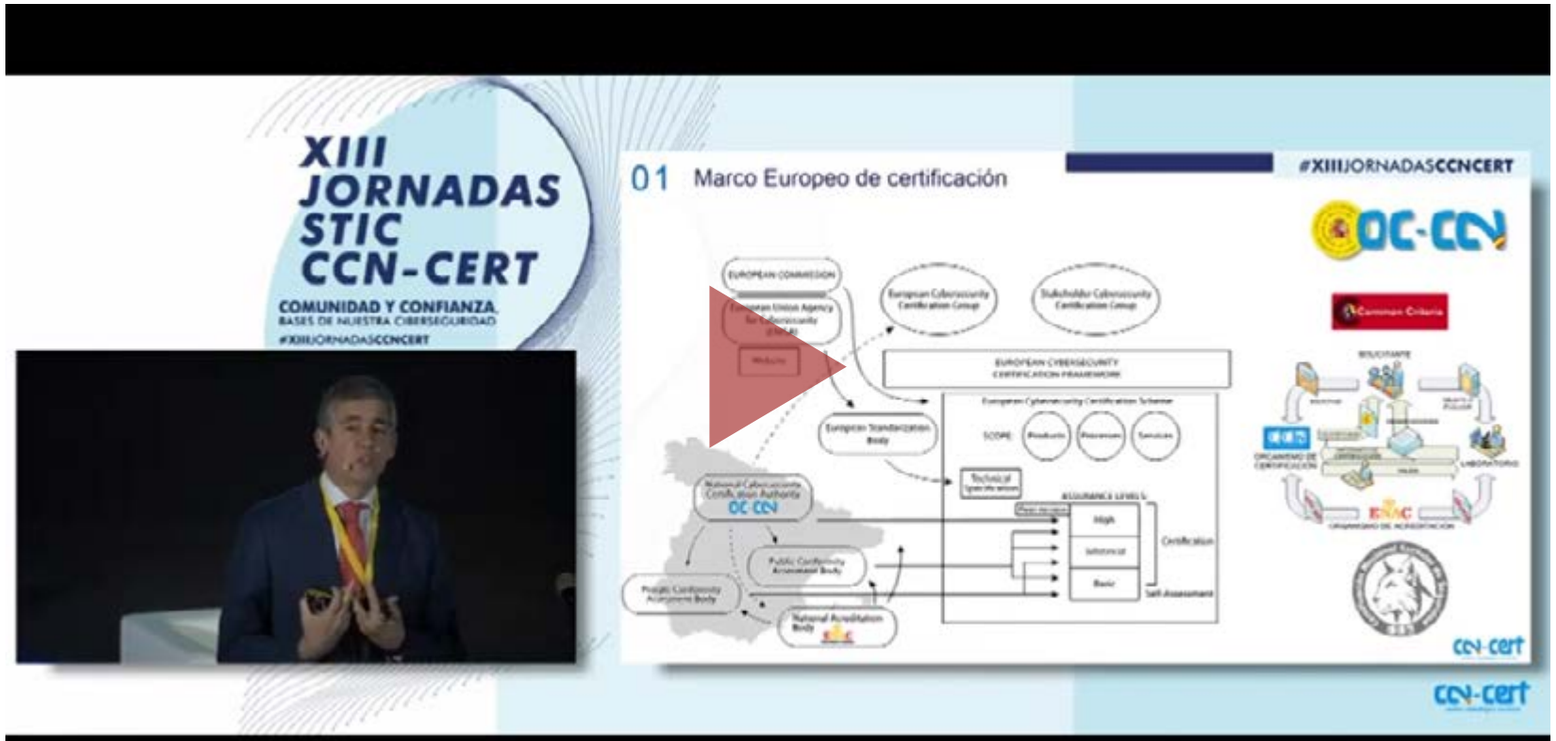
2019 acabó con la celebración de las XIII Jornadas CCN-CERT un evento organizado por el Centro Criptológico Nacional (CCN), Organismo adscrito al Centro Nacional de Inteligencia (CNI), que reunió a más de 3.300 asistentes bajo el lema "Comunidad y Confianza. Bases de nuestra Ciberseguridad".

Más de 130 ponentes de hablaron de amenazas, ataques y retos tecnológicos, de la prevención en ciberseguridad, de operaciones militares en el ciberespacio o de la desinformación y la ciberdelincuencia, entre otros.

La inauguración corrió a cargo de Margarita Robles, ministra de Defensa en funciones, encargada de Asuntos Exteriores, Unión Europea y Cooperación, quién definió la ciberseguridad como “un valor estratégico”, recordó que el ciberespacio es una amenaza para nuestra democracia y que es vital la colaboración entre administraciones y la empresa privada para afrontar estos nuevos desafíos, “ya que es imprescindible tener unidad de acción para garantizar la seguridad en el ciberespacio”.

Javier Candau, jefe del Departamento de Ciberseguridad del CCN, inició su presentación con las novedades en normativas, destacando la nueva Estrategia Nacional de Ciberseguridad, publicada en abril de 2019; y la Cybersecurity Act (EU) 2019/881, cuya misión es fortalecer el papel de la Agencia Europea de Ciberseguridad (ENISA) y crear un marco europeo de certificación.

El jefe de Ciberseguridad del CCN enumeró los principales retos para 2020, haciendo hincapié en la necesidad de crear un modelo distribuido, recalcando que “tenemos todos que colaborar en reducir la superficie de exposición, en la vigilancia continua y en la respuesta eficiente”.



RETOS 2020
(JAVIER CANDAU, JEFE DEPARTAMENTO CIBERSEGURIDAD, CCN)

CLICAR PARA VER EL VÍDEO

También presentó las nuevas soluciones del CCN, como AMPARO y EMMA, esta última clave para conseguir una reducción de la superficie de exposición en las redes. “Los últimos incidentes nos están demostrando que es de vital importancia segmentar las redes”, dijo Javier Candau.

