it TRENDS

OCTUBRE 2019

Tendiendo puentes hacia una nueva generación de TI

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Directora de IT Digital Security
Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Director de IT User e IT Reseller
Pablo García pablo.garcia@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es
Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez, Jaime Domenech
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

En busca de la convivencia perfecta entre la TI tradicional y la de nueva generación

Cloud y la ciberseguridad que se aplica a los entornos de Industria 4.0 son dos claros ejemplos de la continua evolución tecnológica que aviva el sector TI. También lo son de la necesidad de aunar los despliegues heredados, las TI tradicionales, con nuevos planteamientos, dando lugar a entornos híbridos que encontramos tanto si hablamos de cloud, como si lo hacemos de Industria 4.0.

Si nos referimos a cloud, y tal y como ha quedado constatado en la sesión online que hemos llevado a cabo en IT Trends este trimestre (Tendencias y oportunidades de la nube), la necesidad de unir entornos tradicionales, con arquitecturas de nube privada y cloud pública, dando lugar a entornos híbridos, deriva en otro reto, el de gestionarlos adecuadamente, con capacidades de visibilidad y una capa de seguridad que haga que este movimiento hacia la nube sea transparente, sencillo y aporte garantías de flexibilidad y crecimiento en post de la innovación en el negocio.

Si hablamos de Industria 4.0, observamos la convivencia de dispositivos tradicionales y nuevos, conectados a Internet; de tecnologías operativas con tecnologías de la información bajo un mismo paraguas. Y bajo un mismo objetivo, el de los ciberdelincuentes. Por tanto, proteger estos entornos, que nuevamente pueden considerarse híbridos, requiere de renovadas estrategias de ciberseguridad que permitan a estas infraestructuras ofrecer todas las garantías para su correcto funcionamiento, sin generar daños indeseados. Así nos lo contaron los ponentes de nuestro IT Webinars titulado Ciberseguridad industrial, protegiendo el sector productivo.

En esta revista podrás encontrar un extenso resumen del conocimiento que compartieron con nuestra audiencia las 13 compañías que han participado en estas sesiones. Podrás leer sus conclusiones, acceder al webinar completo o ver sesiones específicas, así como descargar documentación sobre estas materias. Como siempre, te ofrecemos cientos de enlaces para que profundices tanto como desees.

Con esta publicación comenzamos el último trimestre del año. Toca pronto echar un vistazo a las tendencias tecnológicas que dominarán el próximo año. Nosotros lo haremos en nuestros próximos Encuentros IT Trends: Ciberseguridad y Tendencias TI 2020. ¿Te apuntas? ¡Te esperamos! ■

Arancha Asenjo
Directora de IT Televisión y Lead Gen Programs

www.ittrends.es

Hewlett Packard
Enterprise

ALMACENAMIENTO HPE 3PAR

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

→ Descubre cómo en

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

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

Cloud, la plataforma que lo cambia todo

En este tercer trimestre de 2019, en IT Trends hemos puesto la mirada en cloud, como una de las principales tendencias tecnológicas que está cambiando el modelo de TI de las organizaciones.

La nube se está convirtiendo en la plataforma por defecto bajo la que las empresas están construyendo sus TI, ya sean sus infraestructuras, plataformas o aplicativos.

La tendencia, claramente, es hacia un entorno de cloud híbrida, donde se conjugan las capacidades y control de una nube privada, con la flexibilidad y los costes de una cloud pública. Así, lo hemos constatado en el Informe IT Trends sobre Cloud, que acabamos de publicar tras la encuesta realizada a los lectores del ecosistema de IT Digital Media Group. Asimismo, los resultados revelan una clara tendencia hacia estrategias multicloud, donde se utilizan diversas nubes públicas (un 55,9% de los participantes afirman disponer de más de un servicio), donde cuestiones como la seguridad, automatización y orquestación son de vital importancia.

Para complementar esta visión de cloud y las tendencias y oportunidades que plantea, celebraremos una sesión online en la que participarán compañías representativas de este cambio que está produciendo la nube, para analizar los cambios que se están produciendo en este entorno. En este IT Summit Cloud, contaremos con HPE, Micro Focus, nCipher, Thales Security, Nutanix, OVH, Retarus, Sophos y Red Hat. ¡No te lo pierdas! ■

Visita nuestra web www.ittrends.es y conoce cómo avanzan en el mercado las principales tendencias tecnológicas que están transformando las empresas.

#ExpectTheUnexpected

RECONOCER**RIESGOS**

aunque aún sean desconocidos

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

retarus

itTRENDS

CLOUD

Tendencias de computación en la nube para 2019

La adopción de servicios en la nube pública avanza inexorablemente, configurando un sector cada vez más amplio y con mayor diversidad de ofertas y tecnologías disponibles. El cambio en el entorno cloud es constante y los expertos identifican algunas tendencias que marcarán el devenir del sector durante este año y los venideros.

A medida que avanza la digitalización, las organizaciones desarrollan nuevas necesidades tecnológicas para continuar siendo competitivos en los nuevos modelos de negocio vinculados a los datos y a los entornos digitales. En este contexto, la nube se ha convertido en un pilar fundamental de las estrategias digitales de las empresas, y su negocio está marcado por la evolución tecnológica, imprescindible para continuar proporcionando servicio a una masa cada vez mayor de clientes.

Comprender hacia dónde se dirigen los vientos evolutivos y de cam-

Las bases de datos también se rinden ante cloud

En 2022, el 75% de todas las bases de datos se desplegarán o se migrarán a una plataforma cloud, según Gartner. La firma ha constatado que las organizaciones están desarrollando e implementando nuevas aplicaciones cloud y moviendo sus activos a estas nuevas plataformas a un ritmo cada vez mayor, tendencia que, además, no tiene visos de cambiar.

Según su investigación, los ingresos generados por los sistemas DBMS crecieron un 18,4% hasta los 46.000 millones de dólares. La facturación procedente de sistemas en la nube supuso el 68% de ese crecimiento. De los datos se desprende también que Microsoft y Amazon Web Services (AWS) representan el 75,5%, lo que muestra que los proveedores de servicios cloud se están convirtiendo en las nuevas plataformas de gestión de datos.

En este sentido, la firma explica que los ecosistemas se están formando alrededor de este tipo de proveedores que integran los servicios y permiten a las empresas dar los primeros pasos hacia una gestión de datos entre nubes. Sin duda, esto contrasta claramente con el enfoque on-premise, en el que los productos individuales a menudo desempeñan múltiples funciones, pero rara vez ofrecen sus capacidades integradas para admitir la integración con otros productos adyacentes dentro del entorno de implementación local.

bio es fundamental para mantenerse a la vanguardia en un sector cada vez más competitivo, por lo que los expertos se centran en analizar las tendencias que marcarán el camino en el sector de los servicios en la nube. En este sentido, Daniel Newman, miembro de Futurum y colaborador en Forbes, publicó una lista con las principales tendencias que se seguirán en este sector en 2019, y que también tendrán mucha influencia en los próximos años.

CRECIMIENTO DE LOS ECOSISTEMAS SAAS

Tras unos inicios inciertos, el modelo de software como servicio (SaaS) se está convirtiendo en una de las tendencias emergentes entre los servicios cloud, especialmente para industrias como la cadena de suministro global o la atención médica, que necesitan sistemas que les permitan compartir datos para que sus avances tecnológicos

EL GASTO EN SOFTWARE COMO SERVICIO PODRÍA SUPERAR LOS 100.000 MILLONES DE DÓLARES

sean verdaderamente útiles, y les proporcionen los beneficios esperados. Por ejemplo, mediante un ecosistema de SaaS, todos los miembros de una cadena de suministro se pueden mantener vinculados para garantizar la integridad de los productos que se mueven a través de ella.

ESTRUCTURAS QUE VAN DESDE LA NUBE A LA PERIFERIA

El avance de la computación en el extremo tendrá un impacto importante en los ecosistemas de nube pública, que se enfocarán en servir como intermediarios entre las organizaciones, sus servicios en la nube y sus plataformas de computación Edge, que operan en el borde de su red. Las tecnologías que más influirán en esta tendencia serán IoT y 5G, que impulsarán el despliegue de nuevos tejidos de red para una distribución más flexible de los datos en numerosos casos de uso. Gracias a esto, se logrará una transferencia de datos en tiempo real entre las diversas plataformas, abriendo las puertas al futuro de IoT, el aprendizaje automático en el edge y otras aplicaciones de alto consumo de datos que podrán operar fuera de las instalaciones.

DIVERSIFICACIÓN EN EL USO DE LOS CONTENEDORES

Los proveedores de la nube como AWS, Google, IBM o Microsoft están incrementando sus inversiones en Kubernetes y otros contenedores para la "computación sin servidor". Esto permitirá a las empresas implementar aplicaciones y microservicios sin preocuparse por los problemas de configuración. Gracias a esto, pueden escalar, administrar y reemplazar componentes individuales de un sistema distribuido con más facilidad, sabiendo que, si falla una aplicación en un contenedor, no afectará a los demás. Estas ven-

IDC baja sus previsiones de gasto en infraestructura cloud para 2019

La firma de análisis ha bajado sus previsiones sobre el gasto total que se realizará en infraestructura tecnológica en la nube a lo largo de 2019, dejando la cifra en 66.900 millones de dólares, un 4,5% menos de lo que calculaba el pasado trimestre. Esto supondrá que el crecimiento interanual sea menor, del 1,6%.

Pese a ello, los proveedores consiguieron unos ingresos de 14.500 millones de dólares durante el primer trimestre de este año, un 11,4% más que en el mismo periodo del año anterior. Y, como siempre, se han observado diferencias en el comportamiento de las ventas de los diferentes tipos de modalidades de nube.

Los ingresos por infraestructura de hardware para entornos de nube pública en el primer trimestre disminuyeron un 13,4% en comparación con los últimos tres meses del año pasado, pero aumentaron interanualmente un 8,9% hasta los 9.800 millones de dólares. Este segmento sigue viéndose afectado por la demanda de una serie de proveedores de servicios a hiperescala, cuyo gasto en infraestructura de TI tiende a tener altibajos. Por tanto, tras un sólido desempeño en 2018, IDC espera que el gasto baje y que esto provoque una caída de los ingresos de los proveedores hasta los 44.500 millones de dólares, un 2,2% menos que en 2018.

A pesar de todo, seguirá siendo responsable de la mayoría del gasto de TI en entornos cloud, aunque su peso disminuirá del 69,1% en 2018 a 66,5% en 2019.

En cambio, el gasto en infraestructura de TI de nube privada ha mostrado un crecimiento más estable desde que IDC comenzó a hacer seguimiento de la evolución de las ventas. En el primer trimestre de 2019, los ingresos procedentes de esta modalidad aumentaron 16,9% interanual, alcanzando 4.700 millones. IDC espera que el gasto en este segmento crezca un 10,1% este año.

tajas impulsarán a partir de este año el uso de contenedores en las plataformas cloud, encaminando al sector hacia una computación serverless, cambiando el concepto de redes y la forma de desplegar nuevas tecnologías en la nube.

MÁS SEGURIDAD PARA LOS ENTORNOS MULTICLOUD

Los expertos señalan que este año se verá un incremento en las políticas destinadas a mejorar la seguridad y las cuestiones relativas al cumplimiento normativo en los entornos de múltiples nubes, debido a que las empresas clientes de estos servicios están cada vez más preocupadas por estas dos cuestiones.

ARQUITECTURAS NATIVAS DE LA NUBE

Newman afirma que a partir de este año comenzarán a desarrollarse las arquitecturas nativas de la nube. Esto, en sus palabras, implica observar el desarrollo de implementaciones de aplicaciones de una forma que se refleje en el entorno de la nube, mejorando la eficiencia de todos los procesos y flujos de trabajo. También conlleva el uso de entornos de autoaprovisionamiento como código, escalado automático y otros recursos a necesidad, e incluye una redundancia automática para garantizar la capacidad de recuperación de datos. Según señala, esto significa que las empresas podrán por fin optimizar el nivel de la nube, en vez de centrarse en sus sistemas anteriores. ■

MÁS INFORMACIÓN

- Los CIO de empresas españolas prefieren la TI híbrida
- Crece la preocupación por la seguridad de los servicios cloud aplicados a las finanzas
- Las empresas recurren a los proveedores de servicios para administrar sus entornos cloud

Si te ha gustado este artículo, compártelo

OPEN HYBRID CLOUD.
CONSTRUYE TU FUTURO.

