Publicado en América Latina el 28/06/2024

# [DigiCert analiza cómo puede afectar la computación cuántica](http://www.notasdeprensa.es)

## Dean Coclin, Director senior de desarrollo empresarial en DigiCert, analiza la cercanía en la que será inevitable que las computadoras cuánticas serán capaces de romper el cifrado algoritmos en los que se confía actualmente para proteger Internet y una gran cantidad de procesos digitales

 En 2015, McKinsey and Company, una consultora de gestión global, publicó un estudio sobre iniciativas de diferentes naciones del mundo en investigación y desarrollo de tecnologías de computación cuántica.  Si ha estado al día con conversaciones sobre cuántica, probablemente haya oído hablar del Q-Day, el día no especificado, pero inevitable en el que las computadoras cuánticas serán capaces de romper el cifrado algoritmos en los que se confía actualmente para proteger Internet y una gran cantidad de procesos digitales. Es ideal redefinir el término para que signifique el momento en que los usuarios necesiten estar muy preocupados por la criptoagilidad necesaria para preparar las organizaciones por los riesgos de la computación cuántica. El punto de ruptura está más cerca de lo que se creeHTTPS (también conocido como el candado en su navegador) es proporcionado por un protocolo de cifrado llamado Transport Layer Security (TLS). TLS utiliza un esquema de cifrado llamado criptografía asimétrica que depende de un par de llaves: una clave pública que cifra los datos y verifica firmas digitales y una clave privada que descifra datos y genera firmas digitales. Los algoritmos asimétricos más comunes en la actualidad son RSA y ECC. Se utiliza criptografía asimétrica para proteger las comunicaciones de red, como cuando el usuario ingresa la información de su tarjeta de crédito o su identificación de contribuyente en un sitio web. También se utiliza criptografía asimétrica para proteger otras claves de cifrado (encapsulación de claves) como las que se utilizan para proteger bases de datos masivas en nubes y centros de datos de todo el mundo. En pocas palabras, la criptografía asimétrica actualmente protege prácticamente todo. La criptografía asimétrica utiliza matemáticas complejas (números primos grandes) que son muy difíciles de resolver para las supercomputadoras actuales. Pero la computación cuántica es excepcional a la hora de resolver problemas matemáticos complejos. Y en algún momento, las computadoras cuánticas tendrán suficiente potencia para resolver rápidamente el complejo problema matemático que es la criptografía asimétrica. Lo más importante no es cuándo, sino cómo.Nadie sabe exactamente cuándo sucederá esto, pero el "cuándo" no es el punto. Lo que debería preocuparnos, es cuánto tiempo llevará actualizar todos los sistemas para que sean seguros cuánticamente. Los sistemas (Registros médicos. Surtidores de gasolina. Cajeros automáticos. Servicios públicos. Comunicaciones militares) Esto no significa que todo lo que se haya protegido utilizando cifrado RSA quedarán expuestos inmediata o simultáneamente. En cambio, significa que cualquier clave privada se puede obtener rápidamente (piense en horas, no días), lo que facilita a los atacantes falsificar o explotar las cosas que protege cuando lo deseen. Hacer que lo cuántico sea seguroRSA y ECC tienen un propósito muy general. Se utilizan para cifrar y descifrar información y generar firmas digitales para verificar la autenticidad de los mensajes. Ese no es el caso de la actual criptografía poscuántica (PQC) algoritmos. Lo que significa que los casos de uso específicos requerirán algoritmos diferentes. Actualmente, se están desarrollando veintiocho algoritmos PQC, cuatro de los cuales NIST ha propuesto como estándares: Cristales-Kyber para encapsulación de claves de cifrado (ML-KEM) Cristales-Dilitio para firmas digitales (ML-DSA) ESFINCAS+ para firmas digitales (SLH-DSA) HALCÓN para firmas digitales (FN-DSA) En cuanto a los recursos informáticos, por ejemplo, las firmas digitales creadas con RSA 2048 tienen una longitud de 256 bytes, mientras que las firmas digitales creadas con SPHINCS+ tienen 17 kilobytes (66 veces más). Los pasos de hoyPreparación cuántica no es algo que su empresa pueda lograr en un día y no existe una solución única. Las organizaciones mejor protegidas serán cripto-ágil, lo que les permite reemplazar activos criptográficos obsoletos sin interrumpir la infraestructura de su sistema. Lograr la criptoagilidad comienza con: Creando un inventario de sus certificados, algoritmos y otros activos criptográficos Cambiando algoritmos de cifrado por: raíces de confianza, (por ejemplo, la cuenta privada de su organización) autoridades certificadoras, firmware para dispositivos de larga duración y cualquier otro activo que produzca firmas en las que se deba confiar durante mucho tiempo; y Explorando formas de incorporar algoritmos cuánticos seguros en sus productos. Modernizar la infraestructura de ciberseguridad del mundo para que sea segura desde el punto de vista cuántico no será fácil y probablemente requerirá varios intentos. PQC ha estado en desarrollo durante muchos años, pero es lógico que las primeras versiones aprobadas para su uso no resistan la prueba del tiempo. El Q-Day no es solo hoy; es todos los días de ahora en adelante. Es por eso que el verdadero objetivo es la agilidad criptográfica, con énfasis en la "agilidad". La verdadera preparación cuántica significa estar preparado para adaptarse rápidamente al cambio y tener soluciones de seguridad implementadas que le permiten adaptarse sin causar grandes interrupciones en su negocio.

**Datos de contacto:**

Digicert PR Latam

PR DigiCert

573125893314

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

Categorías: Internacional Software Ciberseguridad Innovación Tecnológica



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