Y aprovechando la presencia de centenares de profesionales de la industria de la ciberseguridad, IT Digital Security lanzó tres preguntas que buscan tomar el pulso a lo que ocurre y cómo mejorarlo

1. **¿Qué está haciendo la administración pública en seguridad?**
2. **¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?**
3. **¿Cuáles son los retos de 2020 a nivel de seguridad?**

Objetivos del Esquema Nacional de Seguridad (ENS)

- **Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.**
- **Promover la gestión continuada de la seguridad.**
- **Promover la prevención detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.**
- **Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las entidades del Sector Público en materia de seguridad de las tecnologías de la información; también aportar un lenguaje común para facilitar la interacción, así como la comunicación de los requisitos de seguridad de la información a la Industria.**
- **Servir de modelo de buenas prácticas, en línea con lo apuntado en las recomendaciones de la OCDE «Digital Security Risk Management for Economic and Social Prosperity - OECD Recommendation and Companion Document».**

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

"La forma de contratar debe valorar más la parte de capacidades y experiencia que la parte de parte económica"

Vidal Valdunciel, Account Manager, A3Sec

1. ¿Qué está haciendo la administración pública en seguridad?

Cuando hablamos de administración pública hay que distinguir entre administración general del estado, comunidades autónomas y entidades locales. Creo que sí son conscientes y sensibles a la importancia de la ciberseguridad en su gestión de datos, de procedimientos, todas la parte de administración electrónica... Pasar de la conciencia a la acción depende del presupuesto, y aún no sabemos cómo está el presupuesto.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

Sí. La forma de contratar debe valorar más la parte de capacidades y experiencia que la parte de parte económica.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

Poner en marcha los planes y medidas que seguro que tienen en torno a la ciberseguridad, para proteger sus activos, sus sistemas de información, y a sus usuarios, clientes y similares. En cuanto a retos generales, seguimos tenido problemas con el ransomware. Y estamos viendo cómo ayuntamientos y empresas potentes están tenidos problema con malware de hace diez años. Es básico dotarse de soluciones, servicios y herramientas que respondan a la realidad de lo que hay ahora con respecto a los ciberdelincuentes.

"Hay que predicar con el ejemplo. Como administración no les puedes pedir a las empresas y usuarios que utilicen dispositivos seguros cuando tú no lo estás implementando"

Belén Pérez Rodríguez, Network and Cybersecurity Engineer, Balidea

1. ¿Qué está haciendo la administración pública en seguridad?

Se están dando pasos. El Esquema Nacional de Seguridad está ayudando mucho y se están en las primeras fases de evaluación, de auditorías y de ver qué es lo que hay. Las administraciones que ya llevan un poco más de tiempo están implementando medidas, pero muchas aún están en fases iniciales de evaluación

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

Sí, hay que predicar con el ejemplo. Como administración no les puedes pedir a las empresas y resto de usuarios que utilicen dispositivos seguros, y que utilicen servicios de forma segura cuando tú no lo estás implementando. Y sólo hay que ver algunos navegadores de algunas administraciones, que para poder acceder te tienes que ir a un versión obsoleta porque sino, no funciona.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

Seguir con el camino iniciado de identificar, evaluar, poner medias de seguridad y luego volver a evaluar. La seguridad nunca duerme, hay que seguir trabajando.

"La forma de consumir y la forma de comprar debe ser producto más servicios, porque sino no vamos a avanzar mucho"

María Campos, VP en Cytomic

1. ¿Qué está haciendo la administración pública en seguridad?

A raíz de las oleadas de ataques en ayuntamientos, diputaciones y diversas entidades se han puesto las pilas un poco más rápido de lo que venía siendo el resto del año, incluso aunque no estamos hablando de ataques nuevos. Esto es lo frustrante, que hablamos del Emoted del 2014. La administración funciona así, con oleadas; sacan los presupuestos extraordinarios que no han tenido durante todo el año. Con la parte de respuesta a incidentes hemos conseguido entrar en organismos a los que se había idoantes pero nunca tenían presupuestos, y que cuando han tenido media administración parada, cuando han salido en las noticias, se han puesto las pilas.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

Totalmente. En la administración es tremendamente alarmante la falta de recursos humanos para gestiona herramientas de ciberseguridad, o para dedicarse a tener una protección y una seguridad más o manos aceptable. Están sufriendo ataques que no son tampoco muy sofisticados pero la tecnología de muchas administraciones está desactualiza, nadie mira la consola, tengo sistemas legacy… y la forma de consumir y la forma de comprar debe ser producto más servicios. Sin esa capa de servicio creo que no vamos a avanzar mucho

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

Yo creo que siempre tenemos tres puntos que nos hace mucho daño, a la administración y al resto de la industria. Por un lado, falta de recursos, por otro, una gran heterogeneidad de herramientas y de productos que no se integran entre sí, y por otro lado la capacidad de sacarle partido a lo que realmente tienes. Vuelvo a lo mismo: si tenemos recursos escasos lo cubrimos contratando servicios, contratando arquitecturas que consoliden mucho más. Si tienes pocos recursos, no te puedes permitir comprar 25 tecnologías diferentes que no eres capaz de integrar. Además, nosotros vemos como un gran reto el comportamiento del usuario, porque hay comportamientos infinitos, y cómo atacar ese tipo de situación.

"La administración pública tiene claro que tanto en procesos como en soluciones tiene mucho que mejorar"

Elena Cerrada, Country Manager, Forcepoint Iberia

1. ¿Qué está haciendo la administración pública en seguridad?

La propia administración pública tiene claro que tanto en procesos como en soluciones tiene mucho que mejorar, pero es cierto que como los procesos son un poco más largos, y suelen ir más a rebufo de lo que es la línea que mueve el mercado de la seguridad, pues ellos se van encontrando con que tienen que ir cubriendo esos huecos. Y tiene una problemática adicional, que es toda la enjundia que supone la propia carga de la administración pública a la hora de ejecutar proyectos, a la hora de tener presupuestos, esa menor agilidad que tienen con respecto a otro tipo de organismos. Y eso es un trabajo que hay que realizar y que tiene que mejorar, pero por supuesto en materia de seguridad se están poniendo las pilas, entienden el valor y la necesidad de esas herramientas a la hora de poder desarrollar sus propios trabajos y en ese sentido creo que estamos todos en el mismo barco. Entienden y valoran la seguridad que podemos aportarles, hace falta que los ritmos se vayan ajustando a esas necesidades. Pero creo que están en la línea.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

Yo diría que el principal problema que tiene la administración pública son los tiempos. Ocurre que cuando quieren sacar un proyecto de seguridad que han diseñado hace dos años, y que de repente están intentando poner en práctica, casi se les está quedando obsoleto. Desde mi punto de vista si se quieres adecuar a los ritmos a los que crecen las amenazas deberían encontrar la manera de agilizarlo. Creo que todo es mejorable y lo pueden hacer. Todos tenemos nuestra parte de mejora, pero creo que ellos son conscientes de esa problemática, que les afecta a ellos directamente.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

Uno de los mayores retos de la administración pública es que son muy sensibles a llevarse temas a la cloud, pero la cloud está ahí. Es un carro al que todo el mundo se va a subir y es un reto para la administración pública el poder identificar qué tiene que llevar a la cloud. Tienen que conseguir configurar su infraestructura y dotarse de las herramientas y de las capacidades necesarias para poder ir a ese cloud, que es un carro al que se tienen que subir sí o sí.