EMPIEZA AHORA

Red Hat

Tendencias y oportunidades de la nube

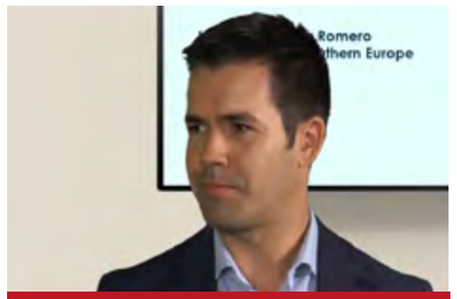
Cloud se ha convertido en LA PLATAFORMA que está alimentando la transformación digital y la modernización de las TI. Prácticamente el 90% de las organizaciones utiliza algún modelo de cloud y la mayor parte, cuenta con dos o más proveedores de servicios de nube, una tendencia que ha ido cogiendo tracción a lo largo de este 2019.

La cloud ha cambiado todo: el aprovisionamiento de infraestructura, el desarrollo de software, la gestión de la TI, el consumo de software, las estrategias de ciberseguridad... Además, en los últimos tiempos hemos visto cómo la nube ha propiciado y se alimenta de otros planteamientos tecnológicas, como son las plataformas de contenedores, la entrega e integración continuas, las soluciones de infraestructura como código, el networking y el almacenamiento definidos por software, por no hablar de IoT y la inteligencia artificial.

En este IT Webinars de IT Trends, descubrimos cuáles son las nuevas tendencias tecnológicas que giran en torno al cloud, así como las oportunidades de innovación que genera para las empresas. Para ello, hemos contado con la presencia de HPE, Micro Focus, nCipher, Nutanix, OVH, Retarus, Sophos y Red Hat. En las siguientes páginas puedes leer un extracto los aspectos más destacados de sus intervenciones. Si pinchas en cada una de las imágenes de los portavoces podrás visualizar su intervención en el webinar o ver la sesión completa aquí. ■

Galo Montes (HPE)

Antonio Picazo (Micro Focus)

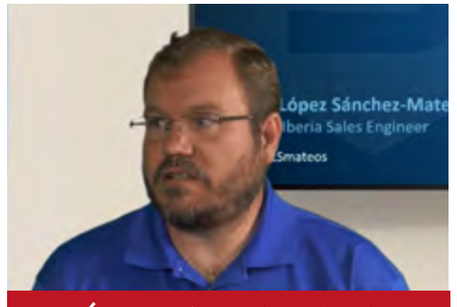


José Perez (nCipher)

Alejandro Solana (Nutanix)


Antonio Pizarro (OVH)


Óscar Arriaga (Retarus)



Óscar López (Sophos)

Ana Rocha (Red Hat)

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

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

SAP Gold Partner

SAPSecure

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

Sothis

www.sothis.tech

GALO MONTES, DIRECTOR TÉCNICO DE HPE ESPAÑA

“Bajo el concepto de cloudless, las cargas de trabajo siempre serán fáciles para el usuario, sin tener que lidiar con la complejidad de la infraestructura que hay por debajo”

“Hace cinco años se decía que el cloud sería dominante, desapareciendo servidores y almacenamiento local. Hoy el mundo es híbrido y seguirá siéndolo”. Así comenzaba Galo Montes, Director Técnico de Hewlett Packard Enterprise España, su intervención en el IT Webinar Tendencias y oportunidades de la nube (a la que puedes acceder aquí), donde desgranó el concepto de cloudless, una experiencia de nube híbrida, con una forma de trabajar abierta y sin fisuras, sustentada en la simplicidad de la infraestructura y en la integración con elementos de terceros, y donde las cargas de trabajo se mueven sin problema entre las distintas nubes y, desde allí, a las instalaciones.

Para lograr la efectividad de su modelo cloudless, HPE ha desplegado una estrategia sustentada en tres pilares: seguridad zero trust para las infraestructuras, incorporando me-

GALO MONTES, HPE ESPAÑA

canismos de seguridad como “silicon root of trust” en sus servidores; encriptación y protección de las comunicaciones entre las distintas cloud y dentro del data center; y provisión de un mayor valor para los clientes, gracias al suministro de una solución completa por parte de HPE.

Dentro de este mundo híbrido, no obstante, existen aún varios retos, como el conseguir que las máquinas sean autónomas y capaces de autoconfigurarse. “Aplicando masivamente la Inteligencia Artificial se consigue que estas puedan auto repararse y autogestionarse, mientras que con soluciones como HPE Primera, el almacenamiento que se configura en cuestión de minutos se actualiza con total transparencia y se entrega como servicio”, dijo Montes. Para que todo esto sea un conjunto “tiene que ocurrir que sea fácilmente componible; esto es, que cualquier carga de trabajo se pueda ejecutar en cualquier modelo de consumo (on premise, SDS o Cloud Pública)”.

Para que cualquier empresa pueda beneficiarse de este modelo, HPE ha dispuesto un modelo de pago por uso que se adapta a las necesidades de cada negocio, y con el que las empresas pagan únicamente por lo que necesitan (recursos de almacenamiento, computación, redes, nube, etc.) con las consiguientes ventajas financieras y técnicas.

Por último, y en su plan de convertirse en una empresa de soluciones “as a service”, HPE ha configurado un sistema híbrido de consumo, trasladando algunos de sus productos a la nube a fin de que los clientes puedan utilizar determinadas infraestructuras en modo servicio, como infraestructuras de computación, de almacenamiento... Se trata de soluciones muy específicas y que tienen un espacio en el tiempo muy concreto donde utilizarse.

Ve la intervención de HPE en el webinar Tendencias y oportunidades de la nube aquí.

Si te ha gustado este artículo, compártelo

ANTONIO PICAZO PREVENTA DE SOLUCIONES ITOM DE MICRO FOCUS

“La administración de los entornos híbridos es compleja. Es necesario centralizar la mayor cantidad de información en un único sitio. Esto ayudará a la toma de decisiones”

Los responsables de IT de las organizaciones se enfrentan a una serie de retos a la hora de abordar un entorno cloud empresarial híbrido. Desde esta perspectiva, Antonio Picazo Preventa de soluciones ITOM de Micro Focus, reconoció en la sesión online Tendencias y oportunidades de la nube que, “en ocasiones, la gestión de la infraestructura es el desafío más complicado al estar repartida en distintos lugares (local o cloud privada y cloud pública)”.

Ante esta situación, se hace necesario implantar una solución que permita agregar y gobernar los servicios de cloud público, gestionar los distintos recursos de forma optimizada, orquestar o automatizar extremo a extremo la infraestructura y mitigar el riesgo que producen las migraciones de cargas de trabajo entre entornos.

En su cartera, Micro Focus cuenta con Micro Focus Hybrid Cloud Management, en el que se integra el Portal de autoservicio CMP, un gran

ANTONIO PICAZO, MICRO FOCUS

marketplace donde se unifican todas las peticiones de servicio (SaaS, IaaS, PaaS) y se informa al administrador dónde es más óptimo desplegar el entorno híbrido. “Entre otras, el portal ayuda a una mejor administración de la capacidad (detección de cuellos de botella, asignación de carga computacional correcta, recomendaciones de provisión en los entornos privados…) y a una adecuada gestión de los costes”, explica Picazo.

A la hora de desplegar la cloud híbrida es muy importante también contar con un componente que ayude a orquestar y a automatizar todo ese proceso completo de provisión, no solo orquestar el despliegue de infraestructura sino a orquestar el proceso completo de la provisión a entornos cloud. Micro Focus Operation Orquestation es una solución para la creación sencilla de flujos destinados a automatizar procesos complejos. Se trata de una solución multi-autor, con gran contenido out-of-the-box y que se integra con cualquier tecnología estándar del mercado, así como con aplicaciones desarrolladas por el propio cliente. También, y a través de asistentes, se importa Webservice, REST, Shell o cualquier script a la librería de operaciones para luego hacer esa automatización de extremo a extremo.

Para simplificar la migración a cloud, Picazo propone integrar una herramienta de descubrimiento que revele las dependencias de los diferentes elementos de IT, a fin de definir los grupos que pueden ser objeto de migración a cloud. Una vez tomada la decisión de lo que se quiere migrar a cloud, automatizar ese movimiento e intentar que la ventana de parada de las cargas sea mínima, es una opción acertada. Adicionalmente, habrá que gestionar las instancias provisionadas.

Por último, en esos entornos complejos, la monitorización también tiene que cambiar. “Es conveniente optar por una solución que ayude a monitorizar esos entornos híbridos y a los clientes a gestionar la infraestructura nueva a la que se ha migrado”, matizó.

Accede a la intervención de Micro Focus en el IT Webinar Tendencias y oportunidades de la nube. ■

Si te ha gustado este artículo, compártelo

GESTIÓN DE NUBES HÍBRIDAS

La plataforma Micro Focus® Hybrid Cloud Management (HCM) es un marco de trabajo de automatización unificado que permite a IT agregar servicios cloud; diseñar, desplegar, gestionar y gobernar recursos híbridos; orquestar procesos de TI y proporcionar medidas para controlar la cloud y los costes.

JOSÉ MARÍA PÉREZ ROMERO, INGENIERO PREVENTA PARA EL SUR DE EUROPA DE NCIPHER

“Cuando las empresas llevan parte de su infraestructura e información a cloud sacan lo más valioso fuera de su casa. Todos estos datos requieren estar debidamente cifrados”

Cuando las empresas llevan parte de su infraestructura e información a cloud sacan lo más valioso fuera de su casa, afirmó José María Pérez Romero, Ingeniero Preventa para el Sur de Europa de nCipher, en su tiempo durante el IT Webinars Tendencias y oportunidades de la nube, de IT Trends. “El cloud es el presente. No existen empresas que no hayan subido su información o parte de ella a la nube, o que no se lo estén planteando”, dijo.

Desde nCipher Security trabajan el cloud con módulos de seguridad de hardware (HSM) as a service, pero también con otros métodos que permiten añadir una capa de seguridad cuando una empresa decide llevar datos a la nube. El primero es Bring Your Own Key (BYOK). “En la nube, los datos residen físicamente en el proveedor de servicios cloud (CSP). Lo que nCipher propone con Bring Your Own Key es

JOSÉ MARÍA PÉREZ ROMERO, NCIPHER

que las empresas sean capaces de generar sus propias claves de cifrado, en local, dentro de un HSM y decidiendo lo que pueden o no hacer con esa clave", explicó José María Pérez. Luego pueden exportarla de forma segura a la nube, para que allí solo se use dicha clave. Este proceso, además, es auditable a todos los niveles, desde que se genera la clave y hasta que se sube a cloud, aportando un sistema de seguridad, y resultado accesible para todo tipo de clientes.

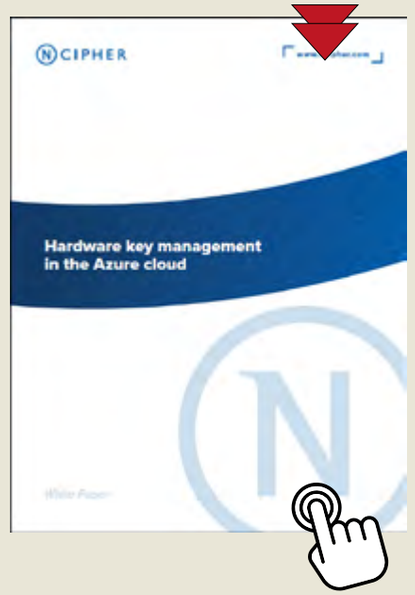
Otro método para aportar seguridad en el cifrado cuando se trabaja en un entorno mixto es Hold Your Own Key (HYOK). Hold Your Own Key está orientado a empresas que tengan contratado Microsoft RMS. Básicamente en estas estructuras, los datos no se encuentran en cloud, sino que están en las oficinas del cliente, en el data center. Lo que está en cloud es la política, lo que decide qué aplicación o usuario puede acceder a una determinada información. Esto se conoce como la Azure Information Protection Policy.

