it TRENDS

OCTUBRE 2020

Hacia un nuevo orden digital inteligente y seguro

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

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

Hacia un nuevo orden digital inteligente y seguro

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

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

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

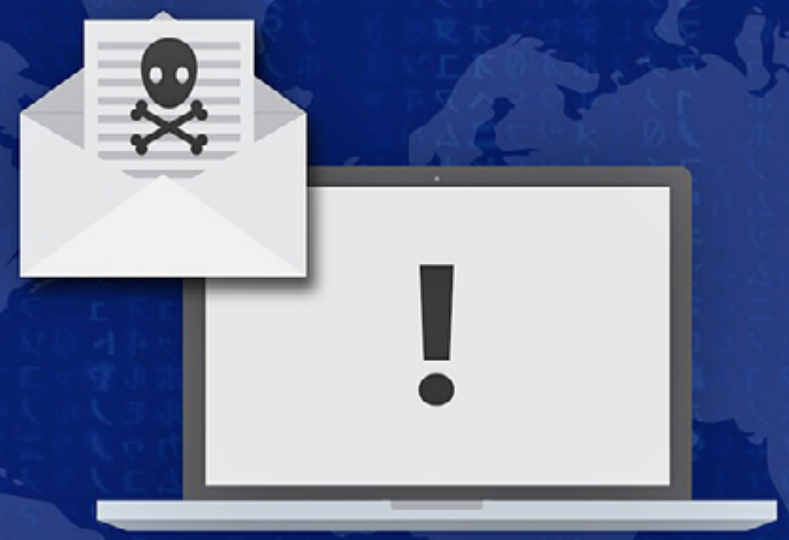
Por otra parte, Alexandre Ramos, CIO de Liberty Seguros Europa, nos contaba en la entrevista IT Trends, cómo la compañía ha decidido migrar todos sus servicios a cloud para aprovechar la flexibilidad de la nube y operar de manera única los servicios de TI en toda la organización.

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

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

Arancha Asenjo
Directora de IT Trends
www.ittrends.es

itTRENDS



Entendiendo el ransomware:

el secuestro informático que pone en jaque a la empresa

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

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

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

RANSOMWARE

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

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

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

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

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

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

CÓMO ATACA EL RANSOMWARE

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

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

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

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

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

TIPOS DE ENGAÑOS

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

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

¿A QUIÉN ATACA?

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

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

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

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

LOS MÁS DAÑINOS

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

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

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

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

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

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

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

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

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

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

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

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

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

Los ransomware con más alcance de los últimos años

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

MÁS INFORMACIÓN

- Crecen los ataques de ransomware y DDoS en el marco de la pandemia
- Aumentan los ataques de ransomware destinados al sector sanitario

Si te ha gustado este artículo, compártelo

CLAVES PARA EVITAR LA ENTRADA

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

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

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

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

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

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

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

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

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

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

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

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

NUEVO INFORME

DOCUMENTO EJECUTIVO

Teletrabajo en 2020:
el futuro se hace presente

ELABORADO POR itResearch

Descarga este **documento ejecutivo** de itResearch

#ITWEBINARS

La persistencia del Ransomware

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

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

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

Si te ha gustado este artículo, compártelo

Francisco Valencia, Secure&IT

Borja Pérez, Stormshield Iberia

Alberto Tejero, Panda Security Iberia, a WatchGuard brand

Horatiu Bandoiu, Bitdefender

José de la Cruz, Trend Micro Iberia

Francisco José Verdugo, VMware

Alberto Rodas, Sophos

Sergio Martínez, SonicWall Iberia

Josep Albors, ESET España

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

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

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

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

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

SECURE&IT. SEGURIDAD 360º

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

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

"Es necesario entender cómo se ha producido el ataque"

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

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

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

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

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

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

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

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

Si te ha gustado este artículo, compártelo

STORMSHIELD ENDPOINT SECURITY

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

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

"Tenemos un problema de concienciación"

