DELL Technologies

White paper

Crittografia post-quantistica: è il momento di prepararsi all'era dell'elaborazione quantistica

White paper di Dell Technologies

Sommario

Panoramica esecutiva

L'elaborazione quantistica sta rapidamente passando dalla ricerca teorica all'implementazione pratica. Un tempo tutto questo era considerato un miraggio lontano, ma i progressi in materia di hardware, algoritmi e investimenti stanno accelerando l'introduzione di macchine capaci di risolvere problemi che sarebbero impossibili per i computer tradizionali. Le implicazioni sono notevoli per tutti i settori: dalla scoperta di nuovi farmaci alla modellazione del clima, fino alla logistica globale, l'elaborazione quantistica promette innovazioni che fino a ieri sembravano fuori dalla nostra portata.

Ma queste innovazioni sono accompagnate da problematiche senza precedenti, perché i computer quantistici finiranno per minare alla base le soluzioni di crittografia che proteggono l'intera economia digitale. La crittografia a chiave pubblica, ovvero gli algoritmi come RSA e la crittografia a curva ellittica (ECC, Elliptic Curve Cryptography), salvaguardano da decenni le comunicazioni digitali, i sistemi finanziari, le cartelle sanitarie e la sicurezza nazionale. Questi metodi si basano su problemi matematici che non possono essere affrontati dai computer tradizionali, ma i computer quantistici crittograficamente rilevanti (CRQC, Cryptographically Relevant Quantum Computer) sono in grado di risolverli efficacemente, rendendo improvvisamente obsolete le misure di sicurezza attuali.

Non si tratta di una minaccia ipotetica. Alcune organizzazioni usano già una tattica nota come "raccogli ora, decifra più tardi" (HNDL, Harvest Now, Decrypt Later), ovvero raccolgono fin da ora i dati crittografati in attesa di violarli non appena saranno disponibili computer quantistici capaci di farlo. Le informazioni sensibili che oggi sembrano sicure potrebbero diventare vulnerabili entro pochi anni. Proprio per questo bisogna cominciare a intervenire ora, senza attendere l'arrivo dei computer quantistici crittograficamente rilevanti (CRQC, Cryptographically Relevant Quantum Computer).

Questo white paper spiega perché la minaccia quantistica è tanto urgente, esplora il campo emergente della crittografia post-quantistica (PQC, Post-Quantum Cryptography) e fornisce indicazioni su come preparare l'ambiente aziendale. Sottolinea inoltre l'impegno di Dell Technologies per la costruzione di un futuro protetto dagli attacchi quantistici, attraverso l'integrazione della sicurezza in tutta la supply chain, nell'hardware, nel firmware, nel software e nell'intero ecosistema dei partner, conformemente agli standard NIST per la crittografia post-quantistica (FIPS 203, FIPS 204 e FIPS 205) e alle linee guida Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). Dell si prefigge un obiettivo chiaro, ovvero garantire il progresso dell'innovazione senza rinunciare ad affidabilità e sicurezza.

Terminologia

In questo white paper vengono utilizzati diversi termini tecnici. Di seguito ne vengono spiegati alcuni, per aiutare i lettori a comprendere meglio il testo.

Crittografia post-quantistica (PQC, Post-Quantum Cryptography): è un nuovo approccio matematico alla crittografia, che si avvale di nuovi algoritmi per proteggere i sistemi dagli attacchi dei computer quantistici. Tali algoritmi, che vengono eseguiti sui computer tradizionali, resistono sia agli attacchi quantistici, sia ai classici attacchi basati sulla crittografia.

Resilienza quantistica: sono resilienti agli attacchi quantistici tutti i sistemi, le infrastrutture e gli algoritmi progettati per rimanere sicuri anche in presenza di computer quantistici crittograficamente rilevanti (CRQC, Cryptographically Relevant Quantum Computer). Un sistema resiliente agli attacchi quantistici utilizza la crittografia post-quantistica o altre misure di protezione in grado di resistere sia agli attacchi classici che a quelli quantistici, assicurando la riservatezza, l'integrità e l'autenticità dei dati anche in futuro. Questo termine viene spesso considerato un sinonimo di "protezione dagli attacchi quantistici".

Agilità crittografica (o crypto-agilità): è la capacità dei sistemi e delle applicazioni aziendali di cambiare in modo rapido e trasparente gli algoritmi, i protocolli o la lunghezza delle chiavi di crittografia, senza richiedere una riprogettazione radicale o interruzioni prolungate delle attività.

"Raccogli ora, decifra più tardi" (HNDL, Harvest Now, Decrypt Later), o "Registra ora, decifra più tardi" (RNDL, Record Now, Decrypt Later): è una tattica in cui i malintenzionati raccolgono e archiviano i dati crittografati oggi, nell'intento di decifrarli in futuro con i computer quantistici crittograficamente rilevanti (CRQC, Cryptographically Relevant Quantum Computer).