Y como reto de 2020 que nos afecta a todos, yo creo que es alinear la seguridad del dato, que ahora mismo es lo más relevante de nuestra infraestructura, teniendo en cuenta también el comportamiento de los usuarios a la hora de proteger el dato; en base al riesgo que genera ese usuario al acceder a la información podamos controlar y mejorar la seguridad.

"Los sistemas de contratación de la Administración Pública no están adecuados a la forma de contratar que requieren las aplicaciones cloud"

Samuel Bonete, Country Manager, Netskope Iberia

1. ¿Qué está haciendo la administración pública en seguridad?

Siguen atados a los principios de seguridad tradicionales, seguridad perimetral, seguridad endpoint, pero no se dan cuenta de que el mundo en el que estamos es un mundo de transformación digital donde hay usuarios en movilidad que están consumiendo datos, que están en cloud. Es cierto que la administración pública no ha ido a cloud de forma masiva, lo cual no quita que sus usuarios no estén utilizando aplicaciones cloud, y que datos que ellos piensa que no están en la nube realmente estén en la nube. ¿Quién no se ha mandado a su Gmail personal algún documento para seguir trabajando cuando acaba la jornada de trabajo? Eso pasa en la administración privada y pasa en la administración pública. Con las soluciones tradicionales, endpoint y perimetrales, que tiene la administración pública no son capaces de controlar qué datos están yendo realmente a las aplicaciones cloud porque los usuarios ya no están detrás de los firewalls, están en movilidad.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

Sí, hay que cambiarlo, porque nos encontramos con que fabricantes como nosotros, que ofrecemos modelos de software-as-a-service, o security-as-a-service, no encajamos con los modelos de contratación normales de la administración pública, que van más orientados a contratos a tres o cinco años con poca flexibilidad y donde se determina desde el principio el número de usuarios y el alcance del servicio. Y en el punto en el que estamos de adopción de soluciones cloud, todo es muy flexible, y hay aplicaciones que aparecen y desaparecen, y cambia el volumen de usuarios, y las maneras de contratación no están adecuados a esta forma de contratar que requieren las aplicaciones cloud

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

Yo creo que hay que quitarse la venda de los ojos y mirar de verdad qué están haciendo otros usuarios y dónde están dejando los datos corporativos, y que con las soluciones perimetrales de toda la vida no vamos a ser capaces. Se está adoptando instancias de cloud públicas, pero: ¿cómo se está securizando?, ¿qué datos acaban en la cloud pública? ¿qué pasa con el Shadow Data? Estos serían para mí los principales retos.

"Deberían cambiar las medidas a la hora de valorar cuáles son las mejores propuestas. Que no siempre impere lo más barato"

César Moro, Sales Consultant, Quest Software

1. ¿Qué está haciendo la administración pública en seguridad?
Difiere mucho respecto a si es administración pública central o local, y a nivel presupuestario lo que pueden hacer o no. Digo esto porque hay bastantes diferencias en cómo lo abordan algunos organismos más avanzados o lo que se han ido invirtiendo en distintas medidas y capas de seguridad que han permitido tener más controlados los entornos. No es una respuesta global porque no podemos poner en el mismo saco a todas las administraciones públicas, hay algunos que sí invierten, otros no tanto y creo que todos deberían invertir mucho más porque se están poniendo barreras clásicas, como las perimetrales, pero no nos damos cuenta que, la mayoría de los ataques son ataques internos, y estos no son fáciles de controlar.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?
Sí, totalmente. Primero porque estamos en los últimos años apostando por los presupuestos más baratos, las soluciones más baratos, y no se tiene en cuenta medidas que pueden ser mucho más críticas que no simplemente el coste de la solución que se está implantando. A veces una solución puede ser más barata, pero no cubre todas las necesidades que puede tener la administración. Deberían cambiar la medida de valorar cuáles son las mejores propuestas. Que se tengan en cuenta otros criterios y no que impere que lo más barato sea lo que salga adelante.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?
Seguir viendo cómo las amenazas que nos encontramos provienen de muchas fuentes, tanto internas como externas, seguir apostando por meter capas de seguridad, porque es lo único que nos va a permitir tener nuestro entornos más controlados, y sobre todo tener la visión de que no vamos a ser capaces de poder parar cualquier ataque. El enfoque tiene que ser la mitigación de riesgos, es decir que, aunque suframos un ataque, seamos capaces de recuperarnos y que el impacto de esa brecha de seguridad sea el mínimo posible.

"El problema que tiene la administración es que los modelos de contratación son muy rígidos"

Joseba Enjuto,
Responsable de Consultoría, S2Isec

1. ¿Qué está haciendo la administración pública en seguridad?

La administración pública está centrando su seguridad en el Esquema Nacional de Seguridad (ENS) y en utilizarlo como driver para avanzar en seguridad, lo que no es un mal planteamiento. Pero se están quedando ahí y que hay aspectos de los que el ENS no habla especialmente, como puede ser todo lo relacionados con la reacción, la monitorización y el contar con perfiles muy especializados, y que como no son una exigencia técnica ni de formación del personal propio, se están quedando o no están llegando a los niveles a los que probablemente sea necesario llegar.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

En este sentido el punto de partida es contratar a empresas certificadas en el ENS. Es un buen punto de partida, pero el problema que tiene la administración es que los modelos de contratación son muy rígidos; además existe el hecho de que la administración no puede descartar empresas con las que ha tenido malas experiencias, lo que le somete a una situación en la que pueden verse obligados a contrataciones en contra de lo que el sentido común diría. Lamentablemente el mecanismo de contratación es el que es.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

El principal reto en 2020 para la administración pública es el presupuestario. Yo creo que todas las administraciones tienen que mejorar en seguridad, pero lo cierto es que la seguridad no vende votos, no vende a nivel de ciudadanía, y por lo tanto cuesta mucho incrementar los presupuestos de ciberseguridad. Y ese es el gran reto que tienen muchas administraciones públicas a día de hoy, que saben que tienen carencias, pero no son capaces de resolverlas.

