DOSSIER Il Sole 24 Ore 17 GIUGNO 2026

La quantistica minaccia i dati, parte la corsa verso il Q-Day

Scenario. Dalle banche alle infrastrutture critiche, la sicurezza si gioca oggi: la migrazione alla crittografia post quantistica richiede anni

Pagina a cura di Antonio Larizza

Il computer quantistico capace di rompere la crittografia che protegge transazioni bancarie, piani industriali, infrastrutture energetiche, dati sanitari, archivi pubblici e segreti militari non esiste ancora. Eppure, dovremmo già preoccuparci di lui. Perché informazioni e comunicazioni cifrate intercettate oggi potranno essere decifrate domani, quando una macchina quantistica abbastanza potente sarà in grado di far saltare lo scudo matematico che le protegge. Proprio in questo momento hacker, organizzazioni criminali, servizi segreti, Stati o industrie in concorrenza tra loro potrebbero essere già all'opera nell'attuare la strategia "harvest now, decrypt later": raccogli oggi, decripta domani.

Questo domani ha un nome, si chiama Q-Day: il giorno che farà da spartiacque tra il prima, il mondo protetto dalla crittografia classica, e il dopo, il mondo che potrà dirsi al sicuro solo se adotterà sistemi di crittografia post quantistica.

La posta in gioco

La posta in gioco è altissima. Secondo uno studio dello Hudson Institute, think tank statunitense, un ipotetico attacco quantistico al Fedwire funds service – il sistema gestito dalla Fed che consente a banche, istituzioni finanziarie e agenzie governative di trasferire somme di denaro in tempo reale e in totale sicurezza – potrebbe, da solo, generare danni e perdite per 2mila miliardi di dollari. Al momento non è possibile fissare sul calendario l'avvento del Q-Day. I computer quantistici disponibili oggi sono ancora lontani dalla scala, dalla stabilità e dalla capacità di correggere gli errori necessarie per mettere realmente a rischio gli attuali sistemi crittografici. Ma la minaccia cresce lungo due direttrici: da una parte migliorano hardware, stabilità e capacità dei computer quantistici; dall'altra diminuiscono le risorse computazionali richieste per condurre un attacco.

Il Q-Day si collocherà nel punto di intersezione tra queste due curve. La maggior parte degli esperti stima che questo giorno possa arrivare già entro il 2030 con una probabilità compresa tra il 5 e il 15%, che sale al 50% entro il 2035. Numeri da trattare con prudenza, non come una profezia. Ma anche una probabilità limitata diventa rilevante quando in gioco ci sono servizi essenziali, patrimoni informativi e infrastrutture strategiche che non possono essere riconfigurate dall'oggi al domani.

In questo scenario, i tempi della transizione alla crittografia post quantistica diventano una variabile decisiva. Per comprenderlo torna utile il cosiddetto "teorema di Mosca", che prende il nome dal ricercatore Michele Mosca. Si basa sul principio per cui il rischio di veder violato un sistema di sicurezza diventa concreto quando il tempo necessario alla migrazione dei sistemi di protezione, sommato al periodo per il quale i dati devono restare segreti, supera il tempo stimato che separa dall'arrivo di una tecnologia capace di violare quegli stessi sistemi. Detto in altri termini e considerando lo scenario più condiviso, ovvero una possibilità compresa tra il 5 e il 15% che il Q-Day si concretizzi entro il 2030: se oggi un governo ha dati sensibili la cui segretezza deve essere garantita

almeno fino al 2030 e prevede, per i propri sistemi di sicurezza, tempi di migrazione alla crittografia post quantistica superiori a quattro anni, i suoi dati sono già a rischio. L'organizzazione è già esposta. Il "teorema" dimostra che attendere il Q-Day per adeguarsi significa avere la certezza di arrivare tardi.

Le prime risposte

La risposta delle istituzioni, dell'industria e del mondo della ricerca è già in atto. La buona notizia, infatti, è che la messa a punto di una crittografia post quantistica non richiede necessariamente l'utilizzo di un computer quantistico. Consiste, piuttosto, nello sviluppo e nell'adozione di algoritmi eseguibili sulle infrastrutture tradizionali ma progettati per resistere ad attacchi quantistici. Nell'agosto del 2024 il National institute of standards and technology (Nist), agenzia governativa degli Stati Uniti che fa capo al dipartimento del Commercio, ha introdotto i primi tre standard: uno per lo scambio sicuro delle chiavi crittografiche, due per la sicurezza delle firme digitali. Non è un punto di arrivo, ma il segnale del passaggio dalla fase di ricerca a quella dell'adozione industriale.

Anche l'Europa si muove. Nel giugno del 2025 la Commissione europea e il Nis cooperation group – l'organo europeo di cooperazione sulla cybersicurezza – hanno definito una roadmap per la transizione alla crittografia post quantistica che fissa obiettivi e scadenze per governi e istituzioni europee. Tutti i Paesi devono avviare la transizione entro la fine del 2026. Per le infrastrutture critiche il passaggio alla crittografia post quantistica dovrà essere completato al più tardi entro il 2030. L'orizzonte del 2035 allarga la migrazione, per quanto tecnicamente possibile, alla maggior parte dei sistemi.

Il tema più delicato sarà quello della "scala" della transizione. La crittografia non abita in un solo luogo. È incorporata nei protocolli di comunicazione, nei server, nelle applicazioni, nei certificati, nei sistemi di autenticazione, nei dispositivi connessi, nelle infrastrutture a chiave pubblica. In questo contesto, vecchi e nuovi strumenti dovranno convivere per anni.

Lo stesso Nist osserva che il percorso dalla standardizzazione di un algoritmo alla sua piena integrazione nei sistemi e nei processi può richiedere dai 10 ai 20 anni. Sarà quindi centrale una visione all'insegna della crypto-agility: la capacità di conoscere gli strumenti crittografici già utilizzati, individuarne le vulnerabilità, stabilire le priorità e costruire architetture capaci di sostituire progressivamente gli algoritmi senza dover riprogettare ogni volta l'intero sistema.

La difesa post quantum non comincia con una sostituzione di massa di infrastrutture e software, ma con un inventario. Ogni organizzazione, sia pubblica che privata, deve capire dove operano i propri sistemi di crittografia, quali informazioni devono restare protette più a lungo e quali sistemi non possono permettersi di aspettare, indifesi, l'arrivo del Q-Day.