PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6167 di Mercoledì 07 ottobre 2026

HDNL: la minaccia quantistica ai dati cifrati e come difendersi oggi

L'avvento del quantum computing rende concreto il rischio "Harvest now, decrypt later": dati cifrati oggi potrebbero essere decifrati domani. Strategie, criptografia post-quantum e migrazione sono essenziali per proteggere le informazioni più sensibili.

HDNL sta per "Harvest now, decrypt later", vale a dire "catturiamo subito un testo crittografato e teniamolo da parte fino al giorno in cui tecniche quantistiche di decrittazione ci permetteranno di comprenderlo".

Tutti gli esperti di criptografia concorrono sul fatto che le tecniche di cifratura e decifrazione, basate su algoritmi e computer quantistici, stanno sviluppandosi ad un ritmo eccezionalmente elevato, da parecchi anni.

Ciò significa che un testo criptografato, che con le tecniche oggi disponibili non è traducibile, è possibile lo possa diventare a distanza di tempo, più o meno lungo.

Le agenzie di intelligence di tutto il mondo sono particolarmente preoccupate per questa situazione, soprattutto con riferimento a dati che hanno una lunga vita utile, come ad esempio i dati relativi ad argomenti militari, i dati sanitari, i dati afferenti a contenziosi legali e via dicendo.

A conferma di questi timori, ricordiamo che nell'aprile 2026 una grande azienda, che tratta applicativi di intelligenza artificiale, ha individuato delle vulnerabilità software ad una velocità straordinaria, mettendo in condizione l'applicativo di sviluppare degli attacchi informatici in poche ore, attacchi che con tecniche tradizionali avrebbero potuto richiedere anni.

Pubblicità

Questo è il motivo perché il National Institute of Standard and technology, negli Stati Uniti, ha sviluppato tre algoritmi, che dovrebbero essere in grado di fronteggiare attacchi con i computer quantistici, anche in tempi prolungati.

Anche l'Europa ha pubblicato delle raccomandazioni in merito a tecniche di criptografia post quantum, che dovrebbero consentire un allungamento significativo dei tempi di resistenza alla decifrazione.

Al proposito, è interessante sottolineare come il regolamento generale sulla protezione dei dati dell'unione europea richieda che i titolari dei dati utilizzino delle tecniche appropriate di protezione dei dati in loro possesso; occorre quindi cominciare fin da adesso a guardare lontano, per evitare che tecniche oggi ritenute soddisfacenti non lo siano più in tempi prossimi.

Per dare un esempio semplicistico di come possano lavorare di computer quantistici, durante le tecniche di attacco di decifrazione, si provi a pensare alla seguente situazione.

Se un uomo deve risolvere un labirinto, egli cerca un percorso alla volta, finché, spesso dopo numerosi tentativi, invece di finire in un vicolo cieco finisce all'uscita del labirinto.

Un computer quantistico utilizza una tecnica completamente diversa, perché può esplorare numerosi percorsi possibili del labirinto, contemporaneamente.

Con ogni qubit addizionale, il numero di percorsi che può essere esaminato raddoppia. Si ha così una crescita esponenziale delle capacità di analisi del labirinto, che portano a trovare il percorso corretto in tempi rapidissimi.

Ecco le raccomandazioni che vengono offerte ai responsabili della protezione dei dati criptografati:

- condurre una rassegna completa tutti i testi criptografati disponibili, con le tecniche di cifratura utilizzate,
- dare delle priorità a dati specifici, che possono richiedere protezione per tempi prolungati, attribuendo loro rapide tempistiche di migrazione verso tecniche ancora più sicure,
- riesaminare tutti i contratti con fornitori terzi, per essere certi che non esistano presso questi ultimi punti deboli sul tema criptografico,
- sviluppare una traccia per la migrazione verso applicativi più sicuri, che possa garantire che tra il 2031 ed il 2035 i dati più sensibili siano adeguatamente protetti,
- infine, introdurre criteri flessibili per la eventuale sostituzione di applicativi criptografici, in base ad informazioni, provenienti dal campo, sul livello di evoluzione degli applicativi di decodifica.

Si tratta di un impegno che non sembra e non è modesto!

Adalberto Biasiotti

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