Y a nivel de sector, el principal reto es ser capaces de reaccionar más y mejor al entorno cada vez más agresivo en el que vivimos. Tenemos que empezar a vivir con la sensación de que hemos sido atacados y tener más capacidad de respuesta, porque a día de hoy la prevención la tenemos muy clara, pero la reacción nos cuesta más.

1. ¿Qué está haciendo la administración pública en seguridad?
La administración pública en seguridad tiene un reto importante: la migración que está haciendo de forma paulatina a Office 365 tiene un problema grave porque Microsoft no protege bien el correo electrónico y otras funcionalidades. Esto lleva a que la administración pública esté empezando a pensar en poner en marcha servicios tipo CASB para los diferentes entornos en 2020.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?
Es una buena pregunta porque al final estos entornos se licencian por usuario y los usuarios no son fijos, hoy doy de alta cinco, y mañana de baja diez, y evidentemente habrá que cambiar la forma de hacerlo. Quizá las manera sería hacerlo a través de terceos, y aquí pueden entrar figuras como los MSSP que hagan de buffer ante la volatilidad de este tipo de servicio. Es una idea que lanzo.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?
Hay varios retos. La subida al cloud implica pensar en otro tipo de paradigmas en los que el perímetro ha desaparecido. El nuevo perímetro está en las credenciales; el primer gran problema al que se enfrenta la empresa y la administración pública es el robo de credenciales a través de phishing avanzado, y las herramientas actuales no lo están detectando. El segundo punto, muy vinculado al anterior, son los ficheros infectados con malware avanzado; en 2019 detectamos cerca de 200.000 variantes de malware vinculadas a ficheros de Office y PDF que hacen que el secuestro de credenciales y la infección vía ransomware se disparara en los dos últimos meses de 2019. Y el tercer gran problema, de difícil solución, es el cifrado de las sesiones de los datos en Internet; más del 80% del tráfico está cifrado y menos del 5% de las empresas revisan el tráfico cifrado porque es complejo y esto genera un problema de seguridad muy grande

"El primer gran problema al que se enfrenta la empresa y la administración pública es el robo de credenciales"

Sergio Martínez,
Director General, SonicWall Iberia

"La forma de compra que tiene la administración pública es la misma para comprar coches que para comprar TI y seguridad, y no es lo mismo"

Alberto Fernández, Enterprise Account Executive, Sophos Iberia

1. ¿Qué está haciendo la administración pública en seguridad?

Lo que la administración pública está haciendo muy bien es empezar a madurar el proceso del Esquema Nacional de Seguridad, que ya tiene un nivel de cumplimiento del 52% desde que se lanzara hace diez años. Por lo tanto, se va mejorando, aunque no es perfecto y quede mucho camino por recorrer.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?

La forma de compra que tiene la administración pública es la misma para comprar coches que para comprar TI y seguridad, y no es lo mismo. Bajo mi punto de visto sí que deberían darle una vuelta al modelo de contratación, que ya se lo han dado, pero no lo suficiente. Me he encontrado con organismos en los que los responsables de seguridad tienen muy claro hacia dónde quieren ir y cómo harían un contrato de pago por uso de diferentes tecnologías, pero por cómo es el modelo de contratación no pueden hacerlo. El modelo de contratación es muy rígido para algo que no es rígido, como es el TI, que es totalmente voluble.

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?

En los dos últimos meses de 2019 vimos un montón de ataques tipo EMOTET y tipo Ryuk, y el reto es seguir trabajando y dar una solución efectiva a ese tipo de ataques. Se tiene que ir más allá de un simple antivirus y es lo que tiene que interiorizar la administración pública, sacar presupuesto y abordar esos proyectos cuanto antes, porque al final están expuestos y lo hemos visto en casos como el del Ayuntamiento de Jerez y diferentes administraciones públicas.

"Un mal endémico de la administración, en general, es el tema de presupuestos y de compas a última hora"

Borja Pérez,
Country Manager, Stormshield Iberia

1. ¿Qué está haciendo la administración pública en seguridad?
Depende de qué administración pública. Hay administración pública que está haciendo la cosas muy bien y otras que estamos viendo en los medios de comunicación, que están sufriendo ataques y que no están protegidos. La administración general del estado por lo general suele estar bien protegida. Tienes todo tipo de clientes, igual que en el sector privado.

2. ¿Debe cambiar la manera en la que la administración pública contrata y compra seguridad?
Sí, es necesario un cambio. Como pasa en la privada, los equipos dedicados a TI son pequeños, los recursos son escasos, muchas veces dependen de terceros, y a veces las compras no son las más adecuadas. Un mal endémico de la administración en general es el tema de presupuestos y de compas a última hora y y muchas veces no tan bien pensadas como debería ser. Sobra presupuesto a final de año, voy a ver qué compro y a veces no se compra lo necesario

3. ¿Cuáles son los retos de 2020 a nivel de seguridad?
Los principales retos de la administración pública es tener gobierno y tener presupuestos. Además, yo echo de menos la figura, como existe en otros países, de un CISO de administración general del estado que ayude a las administraciones a afrontar los retos de seguridad y ayudarles en la elección de las tecnologías que tienen que implementar.

Respecto a los retos de la industria en general, 2019 tuvo un final de año muy movidito en cuanto a ataques cada vez más sofisticados y más dirigidos, y ahí es donde tenemos que enfocarnos todo el sector en general. Va a ser necesaria mucha cooperación, incluso entre competidores para hacer frente a este tipo de amenazas.

Enlaces de interés...

- Ciberseguridad adicional en modo cloud para la Administración Pública española
- El CCN-CERT mejora las capacidades de cibervigilancia con ELISA
- Microsoft y el CCN se unen para que las AAPP adopten cloud con total seguridad
- Página oficial de CCN-CERT

it Reseller
TECH&CONSULTING

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

JOSÉ CANO

DIRECTOR DE ANÁLISIS Y CONSULTORÍA DE IDC ESPAÑA

Director de Análisis y Consultoría en IDC Research España. Anteriormente, Director de Consultoría Técnica y Desarrollo de Negocio en GAC Grupo (España) y Director Académico del EMBA Blended (Madrid). Ha trabajado en consultoría de estrategia y operaciones en Avantia XXI S.L Global, y asesor ejecutivo para entidades públicas y privadas en el ámbito de la innovación y desarrollo de negocio (Deusto Business School, ICARUM ANS S.L, etc.). También ha sido socio fundador y director de consultoría de estrategia y operaciones en ACL Strategy S.L, y Senior Manager de Innovación en consultoría de sector público (E&O) en Deloitte.