A diferencia del primer método, Bring Your Own Key, en el que la clave del cliente se genera y se sube a un HSM de nCipher que está en Azure, en el segundo, Hold Your Own Key, se trabaja con un HSM on premise. Al final, lo más importante, es que las claves del cliente nunca quedan fuera del HSM. Y es que, si se produce un incidente de robo de datos nadie quiere resultar damnificado. Aunque una empresa no dependa de una determinada normativa (requisitos normativos o compliance) es positivo que opte por implantar medidas (custodia) para no tener que lamentarlo, aunque confíen en un Service Provider de alto nivel.

Ve la intervención de nCipher en la sesión online Tendencias y oportunidades de la nube. ■

Si te ha gustado este artículo, compártelo

GESTIÓN DE CLAVES DE HARDWARE EN AZURE



La administración de claves criptográficas, que son los grandes números que utilizan los sistemas de cifrado para alimentar los algoritmos que convierten el texto sin formato en texto cifrado, es fundamental para la integridad de cualquier sistema criptográfico. Una vez comprometidas, las claves son inútiles y se pierde toda la protección de datos. Si la criptografía es el arte de hacer que las cosas sean secretas, entonces la administración de claves es el arte mediante el cual las mantenemos en secreto.

Los sofisticados sistemas criptográficos modernos utilizan dispositivos especializados llamados Módulos de seguridad de hardware (HSM) para crear, administrar y usar claves. Microsoft Azure Key Vault eligió los HSM de la línea de productos nCipher nShield para proteger las claves de sus clientes.

ALEJANDRO SOLANA,
RESPONSABLE TÉCNICO PARA INTEGRADORES DE SISTEMAS DE NUTANIX PARA ESPAÑA Y PORTUGAL

“La idea de simplicidad pasa por convertir el centro de datos en un Lego, compuesto por distintas piezas hardware que funcionan como una entidad y que con un clic de ratón reciben su rol”

La cloud lo está cambiando todo. Desde ese punto de partida, Alejandro Solana, Responsable Técnico para Integradores de Sistemas de Nutanix para España y Portugal, hace referencia en su intervención en el IT Webinar Tendencias y oportunidades de la nube, a cómo, hoy por hoy, la necesidad de que convivan aplicaciones y el volumen de datos tradicional con nuevas formas y servicios que demandan una agilidad muy importante han puesto en un brete a los departamentos de TI. Ante esta realidad, ha sido necesario mover ficha. Al final surge el cloud público y lo cambia todo.

Ahora bien, para que estos datos y aplicaciones puedan convivir entre los diferentes entornos, Nutanix plantea hacer la infraestructura lo más invisible posible para que finalmente las organizaciones y los departamentos de TI puedan elegir dónde ejecutar

ALEJANDRO SOLANA, NUTANIX

cada tipo de carga en función a tres parámetros fundamentales: rendimiento, coste y seguridad. La idea es, según Alejandro Solana, "que cada pieza del centro de datos funcione como una entidad y el cloud público, considerado también como otro componente más, pueda ser integrado dentro de una infraestructura invisible".

Para lograr esa invisibilidad, Nutanix propugna la misma aproximación que para la infraestructura; esto es, garantizar que cualquier organización tenga una visibilidad completa de dónde se están ejecutando sus cargas, su coste, rendimiento y, sobre todo saber si la seguridad está en el cloud, en el edge o en la cloud privada. En este sentido, plantean una automatización de las operaciones para garantizar el rendimiento y la operativa del día a día, una gestión automatizada del ciclo de vida, tanto de aplicaciones como de datos, y una consola de gestión de gobierno que ofrezca una visión de 360º del centro de datos en las distintas piezas: on premise o en el cloud público. Esa visibilidad absoluta permitirá también romper la barrera física del compliance dando la posibilidad de elegir, siempre y cuando se cumplen las regulaciones, migrar las aplicaciones y datos a la cloud pública.

Además de esa capacidad de conocer cómo se está cumpliendo con las normativas del cloud, migrar a una infraestructura invisible administrada en modo one clic, donde la gestión es homogénea y las piezas se consumen bajo demanda, ayuda a las empresas a disminuir el tiempo de operaciones y las paradas no planificadas. Al reducirse los incidentes, las organizaciones pueden centrase en los servicios que tienen que proporcionar y en los datos que van a consumir.

Ve en este enlace la intervención de Nutanix en la sesión online Tendencias y oportunidades de la nube. ■

Si te ha gustado este artículo, compártelo

ANTONIO PIZARRO, HEAD OF CLOUD ENTERPRISE SOLUTIONS DE OVH

“A la hora de elegir un modelo multicloud para trabajar los clientes no solo valoran el aspecto tecnológico, también la gobernabilidad”

El cloud está evolucionando en todas las áreas de TI y lo hace, además, por la injerencia de otras tecnologías. Al respecto de esta nube inteligente que encontramos en la actualidad, Antonio Pizarro, Head of Cloud Enterprise Solutions de OVH, destacó en su participación en el IT Webinar Tendencias y oportunidades de la nube, cómo este desarrollo ha venido propiciado, entre otras, por el incesante crecimiento del volumen de datos, lo que ha derivado en mayores necesidades de almacenamiento, escalabilidad y flexibilidad. La entrada de tecnologías como IoT, Edge computing o 5G también ha alimentado ese crecimiento de la información. En este punto, el cloud ha surgido como una pieza clave para dar solución a estas nuevas necesidades.

Respecto al tipo de segmento cloud que más se está consumiendo, Pizarro reconoce que la tendencia ha cambiado: “hoy por hoy, el seg-

ANTONIO PIZARRO, OVH

mento que más crece es el de IaaS, frente a Saas o PaaS, y eso es porque la velocidad de adaptación a las nuevas tendencias se hace mucho más rápido sobre un IaaS". Asimismo, el poder trabajar con estándares abiertos y tener la opción de elegir en cada momento qué tipo de infraestructura utilizar, le otorga una flexibilidad mayor.

En lo que concierne a los distintos actores que concurren en el sector de proveedores globales de hiperescala, Pizarro contempla cierta ventaja en el hecho de que OVH sea una empresa europea, ya que ese aspecto le permite responder con mayor solvencia a retos como la gobernabilidad del dato, un aspecto crucial para las empresas europeas.

Según Pizarro, OVH es el único proveedor europeo de hiperescala. Su oferta de SMART Cloud puede entenderse así: una cloud (S)imple y rápida de implementar; (M)ultilocal; (A) sequible y predecible; una cloud Reversible (R), abierta e interoperable; y (T)ransparente en precios.

Además de a las tendencias, Pizarro se refiere también a las oportunidades que está obteniendo OVH de su oferta cloud y que se traducen, entre otras, en contar con una oferta de clientes diversa, desde empresas especializadas en software a otras pertenecientes al sector bancario o financiero y para las que la seguridad y la ley, a la hora de acatar GDPR, es crucial: "uno de los principales problemas a la hora de migrar a la nube es cumplir con el aspecto legal, sobre todo, cuando se trata de cargas críticas", apunta.

Como conclusión y tras presentar un proyecto tecnológico práctico, este responsable reflexiona sobre la realidad actual de la nube. Según él, es posible migrar a cloud y moverse en entornos multicloud y abiertos, de múltiples modos y, sobre todo, de forma sencilla.

Visualiza la intervención de OVH en la sesión online Tendencias y oportunidades de la nube, aquí. ■

Si te ha gustado este artículo, compártelo

MIGRACIÓN DE DATACENTERS EN CALIENTE

Actualizar versiones que ya no reciben soporte del editor, ampliar la extensión de un datacenter o sustituirlo, implementar planes de recuperación ante desastres...: existen muchas circunstancias en las que puede ser necesario mover cargas de trabajo (workloads) entre diferentes centros de datos.

HCX, de VMware, es la tecnología en la que se basa la migración de las cargas de trabajo hacia la plataforma Private Cloud de OVH. Además de gestionar la migración segura de las cargas de trabajo, esta tecnología favorece una transición transparente garantizando la conexión de red entre el datacenter de origen y el de destino.

ÓSCAR ARRIAGA, SENIOR ACCOUNT MANAGER DE RETARUS

“Las empresas están invirtiendo cada vez más en soluciones de seguridad y en plataformas de servicios cloud con la intención de mejorar sus servicios hacia sus clientes”

Desde la perspectiva de que el principal reto al que se enfrentan las empresas que quieren adoptar la nube es el de gestionar de un modo adecuado el flujo de información, Óscar Arriaga, Senior Account Manager de Retarus, habló durante su participación en el webinar Tendencias y oportunidades de la nube, de la importancia que ha adquirido la nube, sobre todo los servicios cloud, y del modo en que Retarus puede ayudar a las empresas a administrar y a proteger la información que generan y mueven en sus canales de comunicación.

Según sus datos, un 50% de las empresas ya tiene implementado algún tipo de servicio cloud por lo que conceptos, como nube híbrida o entornos multicloud, y de modelos de servicios como Iaas, SaaS o PaaS, son tratados con naturalidad. De hecho, muchas organizaciones están desarrollando su estrategia IT con base

ÓSCAR ARRIAGA, RETARUS

en este tipo de soluciones y los servicios cloud son el segmento que más ha crecido durante 2019. A partir de esta evolución, ¿qué necesitan o demandan las empresas?

Para Arriaga, un intercambio de información fiable y seguro es la base de todo proceso comercial. Como experto en logística de comunicaciones, amplia experiencia y centros de datos altamente disponibles a nivel mundial, Retarus permite que clientes, infraestructura y procesos de negocio se comuniquen de un modo eficiente con sus partners de comunicación, ya sean proveedores, clientes o usuarios, independientemente del canal de comunicación que utilicen (SMS, email o fax), de un modo transparente, mejorando el rendimiento, aportando trazabilidad y un reporting detallado para corregir incidencias.

A nivel de seguridad, "Retarus protege las comunicaciones de sus usuarios ya sea vía TLS, VPN o MPLS, con una gestión y control unificado a través de su portal EAS". Asimismo, los clientes obtienen los principales beneficios que buscan de los servicios cloud: simplicidad operativa, reducción de costes y mejora del rendimiento, de mano de un proveedor no intrusivo y totalmente transparente con sus clientes.

Arriaga compartió también algunos ejemplos de clientes, de diferentes verticales de mercado, y con los que han desarrollado proyectos de éxito. A muchos de ellos, reconoce, les han ayudado a incrementar el tráfico y el volumen de sus procesos transaccionales.

En lo que respecta a la adopción del cloud, y tras años desarrollándose, Arriaga observa que hoy ese avance hacia la nube se está produciendo de un modo mucho más seguro. En este sentido, concluye, "las empresas están invirtiendo cada vez más en soluciones de seguridad para cloud y en las plataformas de servicios cloud con la clara intención de mejorar los servicios ofrecidos a sus clientes".

Ve la intervención de Retarus en Tendencias y oportunidades de la nube. ■

Si te ha gustado este artículo, compártelo

FRAUDES CXO, PHISHING Y RANSOMWARE

Una gran parte del correo electrónico ya consiste en mensajes no solicitados. Además de la avalancha de correos electrónicos ordinarios de spam y virus, la empresas y los empleados están cada vez más expuestos a amenazas complejas como los ataques de ingeniería social y phishing. A menudo, los mecanismos de seguridad tradicionales ya no ofrecen suficiente protección contra estos correos electrónicos individualizados. Además, el malware también va mutando a intervalos cada vez más cortos y circula en variantes siempre nuevas. Con las soluciones de seguridad tradicionales resulta complicado distinguir estos correos electrónicos de los mensajes legítimos.

