El Kaafarani, Pqshield: â??Con i computer quantistici niente resta sicuro per sempreâ?•ï»¿

Descrizione

(Adnkronos) â?? La minaccia non Ã¨ piÃ¹ soltanto teorica: con lâ??avanzata del quantum computing, i sistemi di crittografia oggi alla base di banche, cloud, telecomunicazioni, difesa e infrastrutture digitali rischiano di non essere piÃ¹ sufficienti nel medio periodo. A dirlo, durante la diretta Adnkronos da Fii Priority Europe a Roma, Ã¨ Ali El Kaafarani, ceo e fondatore di Pqshield, societÃ britannica specializzata in crittografia post-quantistica e nata come spin-out dellâ??UniversitÃ di Oxford.

â??La crittografia post-quantistica indica metodi di cifratura basati su matematica ancora resistente e difficile da violare anche per i computer quantisticiâ?•, spiega El Kaafarani. Il problema, aggiunge, Ã¨ che con i progressi dellâ??industria quantistica â??i metodi di cifratura che usiamo oggi sono sempre piÃ¹ a rischio di essere violati nei prossimi cinque-dieci anniâ?•, mentre i dati confidenziali hanno spesso un ciclo di vita molto piÃ¹ lungo.

Da qui la corsa dei governi e delle grandi aziende tecnologiche verso nuovi standard. Pqshield, ricorda El Kaafarani, ha lavorato con il governo americano allo sviluppo di nuovi standard di cifratura e ha avuto coautori in tutti gli schemi selezionati dagli Stati Uniti. â??Dal 2025 al 2035 questa Ã¨ la finestra temporale in cui lâ??industria dovrÃ trasferire tutta lâ??infrastruttura di cybersicurezza verso i nuovi standardâ?•, afferma.

Per il singolo utente, il rischio Ã¨ meno visibile ma non meno concreto. â??Dovremmo essere tutti preoccupatiâ?•. Il punto Ã¨ il modello noto come â??harvest now, decrypt laterâ?•: attori ostili possono raccogliere oggi dati cifrati che non riescono ancora a leggere, conservarli e decifrarli in futuro quando avranno gli strumenti per farlo. â??Niente Ã¨ sicuro per sempreâ?•, sintetizza.

Questo non significa, perÃ², che il cittadino debba intervenire direttamente sulla propria sicurezza digitale. â??Come utenti finali non abbiamo molto da fareâ?•, chiarisce El Kaafarani. La transizione deve avvenire piÃ¹ in alto nella catena di fornitura: semiconduttori, reti, produttori di dispositivi, servizi cloud, telecomunicazioni, finanza, difesa, infrastrutture critiche.

Il segnale positivo, secondo El Kaafarani, Ã¨ che il tema Ã¨ ormai entrato nel dibattito mainstream. Cita Apple, Google e Cloudflare tra gli attori che hanno giÃ annunciato percorsi di adeguamento o scadenze per la migrazione. â??Siamo passati da un attacco teorico a standard sviluppati, poi a standard mandati. Ora tutti ne parlanoâ?•, conclude.

â??

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Giugno 18, 2026
Autore
redazione