Seguridad en movilidad, la gran olvidada

La transformación del puesto de trabajo, el futuro del entorno laboral, las nuevas tendencias en el espacio y la cultura de trabajo, la gestión del capital humano son términos bastante conocidos y de gran interés para la toda la comunidad empresarial.

El 45% de los CIOs españoles entrevistados por IDC, dice que los servicios relacionados con el puesto de trabajo y movilidad son la principal prioridad de inversión. El puesto de trabajo ha pasado de ser un commodity a ser algo diferenciador, no sólo en el desempeño de la empresa, sino también a la hora de atraer talento.

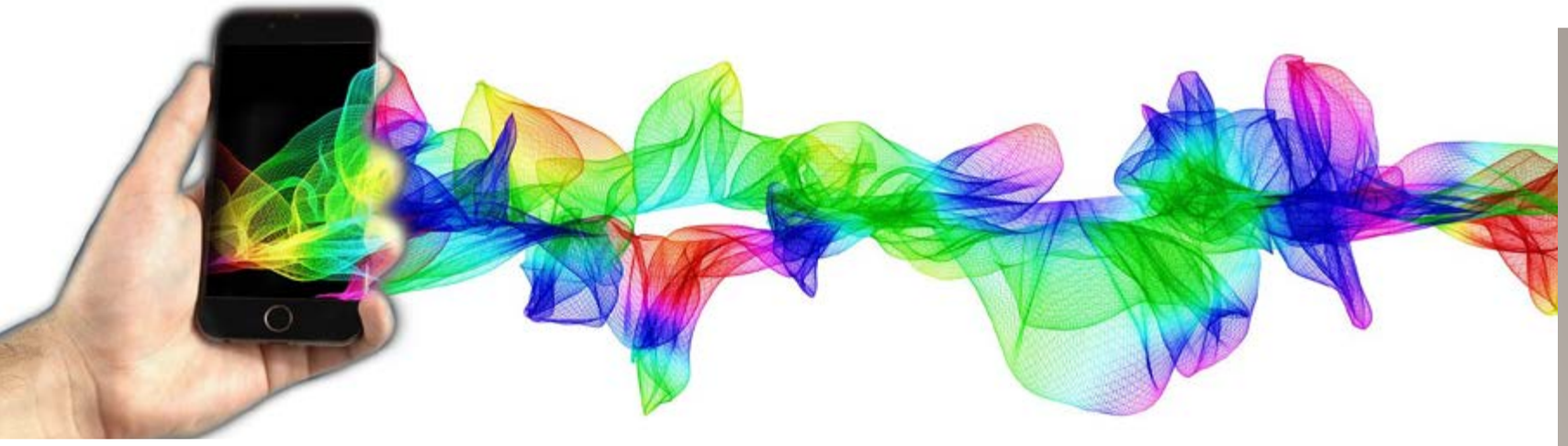
Las soluciones de colaboración empresarial unidas a la movilidad ayudan en a una organización a poder afrontar el reto de la Transformación del puesto de trabajo Digital, al permitir compartir documentos en tiempo real, comunicarse de manera más eficiente entre individuos y grupos en distintas zonas geográficas, lo que agiliza el trabajo, posibilitar la conciliación y mejorar la productividad.

La movilidad sigue siendo un factor clave para abordar con éxito el puesto de trabajo digital

El uso de la tecnología impulsará la productividad, pero no sólo de los trabajadores en entornos de oficina, sino que está teniendo un impacto cada vez mayor en departamentos operativos tales como logística, producción o mantenimiento.

La movilidad sigue siendo un factor clave para abordar con éxito el puesto de trabajo digital. Según datos de IDC, la población de trabajadores móviles de Europa Occidental crecerá a un CAGR del 3,5% en los próximos cinco años, aumentando de 103 millones en 2017 a 120 millones de trabajadores en 2021. Además, el porcentaje de trabajadores móviles en la fuerza de trabajo total en Europa Occidental se espera que aumente del 53% en 2016 al 63% en 2021.

Esta tendencia, unida a la distribución del mercado de trabajo donde actualmente conviven cuatro generaciones diferentes, está impactando en la adopción del fenómeno BYOD (bring your own device), sobre todo en generaciones más jóvenes y acostumbradas a la tecnología, lo que obviamente tiene impactos en ahorros y aumento de productividad pero de riesgo, ya que este fenómeno se asocia cada vez más a la tendencia conocida como BYOA o Bring Your Application (BYOA) en la cual el trabajador busca utilizar también las aplicaciones



El pilar fundamental más allá del tecnológico es de educación. Es crucial sensibilizar al trabajador de los riesgos de ciberataque