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

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

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

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

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

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

PANDA SECURITY REPORT. SODINOKIBI

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

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

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

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

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

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

BITDEFENDER GRAVITYZONE ULTRA PLUS

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

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

"No debemos pagar nunca el rescate"

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

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

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

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

PROTECCIÓN DEL LUGAR DE TRABAJO INTERRUMPIDO POR LA PANDEMIA

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

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

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

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

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

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

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

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

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

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

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

Si te ha gustado este artículo, compártelo

SEGURIDAD INSTRÍNSECA FOR DUMMIES

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

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

"Se necesitan herramientas de nueva generación capaces de detectar comportamiento"

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

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

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

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

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

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

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

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

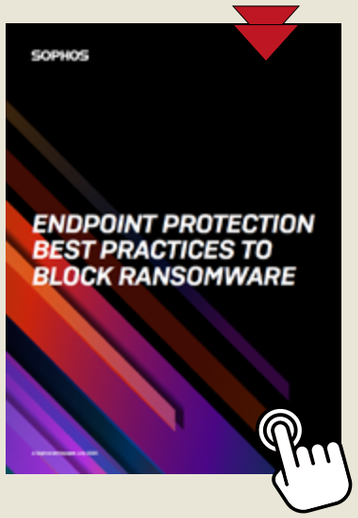
A nivel de puesto de trabajo se cuenta con Sophos Intercept X con capacidades de detección en tiempo de ejecución y control de comportamiento para detectar esa ejecución de ransomware, la propagación o el cifrado no deseado. “Pero además tenemos los servicios de detección y respuesta, donde con el módulo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