ÓSCAR LÓPEZ SÁNCHEZ, INGENIERO PREVENTA DE SOPHOS IBERIA

“Uno de los grandes desafíos para los clientes es gestionar distintas clouds. En ocasiones, hay una falta de visibilidad”

Por la agilidad y escalabilidad que confiere, el ahorro de costes o el acceso inmediato a la información, la nube aumenta en importancia para las empresas. Partiendo de esta realidad, Óscar López Sánchez, Ingeniero Preventa de Sophos Iberia, evidenció durante su participación en la sesión Tendencias y oportunidades de la nube, la necesidad, también creciente, de protegerla, haciendo foco tanto en la propia infraestructura como en la información almacenada. Y es que la seguridad cloud debe ser, según López, una responsabilidad compartida entre los proveedores de nube pública, responsables de la seguridad de la nube, y las empresas, encargadas de proteger lo que se coloca en ella (redes, VPNs...) e incluso actualizar aplicaciones y el contenido.

Como mecanismos de protección, las empresas pueden optar por una estrategia de seguridad basada en soluciones tradicionales como

ÓSCAR LÓPEZ SÁNCHEZ, SOPHOS

firewalls, endpoints o herramientas de monitorización. En este sentido, Sophos cuenta con Intercept X, una solución destinada a salvaguardar todo tipo de servidores (físicos o virtuales) que aúna protección contra amenazas con la detección y respuesta para endpoints (EDR) ofreciendo visibilidad completa. Dicha solución, puede complementarse con Sophos XG Firewall, para proteger todos esos dispositivos.

Por otro lado, y partiendo de la base de que la seguridad no entiende de tamaños -los ataques en muchas ocasiones son aleatorios y buscan puertos que estén abiertos-, la visibilidad ininterrumpida de la infraestructura de la nube pública es trascendental para que las empresas sepan qué están protegiendo y acaten el cumplimiento. Sin embargo, esto es a veces complicado: el uso de múltiples clouds (AWS, Microsoft Azure o Google Cloud), la evolución de las infraestructuras (uso de contenedores, kubernetes, etc.) y del software (prácticas de DevOps) o la propia naturaleza cambiante de la nube, dificultan este trance.

Sophos da respuesta a estos retos con Sophos Cloud Optix, una solución que ofrece visibilidad inteligente, identifica los procesos de cumplimiento y ofrece respuesta ante ataques. Cloud Optix permite conocer el inventario de las cargas de trabajo en cloud, las configuraciones y el tráfico de red a través de algoritmos de Inteligencia Artificial (IA) avanzados.

El sistema de alertas inteligentes basadas en IA permite ver qué sucede en los dispositivos, si hay puertos abiertos que no deberían estarlo, ransomware... pero también, gracias a la clasificación automatizada de alertas combinada con la información contextual, conocer si lo que está sucediendo en un momento determinado es normal. Cloud Optix también simplifica y acelera los procesos de seguridad mediante integraciones con herramientas de terceros como JIRA, Splunk, Amazon Guardduty, etc.

Accede a la intervención de Sophos en la sesión online Tendencias y oportunidades de la nube. ■

Si te ha gustado este artículo, compártelo

PROTEGER LA NUBE PÚBLICA: SIETE PRÁCTICAS RECOMENDADAS

Crear nuevas instancias en Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP) es sencillo. Lo difícil para los equipos de operaciones, seguridad, desarrollo y cumplimiento es llevar un registro de los datos, las cargas de trabajo y los cambios de arquitectura en esos entornos para mantener la seguridad en todos los frentes. Si bien los proveedores de la nube pública se encargan de la seguridad de la nube (los centros de datos físicos y la separación de los entornos y los datos de los clientes), la responsabilidad de proteger las cargas de trabajo y los datos que coloca en la nube recae rotundamente sobre usted. Del mismo modo que necesita proteger los datos almacenados en sus redes locales, también necesita proteger su entorno en la nube. Los malentendidos en torno a esta distribución de la propiedad son muy frecuentes y las brechas de seguridad resultantes han hecho que las cargas de trabajo basadas en la nube sean el nuevo tesoro que codiciar para los habilidosos hackers de hoy en día.

ANA ROCHA DE OLIVEIRA, CLOUD BUSINESS DEVELOPMENT MANAGER DE RED HAT PARA ESPAÑA Y PORTUGAL

“En los últimos años estamos viendo un cambio cultural en cloud. La colaboración entre los distintos equipos empresariales está ayudando al éxito de estos proyectos”

Continuando con las tendencias del mundo cloud, Ana Rocha de Oliveira, Cloud Business Development Manager de Red Hat para España y Portugal, inició su interlocución en el webinar Tendencias y oportunidades de la nube, hablando sobre el gran cambio cultural que se ha producido en los últimos años a nivel empresarial: “la colaboración entre los distintos equipos empresariales está ayudando al éxito de los proyectos cloud”.

Desde 2011, Red Hat se centra en la nube híbrida que es, según Rocha la arquitectura más idónea para la provisión de servicios, independientemente del entorno (físico, virtual o nubes públicas, privadas). Del mismo modo, el desarrollo de aplicaciones cloud nativas permiten aprovechar rápidamente los beneficios que los entornos cloud dinámicos y modernos posibilitan, sin olvidar, la importancia de la orquestación, el gobierno y la au-

ANA ROCHA DE OLIVEIRA, RED HAT

tomatización para optimizar y proteger estos nuevos entornos.

En este sentido, la visión Open Hybrid Cloud de Red Hat pasa por considerar el dato como un elemento fundamental de las arquitecturas multi cloud y por evitar que los silos que existían en las estructuras tradicionales se repitan en los entornos multicloud públicos. Por ello, es muy importante la capacidad de abstraer y portar los datos, independientemente del entorno.

En cuanto a cómo está siendo el ritmo de adopción de estas arquitecturas, lo cierto es que "a pesar de que hace tiempo se esperaba un índice de adopción cloud muy elevado, la realidad es que las cargas críticas que están en cloud no llegan al 20%". Para tener una arquitectura exitosa y acelerar esa adopción hay tres puntos a tener en cuenta: crear una forma de trabajo que permita mover esas aplicaciones entre los distintos entornos, establecer políticas de seguridad consistentes y automatizar y gestionar recursos.

Sin embargo, existen barreras que están frenando esa adopción como la necesidad de reducir los costes, la falta de conocimiento de los equipos, la resistencia organizativa y la integración con el ecosistema existente.

Muy importante dentro de la cloud híbrida ha resultado el código abierto, un modelo de desarrollo que está permitiendo una rápida transformación en las empresas. Como conclusión, Rocha indica que, hoy por hoy, Open Source tiene futuro en el mercado español. La responsable cita e ilustra el caso de éxito de tres grandes clientes que han apostado por tecnologías de código abierto para cambiar y mejorar su cultura organizativa.

Visualiza la participación de Red Hat en el webinar Tendencias y oportunidades de la nube, aquí. ■

Si te ha gustado este artículo, compártelo

RESPUESTA ANTE EL CAMBIO CONSTANTE

Hoy en día, prácticamente todos los aspectos de una empresa están experimentando cambios: los clientes demandan un flujo continuo de nuevos servicios; la organización se enfrenta a una competencia creciente, y la tecnología avanza rápidamente. Muchas organizaciones están utilizando capacidades y tecnologías digitales para crear nuevos modelos de negocio, productos y servicios. De hecho, el 88 % de las empresas actualmente desarrollan experiencias digitales. Este informe refleja las opiniones de 1052 clientes de Red Hat sobre sus planes y prioridades para 2019, analizando las motivaciones para el cambio, las prioridades de financiamiento y los desafíos de alcanzar el éxito.

Encuentros IT Trends

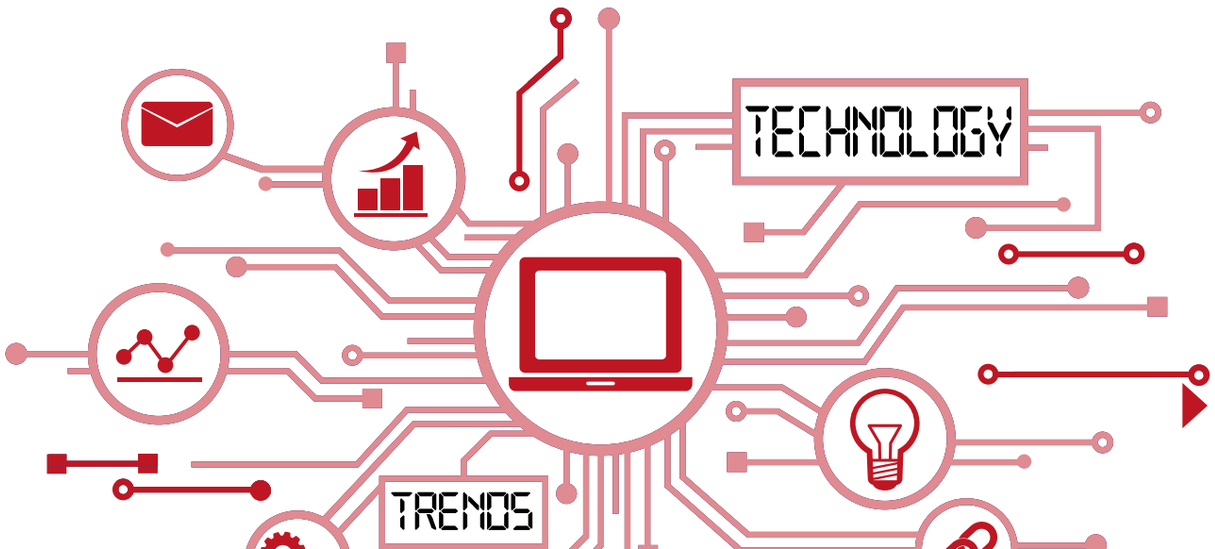
Reducir las vulnerabilidades, mejorar la seguridad de la red, hacer uso de automatización y otros procesos que mejoren la eficiencia, o aumentar la privacidad y el cumplimiento de los datos son algunos de los objetivos que las empresas deberían marcarse de cara al próximo año para mejorar la seguridad.

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

Únete a nosotros en este **Encuentros IT Trends sobre Ciberseguridad en 2020** y descubre qué ocurre en el mundo del cibercrimen, qué tipos de ataques se están produciendo y cómo pueden afectar a tu empresa. Y sobre todo, qué nos espera en 2020.

Las grandes tendencias tecnológicas están dando forma y remodelando la manera en la que se hacen los negocios y se ve el mundo. Están redefiniendo el futuro y es importante que nos aseguremos de que estas tendencias sean útiles para el negocio.

De manera constante, las propias tendencias tecnológicas evolucionan, dando nuevos ritmos a los mercados. ¿Cuáles son esas grandes tendencias tecnológicas? ¿Cómo puedo aplicarlas a mi negocio? ¿Qué retos nos traen? ¿Cuáles son sus beneficios?
Ve el **Encuentro IT Trends Tendencias TI 2020**, visionando el futuro, en el que daremos respuesta a todas estas cuestiones.



La ingeniería social, combinada con ciberataques como LockerGoga, WannaCry, non-Petya, Triton, Sauron, DragonFly y muchas de sus mutaciones, han demostrado que los sistemas industriales digitalizados son muy vulnerables y son un objetivo muy atractivo para los atacantes.

INDUSTRIA 4.0

Las estrategias de ciberseguridad industrial necesitan un replanteamiento radical

El cambio de paradigma generado por la Industria 4.0 e Internet de las Cosas Industrial (IIoT) está mejorando significativamente las capacidades digitales y de conectividad de los Sistemas de Control Industrial (ICS) en múltiples verticales, pero también ha abierto las puertas a graves riesgos de ciberseguridad que amenazan con causar daños a las operaciones industriales por miles de millones de dólares. A pesar del peligro inminente, la inversión en ciberseguridad dentro del mercado de ICS se está quedando muy rezagada, ya que apenas superará los 2.000 millones de dólares en 2025, según ABI Research.