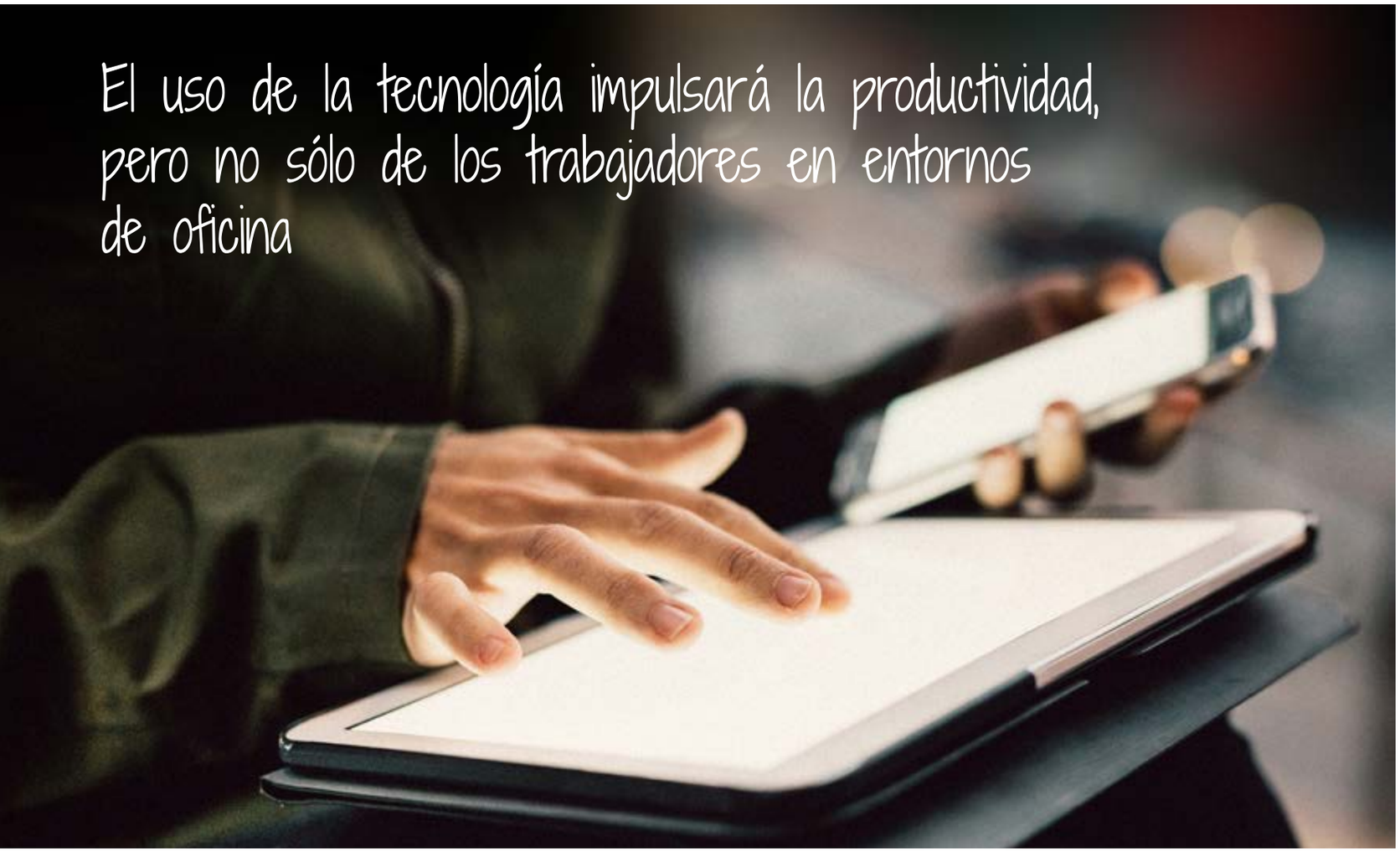
que juzguen adecuadas con o sin la intervención del departamento de TI de la organización (el caso más ilustrativo es el de whatsapp).

El problema de este tipo de tendencia es que requiere un enfoque de seguridad móvil muy diferente al que estamos acostumbrados de manera tradicional en una organización: definición y reforzamiento de políticas de acceso a la red, ofrecer acceso transparente a la misma, ofrecer herramientas de colaboración multidispositivo, administración remota de los dispositivos móviles y de sus aplicaciones, así como localización de dispositivos y capacidad de borrar de manera remota la información de la empresa, ofreciendo por tanto la posibilidad de usar dentro del dispositivo dominios separados de información personal y corporativa.

Este enfoque ayuda a la hora de lidiar con los principales retos de seguridad que se dibujan en la actualidad:

- **El malware para dispositivos.**
- **Un riesgo de robo de propiedad intelectual e información corporativa**
- **El concepto de botnet,** existente desde hace varios años en las computadoras personales, se ha extrapolado a las redes móviles a través de botnets como Rootstrap/Bmaster

Sin embargo, aunque la mayoría de las empresas está potenciando la seguridad para hacer frente a



Enlaces de interés...

- Mensaje de los expertos en seguridad: hay que elevar la protección los dispositivos móviles
- En busca del perímetro perdido

un panorama cada vez más cambiante, es necesario ante de establecer ninguna acción tecnológica, conocer los riesgos para el negocio de este tipo de amenazas, y diseñar así el plan de movilidad de la organización. Posteriormente, dotar a los dispositivos móviles de mecanismos de túnel de VPN que redireccione el tráfico del dispositivo para pasar por la red de la empresa donde puede revisarse que cumpla con los estándares y políticas de seguridad de la misma al mismo tiempo que se filtran malwares y virus, así como un Mobile Device Manager (MDM) que permita como mínimo administrar la localización y las aplicaciones de los dispositivos, implementar soluciones de siguiente generación, etc.

Sin embargo, el pilar fundamental más allá del tecnológico es de educación. Es crucial sensibilizar al trabajador de los riesgos de ciberataque, entender las técnicas de ingeniería social más utilizadas por los hackers y tener buenas políticas de seguridad física. Evolucionamos a una fuerza de trabajo móvil que genera y consume información. Por ello será necesario que la estrategia de seguridad móvil de la organización no sólo esté enfocada en la defensa ante un ciberataque, sino descubrir comportamientos anómalos en la red y poderlos remediar de manera efectiva

¿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:

