DELL Technologies

Crittografia post-quantistica

Guida introduttiva

Introduzione

L'elaborazione quantistica sta favorendo una radicale riprogettazione della tecnologia, con la creazione di opportunità incredibili e nuove sfide. Si tratta di un futuro entusiasmante, che introduce però una notevole minaccia ai sistemi crittografici responsabili della protezione del nostro mondo digitale.

Perché l'elaborazione quantistica è in aumento?

I computer tradizionali, notebook, smartphone o server, elaborano le informazioni utilizzando bit, che esistono sotto forma di numeri zero o uno. Anche se supporta il progresso ormai da decenni, questo modello binario limita le modalità con cui possono essere rappresentate e manipolate le informazioni. I computer quantistici, invece, usano i qubit, che possono trovarsi in diversi stati contemporaneamente, grazie a principi come sovrapposizione ed entanglement (correlazione quantistica). In questo modo, possono esplorare moltissime soluzioni potenziali in parallelo, fornendo notevoli vantaggi computazionali per determinate categorie di problemi.

Che cos'è la crittografia post-quantistica?

L'espressione crittografia post-quantistica (PQC, Post-Quantum Cryptography) si riferisce a una nuova generazione di algoritmi, progettati per proteggere i sistemi digitali sia dagli attacchi classici che da quelli quantistici. A differenza della distribuzione delle chiavi quantistiche, che richiede hardware specializzato, la crittografia post-quantistica è progettata per essere eseguita sulle infrastrutture attuali, ovvero sui server, sugli endpoint e sulle reti di uso comune, pertanto costituisce la soluzione più pratica e scalabile per prepararsi all'era quantistica.

Quali sono i rischi immediati che le organizzazioni devono affrontare con l'elaborazione quantistica?

Le conseguenze vanno ben oltre il rischio teorico. Le organizzazioni che rinunciano a prepararsi finiranno per esporre la proprietà intellettuale sensibile e dovranno affrontare disservizi nei sistemi finanziari, violazioni dei dati sanitari e minacce alla sicurezza nazionale.

La strategia "Raccogli ora, decifra più tardi" complica ulteriormente la situazione, perché i malintenzionati devono semplicemente intercettare i dati crittografati oggi e aspettare di avere a disposizione gli strumenti per decifrarli. Quando verranno introdotti i sistemi CRQC (Cryptographically Relevant Quantum Computer), il danno sarà già irreparabile.

“Raccogli ora, decifra più tardi” (HNDL): indicata anche con "Registra ora, decifra più tardi", è una tattica in cui i malintenzionati raccolgono e archiviano i dati crittografati oggi, nell'intento di decifrarli in futuro quando saranno disponibili i computer CRQC.

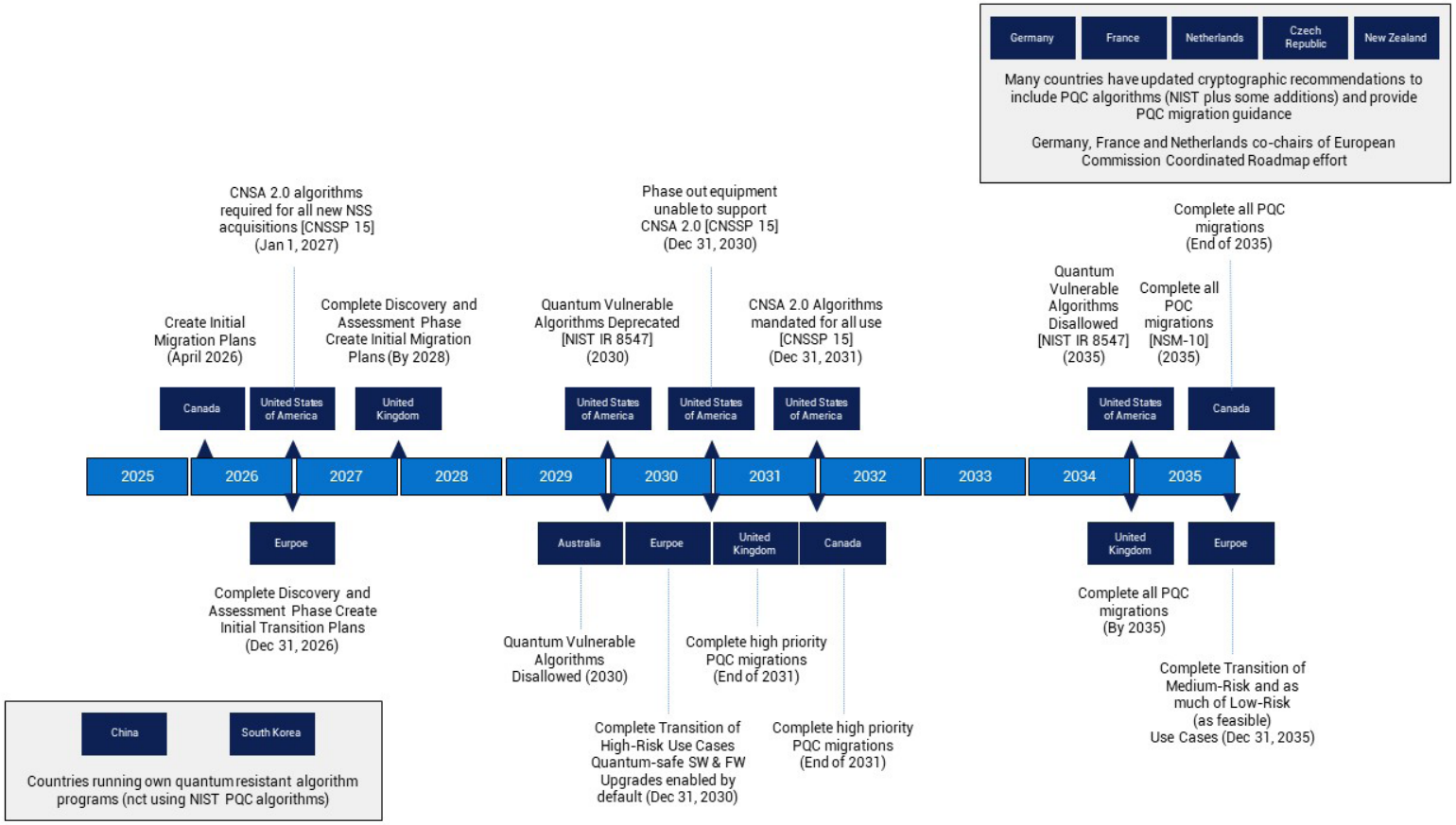
In che modo le organizzazioni si preparano per la transizione alla PQC?