"Los ICS están, literalmente, impulsando las industrias más importantes y críticas del mundo. Un ciberataque bien ubicado puede causar víctimas humanas, miles de millones en daños a la infraestructura e incluso paralizar ciertas operaciones de la infraestructura crítica de un país ", advierte Dimitrios Pavlakis, analista industrial de ABI Research. La ingeniería social, combinada con ciberataques como LockerGoga, WannaCry, notPetya, Triton, Sauron, CrashOverRide, DragonFly y muchas de sus mutaciones, han demostrado que los sistemas industriales digitalizados no solo son muy vulnerables, sino que también son un objetivo muy atractivo para los ciberataques.

La raíz del problema es la yuxtaposición de TI y OT. Se espera que la integración de la seguridad de TI absorba casi el 80% de la seguridad de ICS en 2019, liderada principalmente por implementaciones exitosas de sistemas de Información de Seguridad y Gestión de Eventos (SIEM). Se espera que eso caiga por debajo del 70% para 2025, cuando otras fuentes de inversión, como la gestión de activos de OT, inteligencia de amenazas, encriptación y gestión de identificación, aumenten considerablemente. Además, aunque la inteligencia de amenazas, el cifrado y la gestión de la identificación en ICS se iniciarán lentamente, se espera que su inversión aumente casi el triple en los próximos cinco años.

"Las estrategias de ciberseguridad industrial necesitan un replanteamiento radical y deben construirse desde la base de la OT para hacer frente al panorama de amenazas en evolución. Personalizar la seguridad de TI y colocarla en un entorno de OT no es la respuesta, pero es un ejemplo de una estrategia que indica la confusión inherente con respecto al panorama de ciberseguridad de ICS ", apunta Pavlakis. No es una tarea fácil alejarse de los modelos tradicionales y abrazar la premisa subyacente de la Industria 4.0 para ICS. Los mismos procedimientos de seguridad, protocolos, protección de red / usuario / dispositivo y gestión de ID que tienen sentido en entornos de TI corporativos no se pueden aplicar a entornos industriales. Hacerlo no solo servirá para exacerbar el problema subyacente de "TI contra OT", sino que también dificultará gravemente las operaciones de seguridad y la integración de productos de seguridad con equipos ICS en general.

6 riesgos de ciberseguridad de las utilities

Pese a la creciente digitalización de su infraestructura, solo el 55% del gasto total en seguridad de las utilities en los próximos 5 años se destinará a proteger esa infraestructura inteligente y conectada. Ello expondrá a las empresas del sector a múltiples riesgos de seguridad.

Según un informe técnico de ABI Research, la industria de las utilities invertirá 14.000 millones de dólares al año entre 2018 y 2023 en modernizar su infraestructura, lo que representa un total de 84.000 millones durante ese período. Si bien las inversiones en infraestructura digital se mantendrán muy altas durante los próximos años, las inversiones para asegurar esa infraestructura quedarán rezagadas, ya que solo el 55% del gasto total en seguridad en los próximos 5 años se destinará a proteger la infraestructura inteligente.

De acuerdo con la consultora, los 6 riesgos de seguridad más frecuentes en la industria de las utilities son los siguientes:

- **Actividad no autorizada en sistemas críticos que no ha sido detectada.**
- **Acceso físico no autorizado a actores maliciosos**
- **Asignación de recursos deficiente**
- **Mínima funcionalidad (aumento de vectores para acceso por parte de actores maliciosos)**
- **Identificación y autenticación (falta de responsabilidad y trazabilidad)**
- **Administración de cuentas (comunicaciones de contraseñas no seguras comprometidas)**

"Aumentar la inversión en infraestructura de seguridad sin obstaculizar los objetivos operacionales industriales, administrar la convergencia IT-OT en un enfoque simplificado, desarrollar nuevos KPI para las operaciones de ciberseguridad, forzar la evolución de los SIEM y los SOC para ICS, y atender las crecientes preocupaciones de las ciberamenazas transmitidas por IA, son los componentes esenciales y deben utilizarse como los elementos fundamentales para el desarrollo de cualquier estrategia de ciberseguridad de ICS", concluye Pavlakis.

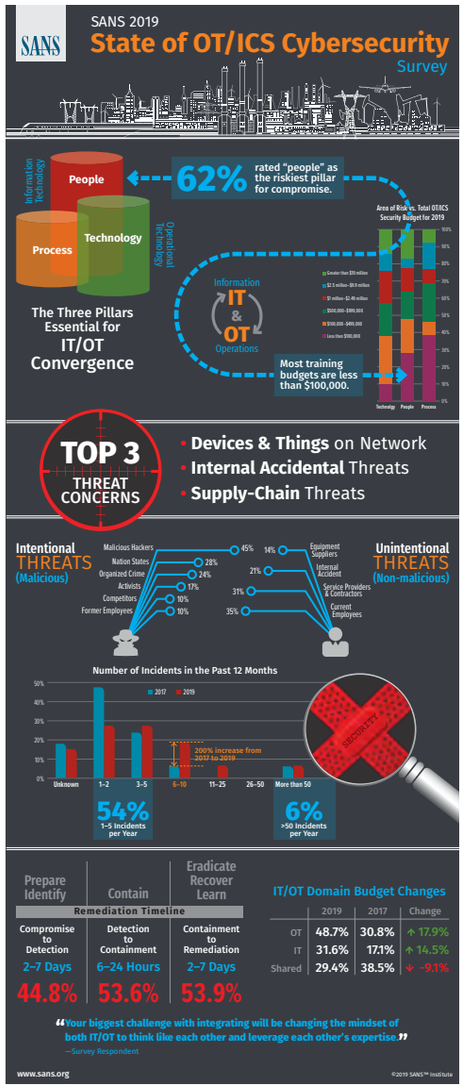
LAS PERSONAS, EL MAYOR RIESGO PARA LA SEGURIDAD INDUSTRIAL

Más de la mitad de los profesionales de seguridad de estos entornos considera que los ciberriesgos son altos o más altos que en años anteriores. La identificación de los recursos conectados, la mejora de la visibilidad de los dispositivos, la red y los sistemas de control es un problema.

SANS Institute publicó recientemente un estudio sobre Ciberseguridad OT/ICS, que revela que más de la mitad de los profesionales de seguridad consultados para el informe considera que los ciberriesgos son altos o más altos que en años anteriores. El 62% cree, además, que las personas son el mayor riesgo para la ciberseguridad, seguidos por la tecnología (22%) y los procesos y procedimientos (14%).

"La preocupación obvia por el riesgo que representan las personas, ya sean profesionales malintencionados con acceso a información privilegiada o empleados descuidados, es consistente en todas las industrias", señala Barbara Filkins, coautora del estudio y Senior Analyst de SANS. "Nos sorprendió la menor preocupación mostrada en torno a los procesos, teniendo en cuenta que existe una complejidad significativa inherente al diseño, la implementación y las operaciones de los ICS para salvaguardar los sistemas OT".

Los encuestados reconocieron que la identificación de los recursos conectados, la mejora de la visibilidad de los dispositivos, la red y los sistemas de control sigue siendo un problema: el 45,5% lo considera un foco de atención principal para sus organizaciones. A esto se suman las preocupaciones tradicio-



Clica en la imagen para ver la imagen más grande

Un ataque de ransomware paraliza la producción de ASCO Industries

ASCO Industries, compañía belga dedicada a la fabricación de componentes para aviones tanto civiles como militares, fue víctima de un ataque de ransomware el pasado 7 de junio, lo que le obligó a paralizar la producción en todo el mundo.

La compañía fabrica partes de aviones para Airbus, Boeing, Bombardier Aerospace, Lockheed Martin y el nuevo avión de combate F-35, y cuenta con plantas en Bélgica, Alemania, Canadá y Estados Unidos, además de oficinas en Brasil y Francia. Aunque la infección se produjo en la planta de producción de Bélgica, las plantas en el resto de las ubicaciones se cerraron como precaución para evitar que el ransomware se propagase por toda la red, enviando a casa a 1.000 de sus 1.400 empleados.

nales de seguridad de TI, en las que la identificación y el seguimiento de los recursos y las redes sigue siendo un reto. No es de extrañar que los dispositivos móviles y las soluciones de comunicaciones inalámbricas contribuyan a aumentar los riesgos generales y la exposición a las amenazas. La creciente adopción y evolución de los servicios en la nube representa asimismo un riesgo adicional al quedar expuestos a nuevas amenazas que deben ser comprendidas y abordadas.

"Sabemos por investigaciones previas de SANS que la incorporación de 'cosas' y dispositivos móviles a ICS representa un riesgo significativo", afirma Doug Wylie, coautor de la encuesta y director de la división SANS Industrials & Infrastructure, añadiendo que "la hiperconectividad y la rápida introducción de nuevas tecnologías en el OT está proporcionando un valor tangible, pero la complejidad añadida que viene con cada una de ellas sigue superando la preparación de los encargados de salvaguardar los sistemas actuales de las ciberamenazas". ■

Casi 4 de cada 10 sistemas de control de edificios inteligentes han sido atacados

El 37,8% de los ordenadores utilizados para controlar los sistemas de automatización de edificios inteligentes fueron objeto de algún tipo de ataque malicioso en la primera mitad de 2019, según una investigación de Kaspersky. Este estudio muestra que, si bien no está claro si tales sistemas fueron atacados deliberadamente, a menudo se convierten en un destino de varias amenazas genéricas. A pesar de no ser sofisticadas, muchas de estas amenazas pueden representar un peligro significativo para las operaciones cotidianas de edificios inteligentes. De los casi 4 de cada 10 ordenadores de administración de sistemas de edificios inteligentes que fueron atacados, más del 11% fueron atacados con diferentes variantes de spyware, destinadas a robar credenciales de cuenta y otra información valiosa. También detectaron gusanos en el 10,8% de las estaciones de trabajo; el 7,8% recibió estafas de phishing, y el 4,2% encontró ransomware. La mayoría de estas amenazas provienen de Internet, con el 26% de los intentos de infección nacidos en la web. Los medios extraíbles, como memorias USB, discos duros externos y otros, fueron responsables del 10% de los casos; el 10% afrontó amenazas a través de enlaces de correo electrónico y archivos adjuntos; y otro 1,5% fueron atacadas desde fuentes dentro de la red de la organización, como las carpetas compartidas.

En lo que respecta a la prevalencia de ataques en diferentes territorios, con un 48,5%, Italia registró el mayor porcentaje de ordenadores de edificios inteligentes atacados, seguido de cerca por España, con un 47,6%; y Reino Unido, con un 44,4%.

MÁS INFORMACIÓN

- SANS Institute Cybersecurity OT/ICS State 2019
- Los ciberataques a tecnologías operativas siguen aumentando
- Los CISO se enfrentan a ataques cada vez más sofisticados
- Cómo lograr que las ciudades inteligentes sean seguras
- El cibercrimen en la industria financiera crece un 1.000%

Ciberseguridad industrial, protegiendo el sector productivo

La digitalización de la industria ha abierto nuevas posibilidades para este sector, básico para cualquier economía. La Industria 4.0 combina y conecta tecnologías físicas y digitales, creando organizaciones más flexibles, capaces de responder a nuevas demandas y de estar interconectadas para así tomar decisiones mejor formadas.

Pero los ataques a sistemas industriales van en aumento. Y no se trata de una intuición, sino de una realidad respaldada por los datos. Además de los riesgos propios de ser atacados como organizaciones, los ataques a sistemas industriales que manejan estas organizaciones hacen que las consecuencias puedan ser aún peores. Hablamos de tiempos de inactividad de la producción, el deterioro de los productos y el daño al equipo, así como las pérdidas financieras y de reputación.

Hacer frente a estos ciberataques en el sector industrial pasa por abordar una estrategia de ciberseguridad adecuada que se integre completamente en la estrategia de la organización combinando la tecnología operativa (OT) y la tecnología de la información (TI).