CITRIX®

Wolters Kluwer

NFON Cloud Telephone System

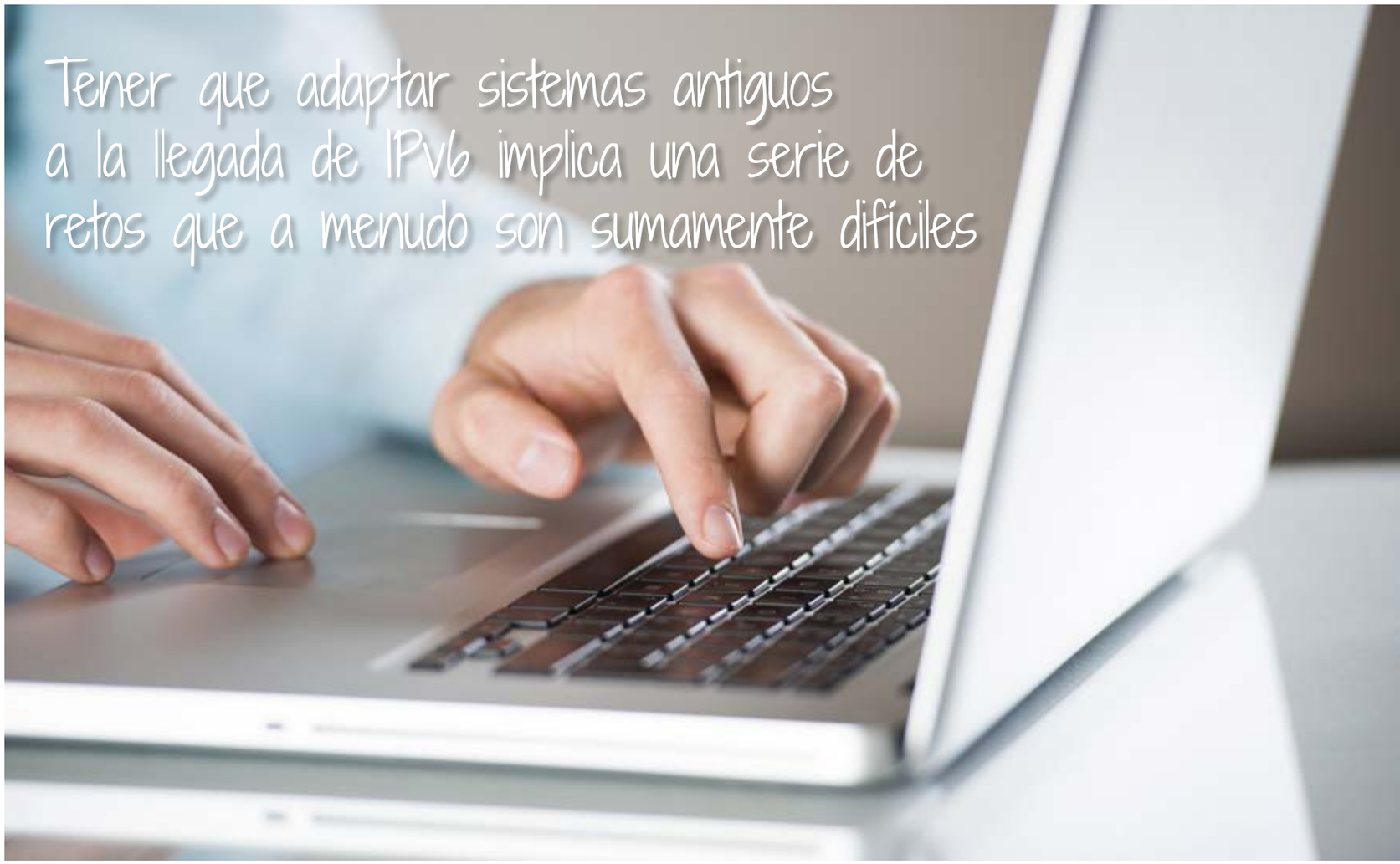
Packlink® PRO Simply Shipping

JAMES LYNE

CTO SANS INSTITUTE
James Lyne es un reconocido experto de ciberseguridad así como un gran orador comprometido a educar sobre las amenazas y las mejores prácticas en seguridad. Enérgico y apasionado, se ha convertido en un destacado presentador al ser capaz de maximizar el impacto de su experiencia en seguridad a través de presentaciones atractivas.

¿Por qué hay tantas organizaciones que siguen sin estar preparadas para IPv6?

Parece que llevamos toda la vida hablando sobre el protocolo de internet IPv6. Se lanzó oficialmente en 2012, pero ya existía unos años antes, en 2011 ya se había implementado en los principales sistemas operativos usados por las empresas y los consumidores. Incluso antes de esta fecha ya se sabía ampliamente que nos estábamos quedando sin direcciones IPv4.



Y, sin embargo, muchas organizaciones europeas siguen sin estar preparadas para implementar IPv6, con grandes diferencias entre países y empresas. Aunque algunas empresas no han adoptado IPv6 oficialmente, o no han desarrollado una estrategia para gestionar su implementación, al permitir la presencia en sus redes de tecnología que ya utiliza este protocolo (ya sea con el permiso explícito de sus departamentos de informática y comunicaciones o sin él) han adoptado IPv6 de forma extraoficial. Esto implica que corren el riesgo de poner en peligro la seguridad de sus organizaciones si las reglas que gobiernan sus cortafuegos (firewall) dejan de funcionar o si los antivirus y otros productos de seguridad no están optimizados para el tráfico IPv6.

La razón por la que encontramos tal problema en Europa es que no hay ningún organismo dedicado a supervisar e impulsar la migración a IPv6. En Estados Unidos, las políticas del gobierno para promover la transición al nuevo estándar han conseguido un mayor grado de adopción. En Asia, el uso de este protocolo se ha visto acelerado por el mero hecho del gran crecimiento de la región y la necesidad de direcciones en un contexto de limitada disponibilidad de direcciones IPv4 tradicionales.

¿Qué impide que las organizaciones completen esta transición?

En un mundo perfecto, las organizaciones podrían construir desde cero una nueva arquitectura informática y de comunicaciones preparada para IPv6. Por supuesto, pocas organizaciones se pueden permitir este lujo, y tener que adaptar sistemas antiguos a la llegada de IPv6 implica una serie de retos que a menudo son sumamente difíciles.

Por ejemplo, las empresas manufactureras dependen de robots y máquinas en sus líneas de producción. Muchos de ellos utilizan Windows 95 como sistema operativo y a menudo llevan años sin actualizarse. En algunos casos, implementar IPv6 significaría detener la producción de toda la fábrica

Si el equipo de respuesta a incidencias y de control central de una gran empresa no está preparado para atender las alertas sobre IPv6, algunos eventos críticos podrían pasar desapercibidos

mientras se migra a IPv6, algo que resultaría extremadamente caro para la empresa.

Las empresas de telecomunicaciones vienen trabajando en esta transición desde hace años y la extenderán a los consumidores y las empresas de forma progresiva y continua. Es realmente importante asegurarse de que estén preparados los equipos de informática y comunicaciones y de seguridad, ya que, si el equipo de respuesta a incidencias y de control central de una gran empresa no está preparado para atender las alertas sobre IPv6, algunos eventos críticos podrían pasar desapercibidos.

Un reto aún mayor es el relacionado con el hecho de que el IPv6 es mucho más que "una dirección IP más larga". El nuevo protocolo es sustancialmente diferente a IPv4, y hay que rediseñar correctamente algunos aspectos de la arquitectura de las redes para mantener su rendimiento y seguridad. Y hay un verdadero riesgo al hacerlo, de cometer errores relacionados con la seguridad que podrían exponer algunos recursos involuntariamente o llevar a depender de una medida de seguridad anterior (como una pasarela con un límite en la traducción de direcciones de red y crear así una isla).