Il percorso verso un futuro sicuro da un punto di vista quantistico è una maratona, non una gara di velocità, ed è in costante evoluzione. Un approccio proattivo, strutturato in più fasi e livelli, aiuterà l'organizzazione a gestire i rischi, a allineare le risorse e a costruire un profilo di sicurezza resiliente e duraturo nel tempo. Dell fornisce le tecnologie e le indicazioni per supportarti in ogni fase. Ecco i passaggi chiave per guidare l'organizzazione nella definizione di un piano di transizione verso la PQC.

Tempistiche di transizione verso la PQC

Riconoscendo l'urgenza della minaccia, governi e organizzazioni di standardizzazione hanno fatto della crittografia post-quantistica una priorità globale. Il governo federale statunitense ha compreso l'importanza di adottare algoritmi di crittografia resistenti agli attacchi quantistici, pertanto ha cominciato a imporre alle proprie agenzie di adottare la crittografia PQC come requisito. Tra gli altri, tali standard includono il National Security Memorandum 10 (NSM-10), la Commercial National Security Algorithm Suite (CNSA 2.0), l'Office of Management and Budget Memorandum 23-02 (OMB M-2302) e il National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547).

Nel resto del mondo, anche altre organizzazioni hanno definito linee guida per la transizione alla crittografia PQC. Queste date non sono casuali, ma rispecchiano i tempi necessari per riprogettare, convalidare e implementare la crittografia negli ecosistemi IT complessi. Per le aziende, questi requisiti non dovrebbero essere visti solo come obblighi di legge, ma piuttosto come indicazioni pratiche per la transizione globale alla resilienza quantistica. Le scadenze obbligatorie per i vari Paesi sono riportate di seguito.



Inventario e audit delle minacce crittografiche

La priorità assoluta è comprendere l'ambiente di crittografia attuale. Questo passaggio fondamentale definisce l'intera strategia di migrazione.

Procedure consigliate per l'igiene di sicurezza

Per prepararsi a un futuro all'insegna dell'elaborazione quantistica, occorre innanzitutto rinforzare le difese già implementate. È consigliabile adottare efficaci best practice per l'igiene di sicurezza, come l'applicazione del principio del privilegio minimo per gli accessi, l'implementazione dell'autenticazione a più fattori e una gestione rigorosa delle patch. Ma bisogna considerare anche altri due aspetti. Potrebbe essere necessario disabilitare la crittografia debole, per garantire l'interoperabilità fra i nuovi sistemi dotati di crittografia più avanzata e i sistemi legacy. Per i sistemi più recenti, è inoltre importante aumentare il livello di sicurezza minimo (AES-256 per la crittografia simmetrica, SHA-384 o superiore per i digest) per contrastare i margini ridotti introdotti dall'algoritmo di ricerca di Grover. Oltre a ridurre i rischi attuali, queste misure consentono anche di ridurre al minimo il debito crittografico, che finirebbe per complicare la migrazione futura.

