PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6185 di Lunedì 02 novembre 2026

Computer quantistici: vantaggi e rischi per la cybersecurity nel 2030!

I computer quantistici promettono prestazioni senza precedenti, ma possono mettere in crisi la crittografia attuale: il GAO invita aziende e agenzie a prepararsi subito alla transizione verso la post-quantum cryptography e a testare nuove soluzioni.

Gli esperti di sicurezza informatica devono prestare molta attenzione ai pregi degli elaboratori quantistici, ma anche ai pericoli connessi.

Uno studio recentemente portato a termine negli Stati Uniti dal General accounting Office offre preziose indicazioni su pregi e pericoli di questi nuovi potentissimi computer.

I computer quantistici utilizzano qubits, vale a dire l'equivalente quantistico dei bits dei computer classici, per risolvere specifici problemi con una velocità molto più elevata, rispetto ai computer tradizionali.

Tuttavia, la diffusione di computer quantistici può compromettere il livello di protezione degli applicativi crittografici, che vengono utilizzati oggi in molte agenzie federali degli Stati Uniti ed anche in altri sistemi informatici, distribuiti in tutto il mondo.

Ad oggi, i computer quantistici non possono ancora violare molti applicativi crittografici, ma non v'è dubbio che lo sviluppo velocissimo delle potenzialità di questi computer potrebbe presto portare a rendere possibili delle violazioni. Al proposito, ricordiamo ai lettori che questi specifici computer, mirati a violare algoritmi crittografici, vengono contrassegnati dall'acronimo CRQC - cryptographically relevant quantum computer.

Pubblicità

Secondo gli esperti, questa tipologia di computer potrebbe essere disponibile già nel 2030 ed occorre pertanto che i responsabili della sicurezza informatica delle aziende comincino già oggi a pensare a come proteggersi dagli effetti potenzialmente devastanti, che questi computer potrebbero creare.

Questo è motivo perché ormai si stanno già sviluppando dei nuovi applicativi crittografici, che vengono definiti con la sigla ***post-quantum cryptography.***

Le raccomandazioni che vengono presentate ai responsabili della sicurezza informatica sono in sintesi le seguenti:

- cominciare a classificare gli algoritmi criptografici utilizzati, assegnando un criterio di priorità agli interventi di miglioramento,
- Identificare le risorse necessarie per effettuare la transizione a post quantum cryptography,
- effettuare dei test su queste nuove tecnologie criptografiche.

Un'indagine effettuata dagli ispettori del GAO ha però messo in evidenza come presso molte aziende manchino ancora le competenze specifiche per affrontare questi problemi ed ecco il motivo per cui è stato lanciato questo tempestivo allarme.

Gli ispettori del GAO, dopo un'accurata indagine, hanno presentato 89 raccomandazioni a 23 agenzie federali, proprio per cominciare fin da adesso a fronteggiare questo rischio e metterlo sotto controllo.

12 agenzie federali hanno recepito queste raccomandazioni, mentre altre hanno messo in evidenza problemi di disponibilità di risorse economiche.

Siamo lieti di trasmettere questo messaggio anche alle aziende italiane, che certamente sono esposte allo stesso livello di rischio delle aziende degli Stati Uniti.

Ancora una volta, come una rivoltella può essere utile per difendersi, ma può essere pericolosa per aggredire, un computer quantistico può essere utile per sviluppare elaborazioni oltremodo sofisticate in breve tempo, ma può essere pericoloso come strumento di attacco!

Adalberto Biasiotti

Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.