PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5756 di Lunedì 16 dicembre 2024

Cybersecurity: la minaccia legata alla diffusione di computer quantistici

Gli attuali sistemi criptografici potranno essere violati da algoritmi gestiti da computer quantistici nel giro di una decina di anni. Ecco perché è necessario avviare fin da adesso una strategia nazionale di messa sotto controllo di questi rischi.

Il General Accounting Office - GAO americano ha effettuato lo studio sulle infrastrutture critiche degli Stati Uniti, come d'esempio la produzione e trasporto di energia, i sistemi di trasporto su strade e ferrovia, le comunicazioni, i servizi finanziari, accertando il fatto che i dati sensibili sono protetti da algoritmi crittografici. Tuttavia, gli esperti, che guardano lontano, hanno cominciato a predire che un computer quantistico, in grado di violare la maggior parte degli attuali algoritmi criptografici, non è molto lontano nel tempo. Un tale computer è stato già battezzato con l'acronimo CRQC- Cryptographically Relevant Quantum Computer. Questi computer sfruttano le proprietà di un qubit, vale a dire l'equivalente quantistico dei bits tradizionali, per risolvere specifici problemi con velocità assai più elevate rispetto a computer tradizionali.

Negli ultimi otto anni, negli Stati Uniti è stata sviluppata una strategia nazionale di messa sotto controllo di questo rischio, ma soluzioni soddisfacenti sono certamente ancora lontane.

Ad esempio, sono stati sviluppati molti documenti che hanno individuato la minaccia presentata dai computer CRQC, ma una definizione standardizzata di questa tipologia di computer non è ancora stata definita.

Ad oggi, sono disponibili ben tre documenti che propongono delle norme per lo sviluppo di applicativi criptografici a prova di attacchi quantistici. La validità di questi documenti normativi però è ancora tutta da provare.

Infine, sono disponibili dei documenti strategici, che indicano gli obiettivi ed attività da svolgere per soddisfare di due aspetti precedentemente illustrati, ma non è ad oggi possibile definire dei tempi di attivazione di queste misure di contrasto.

Un passo avanti è stato fatto dal Congresso degli Stati Uniti, che ha individuato come organismo di riferimento centrale, per lo sviluppo di questi studi, lo Office of the National Cyber Director. Questo è il motivo per cui gli ispettori del General Accounting Office hanno avanzato una raccomandazione, che sollecita il direttore a svolgere la sua attività di coordinamento, in relazione alla messa sotto controllo dei rischi di attacchi con computer quantistici ed a garantire che i vari documenti già elaborati siano

tra loro coordinati e possano essere utilizzati per definire una strategia nazionale di protezione.

In Italia, come siamo messi?

Adalberto Biasiotti

---

www.puntosicuro.it