Inventario e audit degli asset di crittografia

L'elemento chiave di qualunque piano di migrazione è costituito dalla visibilità. Le organizzazioni devono eseguire un inventario completo degli asset crittografici, allo scopo di determinare le posizioni e le modalità con cui viene utilizzata la crittografia a chiave pubblica per applicazioni, dispositivi e flussi di lavoro, inclusi i certificati TLS, le VPN, i sistemi e-mail, i meccanismi di firma del codice, i dati dei clienti, quelli archiviati e così via. Dopo aver identificato gli asset, occorre stabilirne la priorità in base alla criticità, alla sensibilità e alla vita utile all'interno dell'azienda. I dati storici, come le cartelle cliniche o gli archivi classificati, dovrebbero essere gestiti con la massima urgenza, perché sono i più vulnerabili alle minacce HNDL.

Progetti pilota e sperimentazione della crittografia PQC

Con un inventario chiaro, è possibile avviare sperimentazioni pratiche con tecnologie predisposte per PQC, allo scopo di verificare le prestazioni e l'integrazione.

Una volta compreso il panorama crittografico, è necessario cominciare a testare le soluzioni PQC in un ambiente controllato. Sperimentando queste soluzioni in laboratorio, il personale IT ha la possibilità di convalidarne i livelli di prestazioni, interoperabilità e gestibilità prima del deployment su vasta scala. Per garantire la resilienza a lungo termine e semplificare la migrazione è essenziale costruire questa agilità crittografica, ovvero la capacità di cambiare gli algoritmi di crittografia senza ristrutturare completamente i sistemi.

Adozione di un approccio di interoperabilità

Con la maturazione degli standard PQC, è possibile iniziare a pianificare i rollout in produzione. Un approccio ibrido crea un ponte verso un ambiente completamente sicuro dal punto di vista quantistico.

Mentre gli standard maturano, è possibile adottare un modello ibrido per gettare un ponte verso il futuro. Molti fornitori supportano già suite di crittografia ibride, che combinano gli algoritmi classici con quelli resistenti agli attacchi quantistici in una singola implementazione. Questo duplice approccio garantisce la continuità della protezione anche se in futuro uno di questi algoritmi verrà compromesso. Le imprese dovrebbero cominciare ad adottare queste strategie ibride ora, mentre allineano le loro tempistiche interne con le roadmap e le milestone dei fornitori dei loro prodotti di infrastruttura. In questo modo, quando gli algoritmi protetti dagli attacchi quantistici saranno completamente standardizzati, potranno adottarli su vasta scala senza interferire con le operazioni.

Esecuzione della migrazione completa e convalida continuativa

L'obiettivo finale è un'impresa sicura dal punto di vista quantistico, con un'integrazione completa e una convalida continua.

Esecuzione della migrazione completa e convalida continuativa

L'obiettivo finale consiste nel completare le transizione a PQC nell'intera azienda, cosa che non sarà un evento una tantum, ma un processo continuo di adattamento e convalida. È necessario eseguire piani di migrazione dettagliati, che prevedono l'integrazione di PQC in ogni singolo livello dello stack IT, mentre si continuano a testare i nuovi standard e le nuove implementazioni. I clienti possono utilizzare ambienti ibridi, che combinano computer tradizionali e quantistici, per simulare gli scenari di attacco, convalidare l'integrità crittografica e verificare la resilienza dei sistemi a fronte di minacce in continua evoluzione.

Collaborazione e condivisione delle conoscenze

Nessuna organizzazione dovrebbe affrontare questa sfida da sola.

I consorzi settoriali, i ricercatori universitari e gli enti pubblici stanno formando pool di conoscenze per accelerare la transizione a PQC. Le aziende hanno la possibilità di aderire ai gruppi per la definizione degli standard, ai gruppi di lavoro e ai programmi pilota, in modo da mantenersi allineate con le best practice e i requisiti emergenti. Con la sua partecipazione attiva a iniziative come il progetto NIST NCCoE PQC, Dell permette ai suoi clienti di beneficiare direttamente di questa esperienza collettiva.

Conclusioni

L'era dell'elaborazione quantistica non è più una possibilità lontana; è una realtà imminente che richiede un'azione lungimirante da subito. Prepararsi a questo cambiamento tecnologico è un imperativo strategico per proteggere l'asset più prezioso: i dati. Come abbiamo indicato, un approccio graduale che passa dall'inventario e dall'audit alla migrazione completa è il percorso ottimale verso un futuro sicuro contro gli attacchi quantistici.

La transizione alla crittografia PQC sarà uno dei cambiamenti infrastrutturali più importanti degli ultimi decenni e coinvolgerà quasi tutti gli aspetti dell'ambiente IT, dai server allo storage, fino agli endpoint, alle piattaforme cloud e ai protocolli di rete. Il successo richiede lungimiranza, pianificazione e disciplina. Noi di Dell Technologies abbiamo previsto un percorso in varie fasi, per bilanciare il miglioramento immediato della sicurezza con l'obiettivo a lungo termine di prepararsi all'adozione della crittografia PQC.

Dell intende rimanere a disposizione dei clienti, per aiutarli a definire la loro strategia di implementazione di queste nuove tecnologie. Noi consigliamo un piano di migrazione graduale e abbiamo delineato una serie di attività con lo scopo di aiutare i clienti a definire una strategia, per poi pianificare, eseguire e monitorare la migrazione a PQC.