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

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

Si te ha gustado este artículo, compártelo

MEJORES PRÁCTICAS PARA BLOQUEAR EL RANSOWMARE



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

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

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

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

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

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

INFORME SOBRE CIBERAMENAZAS 2020 DE SONICWALL

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

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

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

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

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

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

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

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

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

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

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

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

Si te ha gustado este artículo, compártelo

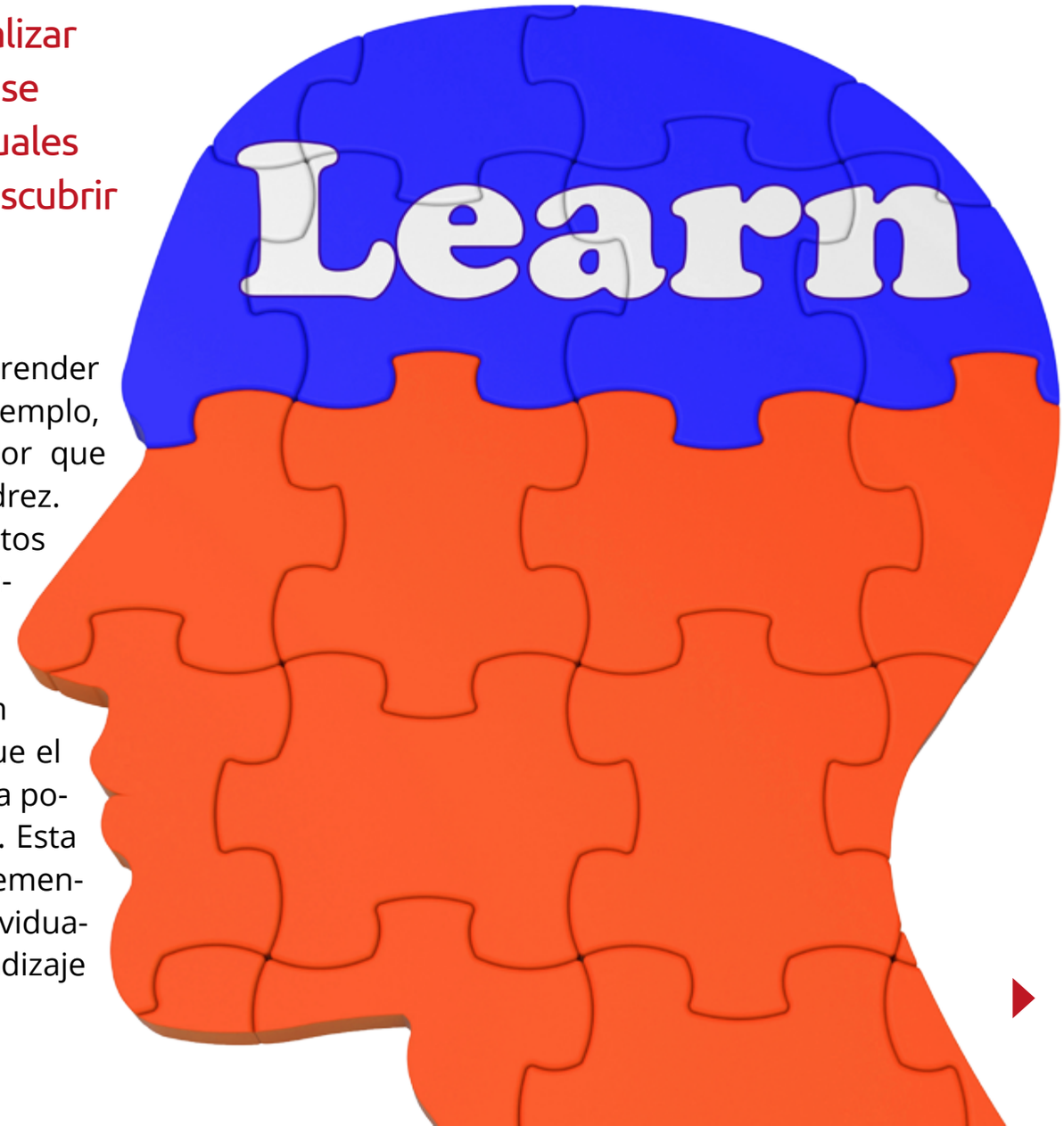
it whitepapers

RANSOMWARE DESDE EL PUNTO DE VISTA EMPRESARIAL

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

Inteligencia Artificial: explotando sus capacidades

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



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

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

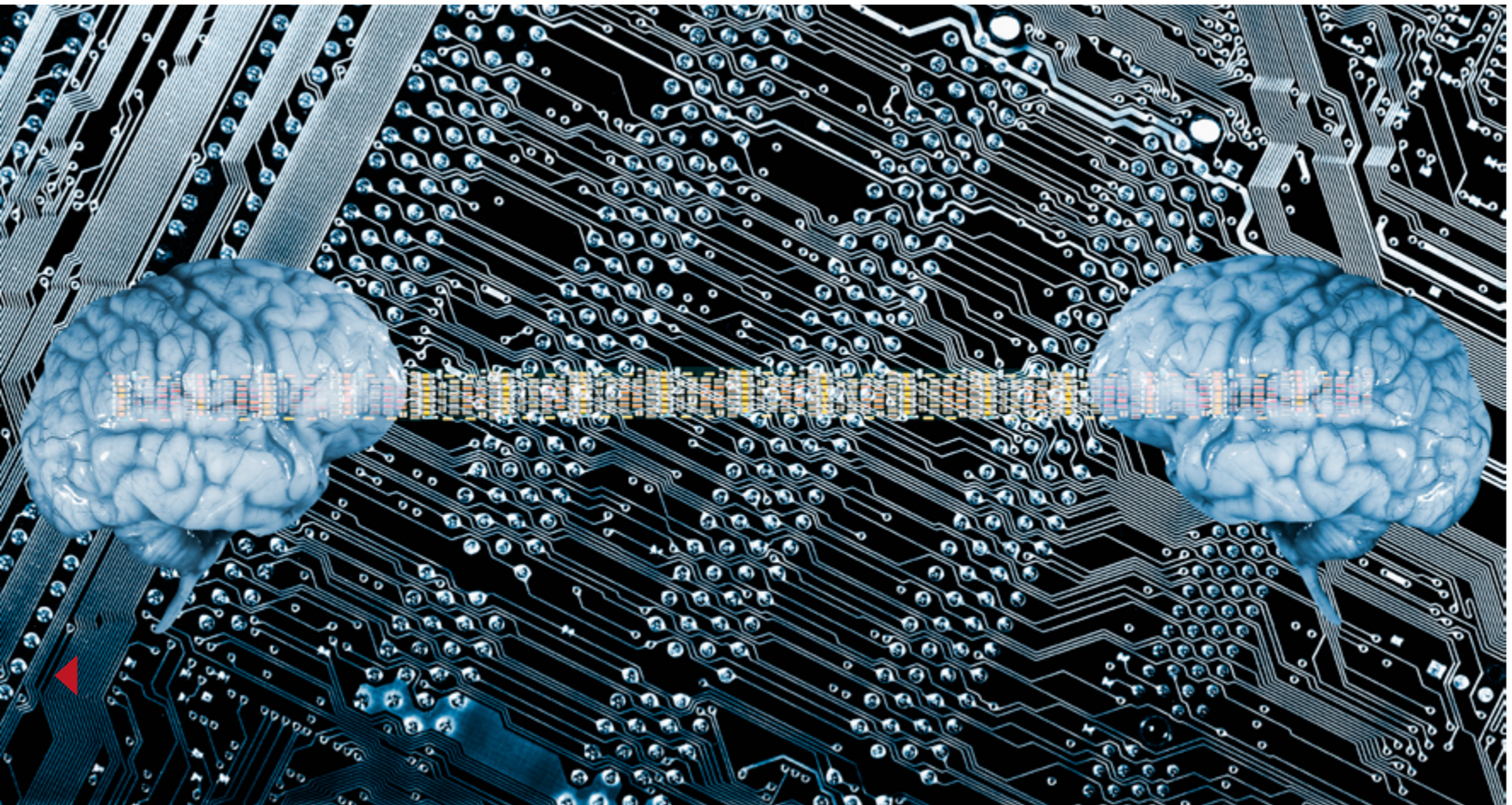
Podría intentar movimientos al azar hasta encontrar el jaque mate. Entonces, el programa podría almacenar la solución con la posición para que la próxima vez que el sistema encuentre la misma posición recuerde la solución. Esta simple memorización de elementos y procedimientos individuales, conocida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

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

Más desafiante es el problema de la generalización, que implica aplicar la experiencia pasada a situaciones nuevas análogas. Por ejemplo, un programa que aprende el tiempo pasado de los verbos regulares en inglés de memoria no podrá producir el tiempo pasado de una verbo irregular nuevo, a menos que previamente se hayan introducido otras reglas.

