Predicciones 2020: qué sigue para la nube, automóviles conectados y la medicina, así como la ciberseguridad

17 de diciembre de 2019

Peter Galvin | Director de estrategias

Vehículos autónomos. Informática en la nube. Medicina conectada. Vulneraciones de datos.

Estas invenciones, casos de éxito y retos han sido temas clave durante varios años. Y todos ellos están a punto de experimentar un cambio significativo en el próximo año.

Estos cambios serán posibles gracias a investigaciones recientes, avances tecnológicos y mejor organización. Y esto es sobretodo (aunque no todo) bueno.

¿Qué podemos esperar de estas importantes áreas en 2020? Estas son mis predicciones.

El camino que le espera a los automóviles autónomos es más largo y más limitado

Si crees que los automóviles que se conducen solos es cosa de ciencia ficción, no estás solo. Somos muchos los que pensamos que todavía falta mucho para que los automóviles sean autónomos. Y, en parte, es verdad.

Sabemos que los automóviles autónomos existen en el mundo real, pero eso no significa que vayamos a verlos pronto recorriendo las calles. Lo cierto es que la mayoría de los vehículos autónomos que llegan al mercado tendrán un alcance más bien reducido,

pues dejar que los automóviles autónomos circulen de forma segura por las calles es un gran reto.

Por lo que es comprensible que quienes se encargan de ello se encuentren con algunos retos en el camino. Los vehículos autónomos han presentado más problemas de los que se esperaba, incluso un accidente mortal.

El resultado es que los vehículos autónomos están más lejos de lo que se predijo, y por eso, veremos un cambio en su uso: se limitarán a las carreteras a las que pueden acceder, así como a ciertas velocidades y solo podrán usarse en distancias establecidas. Al igual que un transbordador, circularán por vías muy específicas y solo tendrán unas pocas responsabilidades.

El efecto boomerang propicia una mayor adopción de implementaciones multinube

IDC estima que el gasto público mundial en la nube será de 229 mil millones de dólares este año y de 500 mil millones de dólares en 2023. Una encuesta de Gartner indica que el 81% de los usuarios de la nube pública trabajan con dos o más proveedores. Pero aconseja a las empresas que no vayan directamente de la implementación local a la multinube. Los matices de cada plataforma hacen que sea más difícil construir servicios en más de una, por eso, las empresas deberían ir poco a poco y permitir que los trabajadores tengan tiempo de adaptarse a la curva de aprendizaje.

A pesar de los retos, espero que haya una mayor adopción multinube en lo que queda de año. Además, creo que el 2020 nos traerá un mayor enfoque en tecnología que se adaptará a los entornos en la nube privados y locales, además de los entornos públicos. Esto podemos agradecérselo al efecto boomerang.

Hace solo un par de años muchas empresas estaban pensando en trasladarse a la nube pública en su totalidad. Y algunas trasladaron varias de sus aplicaciones a la nube. En el proceso, muchas se dieron cuenta de que la nube no siempre se ajustaba a sus necesidades. Para darse cuenta de esto hicieron falta problemas de seguridad, la necesidad de reescribir aplicaciones y otros retos. El resultado fue que muchas aplicaciones se volvieron en contra de las implementaciones locales.

Actualmente, las empresas adoptan cada vez más los entornos de implementación multinube. Desarrollan aplicaciones porque ofrecen la mejor tecnología y porque son seguras, independientemente de si son locales o en la nube.

Creo que seguiremos viendo un incremento en aplicaciones empresariales que imitan los entornos en la nube, incluso si técnicamente no entran en lo que es la nube pública. Las empresas construirán infraestructuras y arquitecturas que les permitan ampliar y expandir las aplicaciones, así como gestionar la carga de trabajo. Estos entornos serán sorprendentemente parecidos a la nube pública pero construidas de formas locales o en la nube privada.

La medicina conectada permite más visitas a domicilio

Hace unos años, WIRED publicó un artículo titulado "Healthcare 2020: The e-Doctor Will See You Now" (Sanidad 2020: el doctor electrónico te visitará ahora). Observaba la posibilidad de reducir los procesos en papel de la profesión médica. Declaraba que, con el tiempo, los pacientes tendrían más control sobre su salud, y observaba que las tecnologías ponibles monitorizarían la salud de los pacientes, estuvieran donde estuvieran.

En cierta manera, estas tendencias ya se están viendo. Esto se verá con mayor frecuencia el próximo año.

En 2020, veremos cómo grandes dispositivos médicos como los respiradores, que tradicionalmente solo se encontraban en instalaciones médicas, se abren camino en las casas. Estos dispositivos serán más pequeños, se conectarán a Internet y podrán usarse en casa ya que estarán conectados a la red. El acceso a estas máquinas desde casa se traducirá en un ahorro de tiempo y dinero tanto para la

industria médica como para los usuarios. Además, tienen potencial para mejorar la salud y salvar vidas.

La vulerabilidad de datos siguen siendo uno de los mayores retos

El aumento de los dispositivos conectados y la migración de datos personales a los sistemas conectados aumentan el riesgo. Por eso en 2020, se verán tantas o más vulnerabilidades de datos como en 2019.

Los delincuentes se han dado cuenta de que las vulnerabilidades de datos podrían convertirse en la gallina de los huevos de oro. Como consecuencia, hemos pasado del hacker solitario a grupos criminales organizados que buscan información de identificación personal (PII).

Los datos médicos, se han convertido en un valioso tesoro de información, y por lo tanto, son muy atractivos para los ciberdelincuentes. Algunos informes indican que los expedientes médicos completos pueden tener un valor de hasta $1,000 dólares en la internet oculta. Mucho más que la información de las tarjetas de crédito o los números del seguro social. Los grupos no autorizados pueden acceder a los historiales médicos hackeando dispositivos implantados o de tecnología para forjarse un camino en el sistema sanitario con los historiales médicos electrónicos de los pacientes.

Muchos otros factores se suman a la fragilidad del reto de la ciberseguridad, como los errores humanos y las empresas que tienen dificultades para encontrar el equilibrio entre "suficiente" o "demasiada" seguridad.

Las empresas necesitan controles de seguridad y privacidad, pero no demasiados, ya que podrían ahuyentar a los clientes. Encontrar el punto ideal es un verdadero reto. Las empresas que cometen el error de tener poca seguridad estarán en el punto de mira de la vulneración de datos en el próximo año.

Visite la página web de nCipher para obtener más información sobre nuestras soluciones de seguridad. También puede seguirnos en Twitter, LinkedIn, y Facebook.