Publicado en América Latina el 25/10/2023

# [DigiCert explica cómo afectará la criptografía post cuántica (PQC) a IoT en 2024](http://www.notasdeprensa.es)

## Según DigiCert, una vez que las computadoras cuánticas se conviertan en realidad, los dispositivos de IoT, que ya suelen ser vulnerables a ataques, se convertirán en uno de los sectores verticales más vulnerables. Las consecuencias son significativas si la criptografía post cuántica (PQC) permite a un atacante piratear los dispositivos que habilitan ciudades inteligentes, dispositivos de salud conectados, vehículos conectados o incluso el hogar inteligente de un individuo

 Las computadoras cuánticas cambiarán la forma en que operan muchas industrias y los impactos de la computación cuántica afectarán todos los aspectos de la sociedad. Las computadoras cuánticas podrían usarse para resolver problemas complejos de manera más rápida y precisa que las computadoras tradicionales, lo que conduciría a nuevos descubrimientos y avances en diversos sectores. Sin embargo, las computadoras cuánticas podrían romper muchos de los algoritmos de cifrado que se utilizan actualmente para garantizar la confianza digital. Se prevé que en 2024, se van a ver beneficios a medida que se aplique en varios campos con mucha computación, incluido el descubrimiento de la criptografía, la meteorología, fármacos, la secuenciación del genoma, optimización de sistemas complejos como el flujo de tráfico en las grandes ciudades etc. Hoy la sociedad se sumerge en el Internet de las cosas (IoT), o todos los dispositivos físicos que se conectan a Internet. El IoT es una categoría amplia que incluye tanto el IoT de consumo (CIoT) como el IoT industrial (IIoT), es decir, todo, desde dispositivos domésticos inteligentes como termostatos, asistentes de voz y cámaras hasta dispositivos de fabricación, transporte y atención sanitaria. Una vez que las computadoras cuánticas se conviertan en realidad, los dispositivos de IoT, que ya suelen ser vulnerables a ataques, se convertirán en uno de los sectores verticales más vulnerables. las consecuencias son significativas si la criptografía post cuántica (PQC) permite a un atacante piratear los dispositivos que habilitan ciudades inteligentes, dispositivos de salud conectados, vehículos conectados o incluso el hogar inteligente de un individuo. La realidad: IoT siempre ha sido vulnerableLos atacantes frecuentemente apuntan a dispositivos IoT, que se consideran el blanco más fácil o la parte más vulnerable de una red a los ataques. Los piratas informáticos pueden utilizar las vulnerabilidades de los dispositivos IoT para obtener acceso a otros dispositivos o redes, lo que los convierte en un objetivo atractivo. En los primeros dos meses de 2023, hubo un aumento del 41% en los ataques a dispositivos IoT desde 2022, y triplicó la cifra desde 2021. Esto es especialmente preocupante dado que se estima que habrá 75 mil millones de dispositivos IoT para 2025. "Parte de la razón por la que los dispositivos IoT son conocidos por ser objetivos fáciles es que tienen capacidades informáticas y memoria limitadas. Muchos dispositivos de IoT están diseñados para ser de bajo costo y desechables, por lo que puede resultar difícil implementarles actualizaciones de software. Si bien algunos dispositivos de IoT tienen más recursos que otros (por ejemplo, en el espacio de IoT industrial), suelen ser muy costosos e imposibles de reemplazar. Aún así, es posible que algunos dispositivos (por ejemplo, surtidores de gasolina en ubicaciones remotas) no tengan conectividad de red en absoluto", explicó Dean Coclin, director senior de desarrollo empresarial de DigiCert. Una vez que las computadoras cuánticas se conviertan en realidad, los algoritmos existentes que protegen la IoT podrían volverse vulnerables, exponiendo datos confidenciales transmitidos por dispositivos de IoT, comprometiendo la confidencialidad y la integridad. También podría haber riesgos en la cadena de suministro, ya que la computación cuántica podría permitir a los adversarios comprometer el firmware del dispositivo, las claves criptográficas o el propio proceso de fabricación, introduciendo vulnerabilidades que son