En este IT Webinars hemos reunido a expertos del sector para hablar de la situación de la ciberseguridad industrial y las mejores estrategias para abordarla. Contamos con Kaspersky, Stormshield, Sothis, Nozomi Networks y Forescout. 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. ■

Pedro García (Kaspersky)

Borja Pérez (Stormshield)

Enrique Martín (Sothis)

Vesku Turtia (Nozomi)

Ricardo Hernández (Forescout)

PEDRO GARCÍA VILLACAÑAS, DIRECTOR PREVENTA DE KASPERSKY PARA IBERIA

“La mayoría de los ataques contra industria son APTs. Las empresas necesitan integrar tecnología muy sofisticada para detectar esos ataques”

Desde el punto de vista de la seguridad, la industria 4.0 está viviendo una serie de cambios. Así lo advirtió Pedro García Villacañas, Director Preventa de Kaspersky para Iberia, al inicio de su intervención en el IT Webinar Ciberseguridad industrial, protegiendo el sector productivo, al señalar que “cuando los procesos de sistemas de control industrial comenzaron a utilizar recursos disponibles en Internet, se abrieron distintas posibilidades de ataques y diferentes riesgos para todas las empresas que utilizan Sistemas de Control Industrial”.

Ahora bien, dado que en el sector industrial es prioritario que la producción no se detenga nunca, modificar estos Sistemas de Control es una acción casi impensable. En este contexto, Kaspersky mantiene acuerdos con diferentes fabricantes de sistemas para reportar distintas

PEDRO GARCÍA VILLACAÑAS, KASPERSKY

vulnerabilidades a fin de que la producción no se vea afectada, tal y como detalló en la sesión.

Por otro lado, y en lo que respecta a equipos o soluciones de seguridad para el sector industrial, García Villacañas matizó que, "hoy por hoy, hay pocos específicos para industria. Muchas empresas siguen utilizando soluciones de seguridad para IT que no ofrecen respuestas para OT".

Para solucionar estos retos, Kaspersky cuenta con Kaspersky Industrial CyberSecurity (KICS), una solución holística, completa y basada en una serie de productos para la protección de los sistemas, tanto a nivel de endpoint como de red, y la provisión de servicios (concienciación, evaluación de la seguridad o formaciones específicas a los equipos de seguridad).

Esta solución integra, entre otras, un módulo destinado a proteger los nodos. Dicho módulo permitir verificar de forma periódica la integridad del PLC como objeto de ataques, de modo que, si se produce alguna alteración, se genere un evento alertando sobre la integridad del proyecto. Adicionalmente, también incluye otro módulo para redes, una solución tipo appliance que se incorpora en un servidor y recoge todo el tráfico de red. Se trata de una solución pasiva, no proactiva, a fin de que la producción no se vea detenida. Permite tener visibilidad y control sobre la red y recibir alertas en tiempo real.

Además de soluciones enfocadas en la industria, Pedro García expuso también la importancia que supone para Kaspersky ofrecer una serie de valores adicionales tanto para IT como para OT, con los que proteger a sus clientes de las amenazas conocidas y desconocidas y de aquellas, como las APTs, que solo pueden ser detectadas con tecnología sofisticada.

Por último y en lo que atañe al nivel de concienciación que tienen las empresas e instituciones sobre la importancia de la seguridad en la industria 4.0, Pedro García afirmó que dicho trabajo (de concienciación) está funcionando más a nivel corporativo que a escala institucional, donde todo discurre siempre más despacio. No obstante, reflexionó, aún queda mucho camino por recorrer.

Ve aquí la intervención de Kaspersk en Ciberseguridad industrial, protegiendo el sector productivo. ■

EL ESTADO DE LA CIBERSEGURIDAD INDUSTRIAL

Este estudio pretende saber cuál es el estado de los Sistemas de Control Industrial (ICS), así como las prioridades, preocupaciones y desafíos que conlleva para las organizaciones industriales. El objetivo de la investigación fue comprender las medidas y procesos involucrados en la prevención de incidentes cibernéticos en la industria. Este informe explora los resultados de la encuesta y es una continuación de las encuestas anteriores de ARC y Kaspersky sobre la ciberseguridad de ICS.

Si te ha gustado este artículo, compártelo

BORJA PÉREZ, COUNTRY MANAGER DE STORMSHIELD IBERIA

“Ya no existen redes OT aisladas. A través de sistemas IT, como aplicaciones para el control de producción, puede establecerse ese punto de conexión”

La industria 4.0 se enfrenta a una serie de riesgos. Borja Pérez, Country Manager de Stormshield Iberia, enumeró cinco retos que amenazan a la industria 4.0, en la sesión online Ciberseguridad Industrial, protegiendo el sector productivo, de IT Trends, y que parten de la distinción entre las redes OT, o redes de producción e infraestructuras críticas, y las redes IT tradicionales. Así, “el mundo industrial se enfrenta a ciclos de vida de las soluciones mucho más largos que en IT, múltiples protocolos, variedad de normas, distintas legislaciones o nuevas y mayores amenazas a su seguridad que están marcando su día a día”.

En este contexto, ya han tenido lugar ciertos ataques específicos contra el sector industrial, que por su virulencia han puesto de manifiesto una realidad: ya no hay redes OT aisladas. Cualquier red puede ser atacada y

BORJA PÉREZ, STORMSHIELD IBERIA

estas amenazas pueden entrar a través de los sistemas de TI.

Ante este panorama, Stormshield ofrece distintos tipos de soluciones de seguridad para proteger los sistemas OT y la convergencia IT/OT. Dentro de esta propuesta, Borja Pérez distinguió dos familias de productos: SNS Network Security, una solución de seguridad perimetral que incluye, entre otras funciones, DPI (Inspección Profunda de Paquetes) y filtrado para protocolos industriales, para la protección de los puestos de trabajo tanto de OT como de IT; y SES Endpoint Security, una solución no basada en firmas, que integra un agente protector de ordenadores industriales, apto para funcionar con sistemas operativos obsoletos (Windows XP) e idóneo para máquinas situadas dentro de infraestructuras críticas. Además de proteger el puesto de trabajo, SES asegura periféricos y entornos no conectados.

Del mismo modo, y aprovechando su pertenencia al grupo Airbus, Stormshield mantiene alianzas muy beneficiosas con empresas como Schneider, lo que le permite ampliar su conocimiento sobre los protocolos industriales y acercarse a los responsables de las redes OT, en ocasiones reacios a conocer a fabricantes de IT.

Sobre este último punto, Borja Pérez reconoció que Stormshield posee otra cualidad esencial que le está permitiendo crecer en este mercado: el hecho de ser un fabricante europeo, con la cualificación y las certificaciones europeas de más alto nivel y muy cuidadoso con la propiedad intelectual, es una cuestión que muchas industrias del continente están teniendo en cuenta a la hora de decantarse por este fabricante. Así, la empresa cuenta con clientes en sectores como el aeroportuario, hidroeléctrico, ferroviario o alimentario, entre otros.

Por último, Borja Pérez apuntó que, en la actualidad, se está viviendo un interés creciente por parte de los clientes industriales, pero antes lo tuvo el canal por integrar soluciones de seguridad efectivas. Dichas soluciones deben ser capaces de defender cualquier entorno: "a veces se habla de industria 4.0 cuando la realidad es que un mismo cliente puede tener una línea de producción 4.0 y otras tareas funcionando en 1.0, a la manera antigua". Por tanto, las soluciones de seguridad deben poder ser desplegadas y responder adecuadamente ante cualquier realidad.

Ve aquí la sesión de Stormshield en el IT Webinar, Ciberseguridad Industrial. ■

Si te ha gustado este artículo, compártelo

POR QUÉ LA SEGURIDAD INDUSTRIAL NO DEBE SER SUBESTIMADA

IT y OT, dos mundos que hasta hoy se mantenían independientes están mostrando signos de acercarse, pero deben aprender unos de otros para reducir los riesgos de ciberseguridad. A medida que los sistemas industriales tradicionales y la Tecnología Operativa (OT) se vuelven más conectados, las amenazas cibernéticas exclusivas de este sector representan un peligro significativo para la industria. Hay muchos ejemplos para resaltar la grave vulnerabilidad de muchos actores: energía, transporte, etc.
En este contexto, el ciberterrorismo puede dañar no solo la producción, sino también la imagen de los actores industriales. Establecer una política de seguridad que se adapte a esta industria hace un gran avance para protegerla contra las amenazas digitales y ayudarla a prepararse para el futuro de la industria con calma y cuidado.

ENRIQUE MARTÍN GÓMEZ, RESPONSABLE DE DESARROLLO DE NEGOCIO DE CIBERSEGURIDAD DE SOTHIS

“Una cosa que hemos aprendido en ciberseguridad industrial es que para proteger y controlar las redes debemos pasar de los sistemas de protección a los de monitorización”

¿Qué está ocurriendo en el mundo industrial desde el punto de vista de la seguridad? Enrique Martín Gómez, Responsable de Desarrollo de Negocio de Ciberseguridad de Sothis, explicó durante su tiempo en el webinar Ciberseguridad Industrial, protegiendo el sector productivo, que la integración del entorno OT con el de IT ha provocado que el primero, aislado en el pasado, se haya visto cada vez más amenazado, sufriendo ataques cibernéticos de los que antes no era objeto.

“Para entender el porqué de estas amenazas basta saber que los sistemas OT suelen integrar software sin actualizar, por lo que los ataques muy sofisticados tienen grandes probabilidades de éxito”, apuntó Martín. Del mismo modo, se trata de dispositivos muy antiguos, fabricados para estar siempre disponibles y no para ser seguros y que, en muchos casos, están protegiendo o

ENRIQUE MARTÍN GÓMEZ, SOTHIS

monitorizando infraestructuras críticas. Por tanto, son un objetivo muy apetecible para los atacantes.

Ahora bien, ¿qué hacer para mejorar esta situación y resolver esta problemática? Martín Gómez ofreció varias soluciones. "Por un lado, es ineludible conocer adecuadamente el entorno que tenemos en ciberseguridad industrial, tanto la parte industrial como la de seguridad, para poder desplegar mecanismos de protección adecuados. Asimismo, hay que cuidar la infraestructura de comunicación, vigilando y monitorizando las redes industriales para que en el caso de que se produzca algún incidente sea posible responder de un modo adecuado", dijo. El responsable de desarrollo de negocio también recordó la importancia de entender que las soluciones que antes utilizábamos en el mundo IT muchas veces no son válidas para OT. Se trata de entornos distintos, con diferentes amenazas y desiguales formas de resolver problemas.

En este sentido, Sothis cuenta con una propuesta 360º basada en la identificación de amenazas, de vulnerabilidades, la exposición al riesgo, el desarrollo de medidas de protección, el establecimiento de planes de contingencia y la respuesta ante incidentes de seguridad. Al igual que en IT, en las redes industriales es fundamental responder muy bien a los incidentes. Por tanto, es crucial trabajar la protección, pero, más aún, esa respuesta. Igualmente, las empresas deben adaptarse a una normativa, leyes y estándares de seguridad concretos.

Para terminar, Enrique Martín reflexiona en la sesión sobre cómo está calando este mensaje de responder de forma eficiente a las amenazas en el entorno industrial. Según este responsable, y aunque ya existe una concienciación, sobre todo en la alta dirección, aún queda mucho camino por recorrer, sobre todo en lo que se refiere a mejorar la respuesta a incidentes, conocer los protocolos que funcionan en las redes OT, y la adecuada integración con IT. El mundo industrial ya no es un entorno aislado sino integrado.

Ve aquí la intervención de Sothis en el webinar Ciberseguridad industrial, protegiendo el sector productivo. ■

Si te ha gustado este artículo, compártelo

VESKU TURTIA, DIRECTOR REGIONAL DE VENTAS PARA IBERIA DE NOZOMI NETWORKS

“En ocasiones, los profesionales de la seguridad alarmamos sobre el hecho de que, si no se hace una cosa bien, puede pasar algo malo. En OT, esto no es una exageración”

La demanda de soluciones de seguridad por parte del sector industrial es un hecho. Lo que antes pasaba en IT ahora está ocurriendo en OT, aunque haya plantas de producción que apenas tengan salida a Internet. A esta realidad, Vesku Turtia, Director Regional de Ventas para Iberia de Nozomi Networks, suma la inmensidad del sector OT, el cual abarca mucho más que una central nuclear o una planta eléctrica, tal y como explicó en la sesión online Ciberseguridad Industrial, protegiendo el sector productivo. “El mundo OT está en todos los sitios, incluso en una montaña rusa”, afirma Turtia.