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

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



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

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

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

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

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

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

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

IA APLICADA

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

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

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

ÉTICA E IA

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

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

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

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

EL ORIGEN DE LA IA

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

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

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

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

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

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

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

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

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

EL FUTURO DE LA IA

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

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

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

MÁS INFORMACIÓN

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

Si te ha gustado este artículo, compártelo

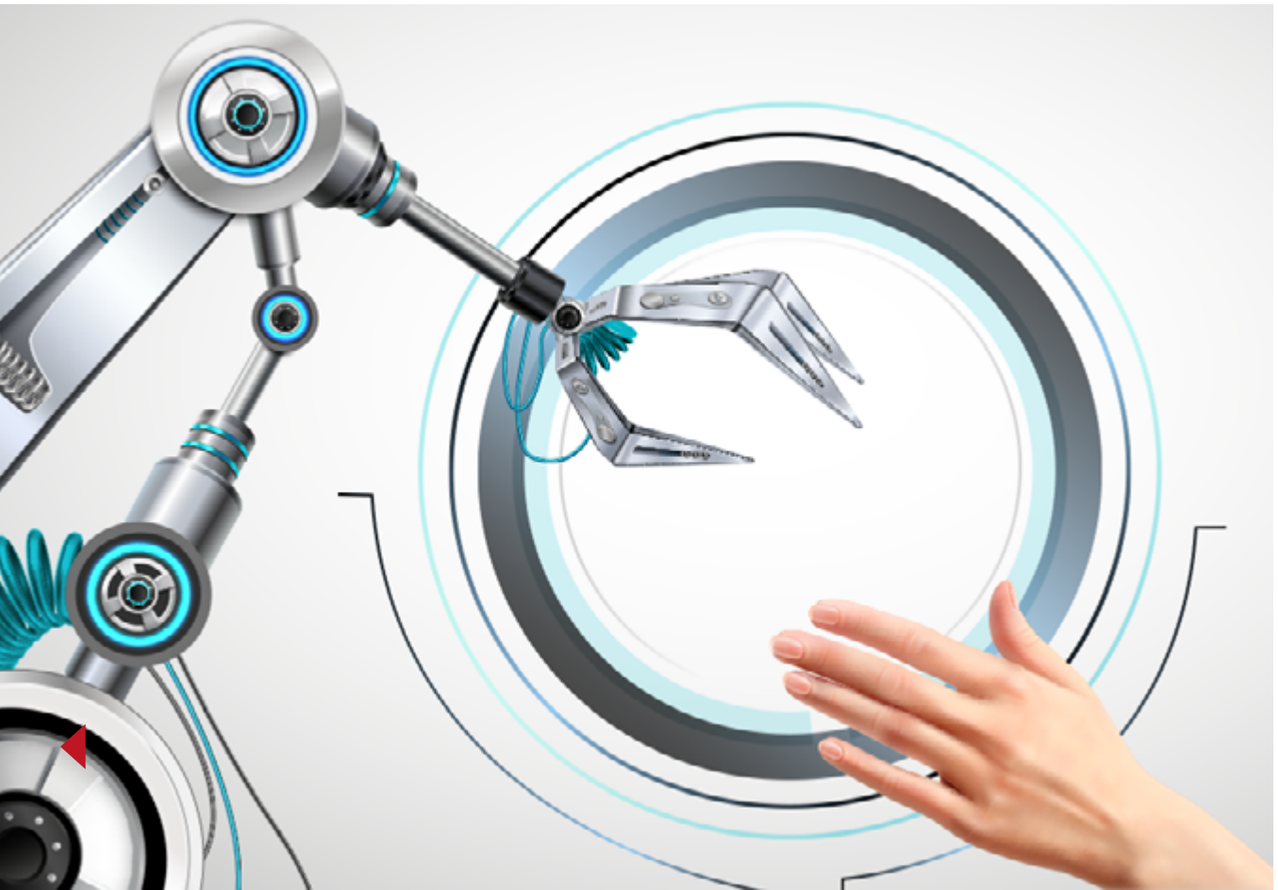
#ITWEBINARS

Inteligencia Artificial, ¿cómo lo aplico en mi empresa?

