La Commissione Ue pubblica la raccomandazione sulla crittografia post-Quantum

La Commissione Ue ha pubblicato una raccomandazione sulla crittografia post-Quantum per incoraggiare gli Stati membri a sviluppare e attuare un approccio armonizzato come la transizione dell'UE alla crittografia post-quantum. Ciò contribuirà a garantire la sicurezza delle infrastrutture e dei servizi digitali dell'UE nella prossima era digitale. Lo scrive la Commissione in una nota.

Mentre le tecnologie quantistiche porteranno molti benefici economici e sociali, ci si aspetta che i progressi nel calcolo quantistico rendano più facile per gli attori malintenzionati accedere ai dati sensibili. E' per questo che bisogna promuovere la crittografia.

Comunicazioni protette

È essenziale che le comunicazioni rimangano protette in futuro per la sicurezza dei cittadini, delle società, delle economie e del mercato unico digitale dell'UE. La crittografia post-Quantum è una delle soluzioni a questa minaccia futura, in quanto si basa su problemi matematici che sono difficili da risolvere persino per i computer quantistici. Come soluzione basata su software, la crittografia post-quantum è compatibile con le nostre infrastrutture esistenti in diversi settori, e quindi può essere implementata in modo relativamente rapido, precisa la Commissione in una nota.

La raccomandazione

La raccomandazione affronta la necessità di un approccio coordinato alla transizione dell'Europa verso un'infrastruttura digitale sicura dal punto di vista quantistico. Aiuterà gli Stati membri a sviluppare una strategia coerente in quanto migrano verso modalità più sicure di proteggere le loro infrastrutture digitali. Ciò promuoverà l'interoperabilità tra i paesi, consentendo a sistemi e servizi di funzionare senza soluzione di continuità a livello transfrontaliero.

La raccomandazione integra il lavoro già svolto da molti paesi e a livello internazionale per sviluppare e selezionare algoritmi di crittografia post-quantum per le norme, compresi gli sforzi di ricerca effettuati dai progetti finanziati dall'UE, la recente relazione dell'Agenzia europea per la cibersicurezza (ENISA) e le discussioni sulla crittografia post-quantum a livello internazionale, ad esempio nel Consiglio per il commercio e la tecnologia UE-USA e nel dialogo informatico.

Un tema, il quantum computing, di grande interesse globale come dimostra l'interessamento in prima persona del presidente Usa Joe Biden, che già lo scorso anno a maggio ha emanato un ordine per effettuare un censimento di tutti i rischi per la sicurezza in seno alle agenzie in vista della diffusione di tecnologie quantistiche.

https://www.key4biz.it/la-commissione-ue-pubblica-la-raccomandazione-sulla-crittografia-post-quantum/486617/