Ante esta dimensión, y con un bagaje, el de sus fundadores, que arrancó en el sector de ciberseguridad IT hace ya muchos años, Nozomi es hoy una referencia clara en el sector de la ciberseguridad industrial. De hecho, este posicionamiento es el que ha permitido

VESKU TURTIA, NOZOMI NETWORKS

a esta compañía estar presente en muchos y diferentes mercados, como el de utilities, petróleo, minería, farmacia y parques de atracciones, entre otros".

Según Vesku Turtia, el mercado industrial adolece de varios problemas, siendo uno de los más importantes, la falta de visibilidad sobre la planta de OT. Para remediar este hecho, la oferta de Nozomi se dirige, en primer lugar, a ofrecer una visibilidad operativa en tiempo real para las redes de control industrial. Aunque eso sí, asegura Turtia, las herramientas como la des Nozomi, pese a ser completas y eficientes, están aún lejos de ser cajas mágicas. "En OT, nunca te puedes desligar de la seguridad. Las plantas de producción no pueden dejar de funcionar, por lo que la seguridad no puede fallar y tiene que ser una prioridad", apuntó.

Además del inventario, el segundo pilar en el que confía Nozomi es en la evaluación de vulnerabilidades y detección de anomalías. De este modo, es posible descubrir si algo no va bien o existe alguna vulnerabilidad en alguno de los autómatas (PLCs).

La tercera parte es la convergencia con los sistemas de IT. Ambos mundos, IT y OT, tienen los mismos problemas, por lo que su estrategia tiene que ser la misma: proteger los bienes de las compañías. Los dos, además, deben entenderse, tanto a nivel organizacional como tecnológico y con otras herramientas de terceros. De igual manera, debe haber una convergencia con otros fabricantes de IT y OT para que la información e inteligencia contra los malos fluya de un modo adecuado y continuo.

Al respecto de la adopción de seguridad en el sector industrial, Vesku Turtia se reafirma en el hecho de que esta debe ser una prioridad. En ocasiones, los fabricantes de seguridad gustan de alarmar sobre determinados aspectos para conseguir una respuesta positiva por parte de los clientes. En OT, no hay cabida para la exageración.

Ve aquí la intervención de Nozomi en el webinar Ciberseguridad industrial, protegiendo el sector productivo. ■

Si te ha gustado este artículo, compártelo

RICARDO HERNÁNDEZ, DIRECTOR COMERCIAL PARA ESPAÑA Y PORTUGAL DE FORESCOUT

“Hace años, el principal riesgo para los entornos OT eran las caídas no programadas, hoy hay mucha problemática por la contaminación cruzada entre los entornos IT y OT”

Desde el punto de vista de Ricardo Hernández, Director Comercial para España y Portugal de Forescout, quien participó en la sesión online Ciberseguridad Industrial, protegiendo el sector productivo, los retos a los que se enfrenta la seguridad de los entornos de industria 4.0 están marcados por dos tendencias: el crecimiento o la explosión de dispositivos que se conectan a la red, ya no solo los equipos específicos de los entornos OT sino también lo denominados Internet Industrial de las Cosas (IIoT), y la responsabilidad de gestionar la seguridad de los entornos industriales, que corresponde y seguirá correspondiendo a los CIOs y CISOs provenientes de IT.

“Hace años, el principal riesgo para los entornos OT eran las caídas no programadas, hoy hay mucha problemática por la contaminación cruzada entre los entornos IT y OT, riesgo de fuga de datos o incluso paradas de la cadena de

RICARDO HERNÁNDEZ, FORESCOUT

suministro", afirma. Asimismo, la explosión de los datos (Big Data), también está impactando sobre la seguridad del entorno industrial, máxime, cuando este crecimiento de la información está chocando con una carestía de herramientas adecuadas para analizar dicha información. Todo esto está derivando en una dificultad para saber qué está pasando en la red (número de dispositivos conectados, segmentación adecuada, etc.) y provocando importantes fallos de seguridad, así como un incremento de los ataques dirigidos contra los dispositivos conectados.

Del mismo modo, el hecho de que existan problemáticas comunes entre IT y OT, como puedan ser el riesgo de sufrir ciberataques, caída de servicios no planificadas o requisitos de cumplimento, da como resultado retos comunes, pero con diferentes perspectivas. Se habla, por tanto, de una cada vez mayor convergencia entre ambos mundos, que, según Hernández, "seguirá produciéndose y que, al final, derivará en la necesidad de contar con una única solución que sea capaz de proteger a los dos entornos".

En este contexto, desde Forescout proponen una solución transversal para IT y OT, sustentada en la visibilidad, para saber qué se necesita proteger. También, quieren ayudar a los clientes a que puedan establecer de una forma real la detección y la ciber-resiliencia ante los ataques y a simplificar los procesos de cumplimiento. Muy importante es, a su vez, "la capacidad para segmentar la red, para tener un primer nivel de defensa, y, que la respuesta sea lo más rápida y automatizada posible".

Tecnológicamente, Forescout cuenta con una plataforma de automatización, que, gracias a su integración con diferentes herramientas de seguridad, como firewalls de nueva generación, anti APTs o sistemas de gestión de vulnerabilidades, es capaz de coordinar una respuesta automatizada ante determinadas situaciones. Dicha solución, además, es transversal a cualquier entorno (IT, OT, nube, data center) por lo que es óptima para cualquier cliente. Tal y como comenta Ricardo Hernández, "no importa qué tipología tenga el cliente, al final necesita tener visibilidad y control a lo largo de toda su red".

Aquí puedes visualizar la intervención de Forescout en el IT Webinars Ciberseguridad industrial, protegiendo el sector productivo. ■

Si te ha gustado este artículo, compártelo

ESTRATEGIA DE CIBERSEGURIDAD ICS: 4 PASOS PARA LA VISIBILIDAD Y CONTROL DE DISPOSITIVOS

Regulaciones cada vez más estrictas, amenazas de ciberseguridad crecientes y la exposición de las redes ICS a Internet está haciendo que la protección de estas redes sea haya convertido en asunto estratégico. Además, la creciente complejidad causada por la integración de TI y OT dentro de las redes ICS aumenta la probabilidad de configuraciones incorrectas, errores y fallos. En este contexto, un enfoque holístico para proteger las redes ICS es cada vez más vital para minimizar los riesgos financieros y operativos de una falla y las consecuencias resultantes. Este documento técnico describe un enfoque óptimo de 4 pasos para proteger las redes ICS.

Redefiniendo el almacenamiento para entornos críticos

Galo Montes,
director técnico
de HPE España

El almacenamiento tradicional está acometiendo nuevos retos ya que parte de sus usos tradicionales se están yendo al almacenamiento basado en software (software defined Storage), sobre equipos servidores estándar, y las cargas de trabajo que asumen son cada vez más críticas. Por todo ello, hay una tendencia en los fabricantes líderes del mercado en aprovechar IA para ofrecer una mayor simplicidad, disponibilidad y rendimiento.

Las empresas buscan introducir nuevas aplicaciones de misión crítica en el mercado y dar soporte a las ya existentes para acelerar la velocidad del negocio, la agilidad y la innovación. Sin embargo, es casi imposible para los departamentos de TI satisfacer estas demandas porque siguen atados a la administración, ajuste y soporte de la infraestructura. Como resultado, se ven obligados a sacrificar la agilidad por la fiabilidad.

Gracias a la existencia de plataformas que recopilan datos continuamente del funcionamiento de los sistemas de almacenamiento y de su entorno, se ha podido aplicar la inteligencia artificial para que las nuevas plataformas que están apareciendo tengan un 90% menos de tiempo dedicado a la gestión, así como la capacidad de predecir y prevenir problemas, y acelerar el rendimiento de las aplicaciones. Esto permite eliminar los compromisos y redefine lo que es posible en el almacenamiento de misión crítica, combinando la innovación para ofrecer una experiencia de usuario sencilla y de calidad, fácil de instalar, manejar y actualizar.

Pero la nube ofrece ciertas ventajas de flexibilidad que los fabricantes de infraestructura también han tenido que acometer. Así, los nuevos almacenamientos se ofrecen cada día más en pago por uso o como un servicio. Con ello, los clientes reducen los riesgos inherentes a una gran inversión inicial que no saben si podrán amortizar, y liberalizan valiosos recursos que pueden aplicar a innovar. Un ejemplo de esta transformación es HPE Primera. Es parte de HPE Intelligent Data Platform, una cartera de productos y soluciones diseñados para acelerar el rendimiento de las aplicaciones, transformar la gestión de datos, aprovechar la agilidad de todas las nubes y potenciar a las empresas mediante el desbloqueo de información oculta dentro de los datos en tiempo real. ■

ENERGÍA INTELIGENTE ALIMENTADA POR LOS DATOS

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

itTRENDS

El futuro es abierto e híbrido

Jim Whitehurst,
presidente y
CEO de Red Hat

La transformación digital no ocurre de la noche a la mañana. Las organizaciones no pueden darle a un interruptor y convertirse de un momento a otro en nativas de la nube. Es necesario seguir haciendo uso de la infraestructura existente al mismo tiempo que se va trabajando en los planes de futuro. Por eso, en Red Hat creemos que el futuro es híbrido.

Y cuando hablamos de ese futuro híbrido, no solo pensamos que es relevante para TI sino que se aplica a la organización en sí misma, ya que las tecnologías abiertas e híbridas funcionan mejor cuando tienen el apoyo de equipos abiertos con culturas abiertas. Estamos convencidos de que la apertura libera el potencial del mundo, y por ello, no sólo se limita a las tecnologías, sino que se extiende a la cultura y la metodología de trabajo de las organizaciones.

Pongamos como ejemplo, la nube. Es una realidad, pero muchos de nuestros clientes no saben exactamente cómo sacarle el mejor partido. Y se debe a que una estrategia de nube va más allá de la "nube". Se trata de contar con la infraestructura necesaria para soportar y ejecutar aplicaciones. Conscientes de ello, desde Red Hat hemos desarrollado un amplio portfolio con la nube como eje central, en el que se cuenta con una oferta de contenedores. Plataformas como Red Hat OpenShift Container proporcionan una solución para impulsar la transformación digital, ayudando a adoptar tecnologías emergentes como los contenedores Linux y Kubernetes, sin sacrificar las aplicaciones ni la inversión de TI existentes.

Y no es la primera vez que hacemos frente a una migración de este tipo. Durante décadas, hemos ayudado a las organizaciones a pasar de UNIX a Linux, y estamos preparados para seguir ayudándolas a medida que migran a la nube, modernizan sus infraestructuras o automatizan sus complejas cargas de trabajo.

Llevar a cabo esta migración requiere de un partner como Red Hat, que alcance el equili-

El uso del código abierto empresarial aumentó el año pasado un 68%. Una gran parte del mundo mira a las empresas de código abierto no solo como una poderosa fuente de innovación tecnológica, sino también como un estándar para construir las organizaciones del futuro

brio entre la innovación experimental y la consistencia operativa, que entienda el concepto de "híbrido" en toda la organización. Ayudamos trabajando al estilo del código abierto, juntando redes de diversos partners para crear las mejores soluciones. Nuestro enfoque de comunidad se está volviendo un distintivo en una época en la que la cocreación supera al consumo, en la que los clientes no se conforman con pedirnos que resolvamos problemas, sino que quieren que lo resolvamos con ellos.