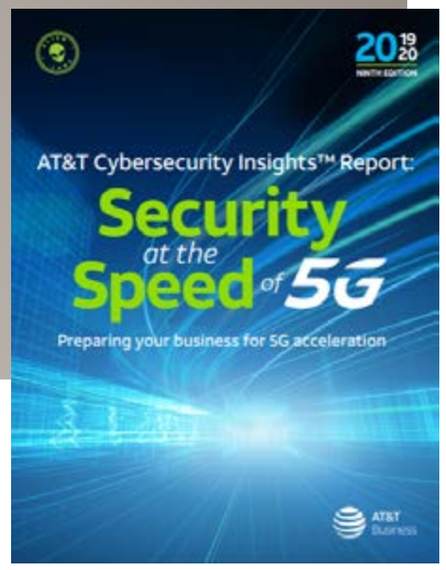
Software y formación

En muchos casos, incluso las empresas y los distribuidores de software no están aún preparados

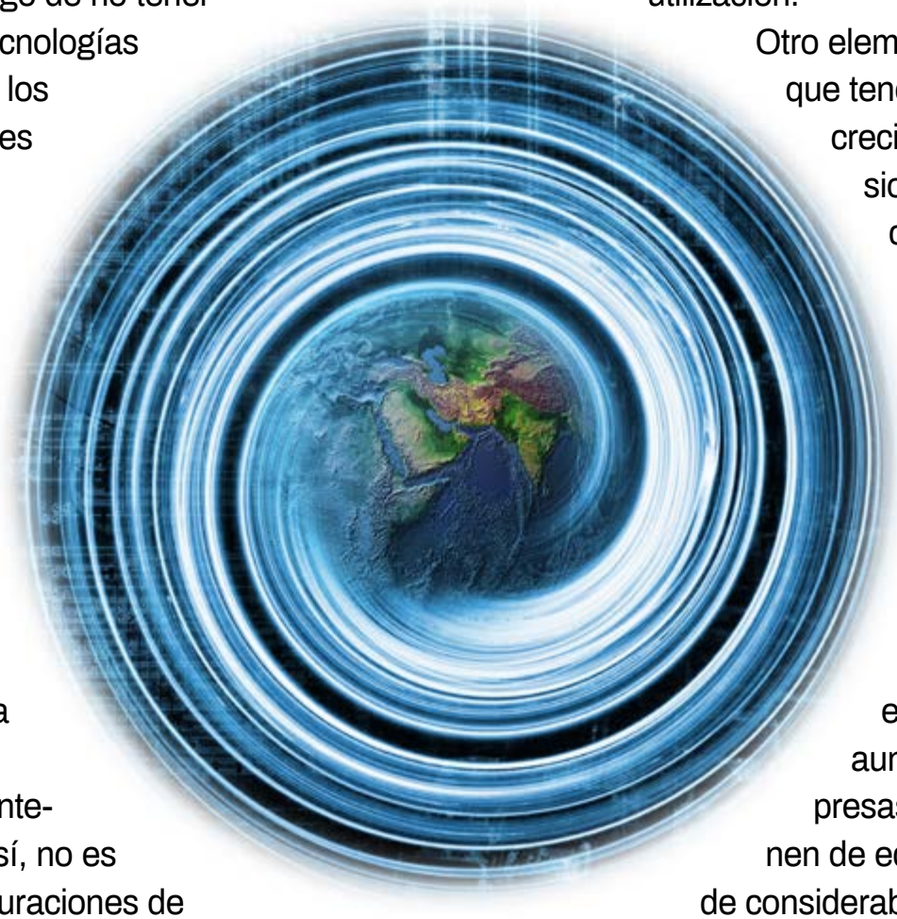
SEGURIDAD A VELOCIDAD DE 5G

5G no sólo es una 4G más rápida. La siguiente generación de redes móviles tiene el potencial de añadir más dispositivos a la red, ampliando la superficie de ataque e incrementando la posibilidad de nuevas amenazas.

Este informe de AT&T analiza cómo las empresas están afrontando su seguridad para 5G, encontrando que muchas no están preparadas adecuadamente para la última aceleración de big data. Entre otras cosas el informe recoge que las empresas se están quedando atrás en la expansión de sus capacidades de virtualización y redes definidas por software (SDN) y no están aprovechando la oportunidad para automatizar la seguridad.



para IPv6 en lo que respecta a sus productos. Algunos productos de seguridad y de tecnología sí están preparados, pero otros siguen sin ofrecer las mismas prestaciones en el entorno IPv6 que en el IPv4. Aparte del riesgo de no tener preparadas algunas tecnologías (como los filtros web o los cortafuegos), también es muy importante asegurarse de que los profesionales de la ciberseguridad estén bien formados en el nuevo protocolo. IPv6 incluye nuevos conceptos que deben entenderse plenamente, y no es raro encontrarlos en uso de forma casual en una red sin los controles convenientemente actualizados. Así, no es extraño ver autoconfiguraciones de IPv6 en una red o que se use el protocolo en asociación con aplicaciones de Microsoft o servicios del sistema operativo sin que el equipo de seguridad y de resolución de incidencias esté al tanto de esta utilización.



Otro elemento clave que hay que tener en cuenta es la creciente falta de profesionales de seguridad cualificados y el ingente número de tareas diarias que se tienen que llevar a cabo. Hay pocos profesionales de la seguridad en general, y menos aún que tengan experiencia en esta área específica. Además, aunque las grandes empresas normalmente disponen de equipos de seguridad de considerable tamaño y la capacidad de realizar grandes inversiones en proyectos tecnológicos como la transición a IPv6, las pymes no tienen esos recursos. Dado que incluso las grandes empresas no están preparadas, podemos empezar a apreciar las dimensiones del problema si tenemos en cuenta que a lo largo de toda la cadena de suministro hay normalmente muchas empresas medianas que proveen componentes críticos a esas grandes empresas.

¿Qué viene ahora?

Sin duda, la transición a IPv6 es un proceso doloroso para muchas organizaciones, pero es un camino que todos acabarán emprendiendo. Es importante que las empresas sigan adelante con la implementación de IPv6, dado que ya hay un sorprendente volumen de tráfico IPv6 en nuestras redes y en internet. IPv6 no se considera una moda pasajera, y las organizaciones tienen que asegurarse de no seguir adelante con su uso sin prestarle toda la atención que merece.

> IPv6 incluye nuevos conceptos que deben entenderse plenamente, y no es raro encontrarlos en uso de forma casual en una red sin los controles convenientemente actualizados

Enlaces de interés...

- Un tercio de las empresas utilizan plataformas de comunicaciones seguras
- Recomendaciones para blindar las comunicaciones de email

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos IT User

Almacenamiento it

Con la colaboración de: Hewlett Packard Enterprise