difíciles de detectar y mitigar. Largos ciclos de vida y riesgo de ataques PQCLos dispositivos de IoT suelen tener una vida útil relativamente larga y, sin una forma clara de implementar actualizaciones de software, se vuelven vulnerables rápidamente. Para dispositivos con una vida útil de 10 a 20 años o más, los fabricantes de dispositivos deberían implementarlos con algoritmos poscuánticos hoy. Si bien no se sabe exactamente cuándo las computadoras cuánticas serán relevantes para los ataques a dispositivos, al menos algunos dispositivos implementados hoy con vidas más largas ya necesitarán algoritmos PQC antes del final de su vida. Como mínimo, cualquier dispositivo de larga duración que no esté implementado con algoritmos PQC en la actualidad necesitará un plan de actualización en el futuro. "Sin embargo, existen movimientos regulatorios para aumentar la seguridad y la transparencia de IoT incluso antes de la computación cuántica. Por ejemplo, la Ley de Resiliencia Cibernética de la UE probablemente exigirá que los fabricantes de dispositivos cifren datos confidenciales, apliquen actualizaciones periódicas de los dispositivos y proporcionen más información a los consumidores para que tomen decisiones de compra informadas. En el último punto, en Estados Unidos y otros países se están implementando etiquetas de seguridad de IoT, similares a las etiquetas nutricionales. El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ha proporcionado un marco para el etiquetado de IoT que incluirá información no solo sobre el dispositivo sino también sobre el software de soporte", agregó Dean Coclin. Estos cambios regulatorios ahora serán útiles cuando surjan las computadoras cuánticas, ya que los consumidores tendrán más transparencia sobre la seguridad de sus dispositivos y probablemente se aplicará más seguridad en el IoT, lo que con suerte hará que el IoT deje de ser el fruto más fácil de la industria a un poco más difícil de alcanzar para los atacantes. Cómo proteger IoT contra PQCDado que el NIST seleccionó algoritmos PQC para reemplazar los algoritmos criptográficos tradicionales existentes en Internet, se prestó especial atención para garantizar que los algoritmos PQC seleccionados pudieran ser utilizados por dispositivos IoT. Los dispositivos IoT necesitan una amplia gama de servicios criptográficos que incluyen: Certificados TLS/SSL para UI web y servicios web. Certificados de autenticidad que acrediten al fabricante del dispositivo. Firma de software para aplicaciones y actualizaciones de firmware. Mecanismos de seguridad específicos del protocolo y de la aplicación, según el caso de uso. Por lo tanto, los fabricantes de dispositivos deben evaluar y hacer un plan ahora sobre cómo incluir los algoritmos PQC seleccionados por el NIST en sus productos y software. Desafortunadamente, estos algoritmos no son cambios rápidos para los algoritmos tradicionales vigentes en la actualidad y puede llevar tiempo hacer la transición a PQC, lo que deja un período de transición durante el cual los dispositivos de IoT siguen siendo vulnerables. Mientras tanto, crear un plan de transición es esencial para prepararse para proteger la IoT contra las computadoras cuánticas. "Además, como se mencionó anteriormente, los dispositivos IoT con una larga vida útil implementados hoy deberán estar habilitados para recibir actualizaciones de software. Los estándares de "Actualización de software para Internet de las cosas" del IETF incluyen explícitamente soporte post-cuántico y la regulación de la UE también ayudará a hacer cumplir las actualizaciones periódicas de los dispositivos", concluyó Dean. Finalmente, los fabricantes pueden crear más transparencia en torno a la seguridad de IoT adoptando el etiquetado de IoT, que ya está regulado en varios mercados como Singapur, Alemania, Finlandia y con regulación en curso en EE. UU. y la UE.

**Datos de contacto:**

DigiCert Latam

Digicert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-explica-como-afectara-la-criptografia\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Hardware E-Commerce Ciberseguridad Industria Automotriz Otras Industrias



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)