Los clientes se dirigen a Red Hat porque están interesados en hacer cambios profundamente arraigados en su cultura organizativa que los preparará para un futuro exitoso. Este tipo de colaboración está en nuestro ADN y nos reconocen como la organización que siempre trabaja de manera transparente, inclusiva y abierta, tal y como les gustaría hacerlo a ellos mismos.

Ese futuro se mantiene abierto. Según el informe "El Estado Actual del Código Abierto Empresarial", patrocinado por Red Hat y publicado en abril, el uso del código abierto empresarial aumentó el año pasado un 68%. Una gran parte del mundo mira a las empresas de código abierto no solo como una poderosa fuente de innovación tecnológica, sino también como un estándar para construir las organizaciones del futuro. ■

Si te ha gustado este artículo, compártelo

RED HAT ENTERPRISE LINUX Y SU IMPACTO ECONÓMICO EN LAS EMPRESAS

Red Hat acaba de lanzar Red Hat Enterprise Linux (RHEL) 8. Según datos de la compañía, de los 188 billones de dólares facturados por las empresas a nivel mundial en este 2019, 10 billones están "tocados" por Red Hat Enterprise Linux. Este documento, elaborado por IDC, valora la magnitud del impacto económico de Red Hat Enterprise Linux en tres dimensiones: los ingresos y los gastos que alcanzan las empresas que utilizan RHEL y su consiguiente ventaja económica, el impacto de los gastos de TI en tecnología y mano de obra del personal de las empresas que utilizan RHEL, y el tamaño y alcance del ecosistema cuyos productos y servicios forman parte de RHEL.

it TRENDS

Cómo repeler eficazmente los ataques al correo electrónico

Martin Mathlouthi,
jefe de línea
de productos para
la seguridad del correo
electrónico en Retarus

La protección total frente a los ciberataques perpetrados por correo electrónico no existe. Las secuelas de troyanos, ransomware, phishing y spam pueden llegar a ser muy graves: pérdida de datos, interrupciones del servicio, pérdidas económicas importantes y a menudo también el deterioro de la reputación. La perseverancia es la gran aliada de los responsables de TI para proteger la comunicación comercial de sus empresas.

En la actualidad, cada vez son más numerosos los métodos de ataque que burlan los mecanismos de defensa convencionales. Las medidas de protección tradicionales, como los exploradores antivirus y los filtros de spam y phishing, no son suficientes para protegerse de estas amenazas avanzadas. Sin embargo, tecnologías como el Sandboxing y la reescritura de URL garantizan un mayor nivel de seguridad. Lo idóneo es combinarlas con métodos innovadores de reacción y análisis. No obstante, resulta complicado cumplir todos estos requisitos con sistemas autogestionados. En cambio, los servicios profesionales de seguridad de correo electrónico desde la nube combinan las medidas necesarias según las necesidades, se actualizan continuamente y constituyen, por tanto, una alternativa sensata.

RECONOCIMIENTO PRECOZ DE ATAQUES DIRIGIDOS

La ingeniería social es también un método de ataque muy utilizado que apunta directamente a las debilidades de los usuarios. Recientemente, por ejemplo, se han multiplicado los casos de "fraude del CEO": los ciberdelincuentes se hacen pasar por el CEO de una empresa mediante mensajes de correo electrónico falsificados a la perfección en los que solicitan a personas potencialmente autorizadas que transfieran grandes sumas de dinero. Los delincuentes buscan a las personas de contacto adecuadas en la empresa y les envían correos electrónicos personalizados, siempre adaptados en función del destinatario. Una medida importante para protegerse contra este tipo de fraude es sensibilizar a los empleados, puesto que resulta extremadamente difícil reconocer estos correos electrónicos como intentos de fraude. Por este motivo, una solución de seguridad de correo electrónico debe incluir características tales como el etiquetado de mensajes de correo electrónico sospechosos y me-

canismos de detección de fraude del CEO. Estas tecnologías reconocen a tiempo las direcciones falsas y advierten a los destinatarios, además de bloquear o poner en cuarentena dichos correos electrónicos.

DETECCIÓN DE PATRONES DE ATAQUE NO CONOCIDOS

La encuesta de seguridad cibernética de BSI revela que los atacantes pueden penetrar en los sistemas informáticos corporativos a pesar de todas las medidas de protección. Esto ocurre, por ejemplo, cuando aún no se conocen los patrones de ataque (esto es, determinados virus), o cuando el malware que se introduce no se activa inmediatamente. En esos casos, los exploradores antivirus no detectan las rutinas maliciosas e incluso las tecnologías de Sandbox a veces son incapaces de descubrir acciones sospechosas, por lo que se entregan correos electrónicos potencialmente dañinos.

Para prevenir o al menos limitar los daños, se requieren soluciones como la Postdelivery Protection, la cual actúa cuando se conocen nuevos patrones de virus, incluso si el malware ya ha entrado en la infraestructura corporativa a través del correo electrónico. Las tecnologías más avanzadas ya generan una huella digital de todos los archivos adjuntos y de las URL que contienen cuando un correo electrónico llega al centro de datos del proveedor de seguridad de correo electrónico. Tan pronto como se detecte código malicioso en un archivo adjunto idéntico dirigido a un destinatario posterior o se identifique una URL como un intento de phishing, se informará inmediatamente a todos los destinatarios anteriores y a los administradores. Por lo general, el departamento de TI de la empresa recibe una alerta tan rápida que los correos electrónicos infectados posiblemente aún no se habrán abierto y pueden borrarse inmediatamente. Además, pueden integrarse servicios innovadores en el panorama de los sistemas de ciberseguridad de las compañías usuarias para suministrar los eventos necesarios para el análisis forense avanzado; por ejemplo, mediante la integración con las herramientas SIEM para proporcionar eventos relacionados con la seguridad. ■

Si te ha gustado este artículo, compártelo

DETECCIÓN DE MALWARE FIABLE Y ANÁLISIS FORENSE

La mayor parte del correo electrónico consiste en spam, virus o ataques de phishing dirigidos. Cada día se liberan más de 390.000 programas maliciosos nuevos en todo el mundo. Esto se traduce en una media de alrededor de 270 nuevas variantes de virus por minuto. Por lo general, las soluciones de seguridad de correo electrónico filtran de forma fiable los mensajes infectados. Sin embargo, incluso los mejores filtros antivirus no pueden ofrecer una protección totalmente efectiva puesto que, cuando aparece un malware nuevo por primera vez, su firma sigue siendo desconocida.

it TRENDS

5 decisiones que pueden retrasar la implantación del un modelo de Cloud Híbrido

Alejandro Solana,
GSI / SO Practices and Solution Architecture – SEMEA, Nutanix

La mayoría de las organizaciones ya operan con alguna una variedad de la oferta cloud, ya sea pública, privada o híbrida. Pero hoy en día, según se producen avances en áreas como la Inteligencia Artificial, IoT, y Machine Learning, la necesidad de adopción de modelos de cloud híbrida comienza a acelerarse, las estrategias están cambiando y muchas organizaciones están sufriendo ese cambio y comprobando que aún no están suficientemente preparadas.

El desafío actual es definir una estrategia efectiva para una infraestructura más funcional, flexible y preparada para las nuevas necesidades de negocio a futuro. Comienza a ser una prioridad tomar ya las decisiones de modernización del datacenter que permitan acompañar de forma más sencilla la incorporación de innovación y diferenciación, así como la capacidad de adaptarse a un entorno cambiante y responder con agilidad a las necesidades de los clientes.

Y en este punto, ¿por dónde empezamos?

LO PRIMERO ES LO PRIMERO

Antes de decidir a dónde vamos, hemos de analizar el punto de partida. El primer paso para abordar una estrategia de cloud híbrida avanzada pasa por plantearse las cuestiones más relevantes sobre nuestra infraestructura actual. Identificar las ubicaciones, aplicaciones, servicios, y datos.

PLANIFICAR EL FUTURO

Después de analizar la situación actual, podremos plantear cuáles van a ser las necesidades futuras, los nuevos tipos de aplicaciones y servicios que preveemos disponer en el próximo año. Al mismo tiempo, debemos tener en cuenta las posibles iniciativas de negocio o tecnológicas que se nos están planteando relativas a BigData, IoT o DevOps.... y qué recursos adicionales vamos a necesitar.

Una vez analizada la situación y establecidos los objetivos de cloud híbrida a alto nivel, es el momento de tomar 5 decisiones clave.

DECISIÓN 1: Elegir el framework Cloud a implementar

Probablemente esta sea la primera decisión que tomar y la más importante. Merece la pena adelantarnos para evitar tener que reconsiderar la decisión a medio plazo. Necesitaremos un mo-

delo cloud que permita monitorizar, gestionar y orquestar entre todos los entornos de forma sencilla con un conjunto reducido y simple de herramientas, a la vez que permitimos a los usuarios poder trabajar de forma homogénea en cualquier entorno. Deberemos identificar las piezas clave del sistema operativo cloud que necesitará abarcar el soporte de entornos on-premise, público, CSP's, aplicaciones estables y/o volátiles, VMs o contenedores, volumen de datos, etc. Esto nos ayudará a considerar el framework más indicado.

DECISIÓN 2: Definir la estrategia de modernización de los entornos on-premise

En 2021 se predice que las empresas alcanzarán un balance 50/50 en las cargas que ejecutan on-premise vs las que ejecutan en la cloud pública. Con esto en mente, las necesidades de los entornos on-premise no se pueden ignorar, aunque en nuestra cabeza esté siempre la referencia de la cloud pública. La lista de nuestras capacidades críticas incluirá elementos como software-defined, hiperconvergencia, facilidad de automatización, auto-servicio, protección de datos y recuperación ante desastres, así como la facilidad de extender e incorporar clouds distribuidas y Edge Computing.

DECISIÓN 3: Elección de los entornos Cloud públicos para nuestra Cloud Híbrida

¿Cuál es el objetivo? Decidir los proveedores de cloud que se alineen con las decisiones que hemos realizado, y elegirlos en base a simplicidad y compatibilidad. Esto nos llevará a una integración más transparente entre entornos, y permitirá a los desarrolladores utilizar recursos en nuestra cloud híbrida sin necesidad de retooling ni reingeniería de aplicaciones. Es por tanto importante establecer las relaciones con nuestros proveedores cloud, incluso si las necesidades no son inmediatas.

DECISIÓN 4: Decidir qué aplicaciones y servicios ejecutar en qué Cloud

Las decisiones de dónde ubicar ciertas cargas dependerá de requisitos como el precio, elasticidad, rendimiento, seguridad y necesidades de compliance, así como las necesidades específicas de las propias aplicaciones. En el caso de la oferta de cloud pública, nos proporciona un conjunto de opciones y un rango de servicios de infraestructuras y servicios entre los que poder elegir. La clave en este punto es seleccionar las clouds públicas que trabajen de forma óptima con el modelo cloud elegido y que complemente nuestro entorno de aplicaciones.

DECISIÓN 5: Realizar un shortlist de proveedores SaaS

Esta decisión, probablemente, es de menor prioridad que la de modernización del datacenter y la elección de proveedores cloud (CSPs o Cloud públicas), pero merece la pena tener presente las consideraciones a realizar respecto a la oferta SaaS existente. Estandarizar el conjunto de proveedores SaaS tratando de evitar disponer de servicios similares duplicados. Podríamos también considerar la posibilidad de realizar outsourcing de ciertas aplicaciones que estamos ejecutando on-premise a un proveedor SaaS, liberando recursos e infraestructuras. Por otra parte, es importante no olvidar los datos almacenados por estos proveedores SaaS y garantizar que los requisitos de regulación y protección de datos se cumplen.

La foto de la nube híbrida en nuestro país

En España, las empresas realizan más cargas de trabajo en centros de datos tradicionales que las compañías de otros países, pero utilizan la nube privada con más frecuencia. En los próximos dos años, nuestro tejido empresarial planea una reducción del uso de los Data Center y de la nube privada, lo que se traducirá en un incremento del uso de la nube híbrida que llegará al 57% de penetración, sobrepasando la media de EMEA (43%) y la global (41%). ■

Si te ha gustado este artículo, compártelo