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

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

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



Si te ha gustado este artículo, compártelo

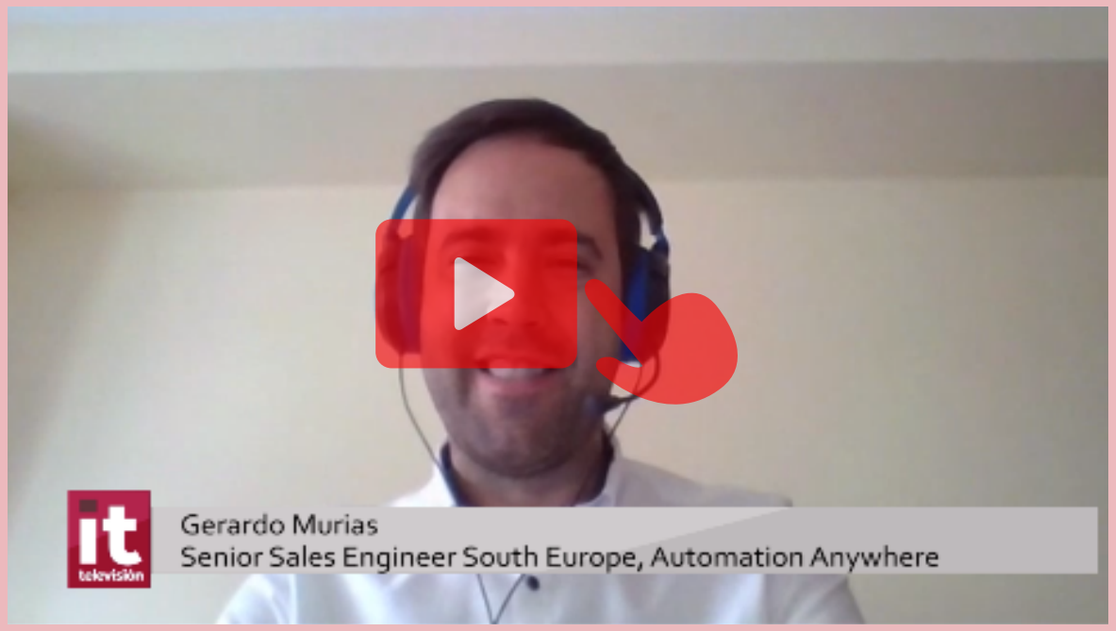
Gerardo Murias, Automation Anywhere

Ramsés Gallego, Micro Focus

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

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

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



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

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

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

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

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

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

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

Puedes ver la intervención de Automation Anywhere aquí. ■

AUTOMATIZACIÓN CON INTELIGENCIA ARTIFICIAL, LA CLAVE DEL ÉXITO DE RPA

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

Si te ha gustado este artículo, compártelo

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

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

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

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

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

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

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

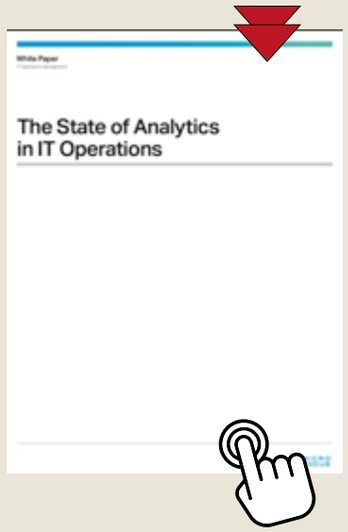
Con esta ayuda, una empresa puede plantearse qué tareas necesita mejorar y hacerse varias preguntas. "¿Por qué hago esto, para controlar los costes, el riesgo, mejorar el servicio interna o externamente? A partir de ahí, hay que ver qué procesos de grandes volúmenes o transacciones puedo automatizar.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

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

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

LA IMPORTANCIA DE LAS OPERACIONES DE ANÁLISIS EN IT

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



Si te ha gustado este artículo, compártelo

itTrends

Ayúdanos a conocer la realidad digital

COVID-19,

¿cuánto y cómo ha influido en las estrategias de TI?

¡PARTICIPA!

en nuestra Encuesta

itResearch

7 pasos para apreciar el valor de las aplicaciones modernas

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

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

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

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

solo el 41% para las organizaciones de menor rendimiento.

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

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

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

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

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

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

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

2 ¿Qué aplicaciones hay que poner en funcionamiento?

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

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

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

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

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

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

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

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

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

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

4 Entonces, ¿dónde ejecutar las aplicaciones?

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

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

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

5 ¿Cómo entregarlas a los usuarios?

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

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

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

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

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

6 ¿Cómo asegurarlas?

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

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

7 ¿Cómo gestionar todo?

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

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

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

Si te ha gustado este artículo, compártelo

Diálogos IT TRENDS

Liberty Seguros se muda al cloud para ganar agilidad

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