LITORALPRESS

Fecha: 12-11-2024
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Noticia general
Título: Computación cuántica: ¿El fin de la seguridad digital?

Pág. : 3
Cm2: 361,9

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Computación cuántica: ¿El fin de la seguridad digital?

El cifrado está entretejido en la misma esencia de nuestras vidas. Establece confianza y protege nuestros secretos. Aunque quizás no pienses en el cifrado mientras te mueves a lo largo de tu día, casi siempre está presente. Cada vez que envías un correo electrónico o un mensaje de texto, pagas una factura desde tu cuenta bancaria o compras con tu tarjeta de crédito, el cifrado está en acción. El cifrado más común utilizado hoy en día es el RSA que, en palabras simples, es un algoritmo que permite darle seguridad a la información. Sin embargo, la computación cuántica tendrá la capacidad de romper este cifrado.

Han sido ya casi 100 años de mecánica cuántica en desarrollo y esta última década ha visto avances absolutamente asombrosos en la ciencia de la información cuántica práctica y en la computación cuántica en particular. Las primeras computadoras de 2 bits cuánticos (qubits) duraban solo segundos, mientras ahora tenemos computadoras cuánticas estables en la nube con más de mil qubits. Esto significa que no se necesitan muchos qubits para comenzar a resolver desafíos masivamente importantes de la humanidad, como la creación de medicamentos que salvan vidas, llevar la inteligencia artificial a niveles sin precedentes y explorar los orígenes del universo.

Naciones Unidas nombró 2025 como el Año de la Cuántica, lo cual será transformador. Y, aunque la computación cuántica puede tener un impacto muy positivo en los negocios, debidoa la capacidad exponencial que representa, también aumentará las amenazas de ciberseguridad.

Para prepararse para ese este nuevo escenario, hay tres consideraciones en las que las empresas deben enfocarse. Primero, evaluar su riesgo cuántico y crear un plan estratégico para mitigarlo. Las compañías necesitan determinar qué partes de sus organizaciones están en riesgo y crear un equipo, plan y presupuesto para implementar una transición a gran escala del cifrado antiguo y vulnerable al nuevo cifrado resistente a lo cuántico.

Segundo, lanzar un esfuerzo a gran escala para descubrir dónde se encuentra todo el cifrado vulnerable en sus redes, aplicaciones, socios, nubes, dispositivos y más. Dado que los algoritmos de cifrado a menudo se han dado por sentado y no se han enfocado en ellos, se requiere un esfuerzo concertado para identificarlos y poner los resultados en un inventario accionable. El reciente surgimiento de herramientas de descubrimiento de criptografía específicas mejora drásticamente este proceso. Añaden un alto grado de automatización e inteligencia artificial (IA) para hacerlo manejable en términos de tiempo, dinero y completitud.

Claudio Ordoñez, director asociado de Accenture Chile

Tercero, crear una nueva arquitectura criptográfica que no solo resista los ataques cuánticos, sino que también gestione este vital recurso defensivo. Hacer esto prepara a las organizaciones para defenderse mejor contra la variedad de ataques actuales. También podrían incorporar los sistemas más nuevos de distribución de claves cuánticas (QKD) que utilizan la física cuántica misma para compartir claves sin riesgo de subversión. Una arquitectura de "defensa en profundidad" de nivel superior también está ahora disponible, que integra lo mejor de cada uno de estos en los niveles adecuados de una empresa crítica compleja.

Frente a los avances de la computación cuántica, el esfuerzo colectivo de hoy determinará un futuro digital seguro y resiliente para las generaciones venideras. Llevará años que las empresas del mundo actualicen su antigua y vulnerable criptografía. Y por eso es imperativo que trabajemos colectivamente y con urgencia.