L'elaborazione quantistica e la minaccia alla crittografia

L'ascesa dell'elaborazione quantistica

Come viene spiegato nel post di blog Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience del nostro CTO John Roese, risalente a circa un anno fa, nei computer tradizionali, ovvero i notebook, gli smartphone e i server, le informazioni elaborate sono costituite da sequenze di caratteri, denominati bit, che possono assumere solo i valori zero e 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.

Le potenziali applicazioni dell'elaborazione quantistica sono straordinarie. I ricercatori prevedono che verranno scoperti nuovi farmaci rivoluzionari, grazie alla possibilità di simulare le interazioni molecolari con una precisione che i computer tradizionali non sono semplicemente in grado di offrire. I climatologi prospettano modelli più accurati dei sistemi globali, mentre nel settore energetico esiste la possibilità di ottimizzare le reti elettriche e i sistemi di accumulazione. Anche la logistica e la produzione industriale prevedono di ottenere grandi vantaggi dalle tecniche di ottimizzazione quantistica. Tutti questi benefici sono reali e alla portata delle aziende, ma ciò vale anche per i rischi associati.

Perché la crittografia è a rischio

Nell'era digitale, la crittografia è alla base del concetto di fiducia. Quando un utente inserisce il numero della sua carta di credito, accede a un sito web sicuro o riceve un aggiornamento software firmato, la crittografia gli garantisce riservatezza, autenticità e integrità. La maggior parte delle misure di protezione è incentrata sulla crittografia a chiave pubblica, che si avvale di algoritmi come RSA ed ECC. Questi algoritmi sono basati su problemi matematici che non possono essere risolti con le capacità di calcolo dei sistemi tradizionali.

Ma l'elaborazione quantistica cambia le carte in tavola. Un computer quantistico abbastanza potente può utilizzare l'**algoritmo di Shor** per risolvere i problemi di fattorizzazione e logaritmo discreto da cui dipende l'efficacia della crittografia RSA ed ECC. I sistemi CRQC saranno pertanto in grado di compromettere le firme digitali che proteggono gli aggiornamenti software, le chiavi utilizzate per creare le sessioni TLS e i certificati di autenticazione dei dispositivi. Si tratta di un impatto sistemico che minaccia il meccanismo stesso su cui si basa la sicurezza delle transazioni digitali.

La crittografia a chiave simmetrica, che si basa su algoritmi come AES e viene utilizzata per proteggere i dati archiviati e le comunicazioni, dovrà affrontare altri problemi, anche se meno gravi. L'**algoritmo di Grover** permette a un computer quantistico di ridurre l'efficacia reale delle chiavi simmetriche, dimezzando di fatto il loro livello di protezione. Anche se il problema può essere mitigato aumentando le dimensioni delle chiavi, come nel caso di AES-256, questo cambiamento non fa che sottolineare l'onnipresenza delle minacce quantistiche.

Urgenza e conseguenze

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, il danno sarà già irreparabile.

Crittografia post-quantistica e standard emergenti

Definizione di 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.

La crittografia post-quantistica si basa su una serie di problemi matematici che, per quanto ne sappiamo, sono resistenti a tecniche quantistiche come gli algoritmi di Shor e di Grover. Le famiglie più promettenti sono costituite dalla crittografia basata su reticolo, dalle firme basate su hash, dagli schemi basati su codice e dalle equazioni multivariate. Questi approcci sono stati rigorosamente testati e standardizzati per garantire gli stessi livelli di affidabilità e interoperabilità di RSA ed ECC, una volta implementati.

L'impegno per la standardizzazione globale - Standard settoriali emergenti

Riconoscendo l'urgenza della minaccia, governi e organizzazioni di standardizzazione hanno fatto della crittografia post-quantistica una priorità globale. Lo U.S. National Institute of Standards and Technology (NIST) ha lanciato il suo progetto PQC nel 2016, invitando la comunità di ricerca crittografica a proporre, analizzare e perfezionare gli algoritmi candidati. Dopo anni di test, nell'agosto 2024 il NIST ha annunciato il primo gruppo di algoritmi standardizzati:

- **CRYSTALS -** Kyber per la crittografia a chiave pubblica e lo scambio delle chiavi
- **CRYSTALS -** Dilithium e SPHINCS+ per le firme digitali

Saranno disponibili anche altri algoritmi, attualmente ancora in fase di revisione, che forniranno i livelli di diversità e flessibilità necessari per rispondere a esigenze di implementazione diverse, inclusi sistemi leggeri come il firmware incorporato. Questo processo di standardizzazione in evoluzione offre alle organizzazioni di tutto il mondo un percorso chiaro per l'adozione di soluzioni resistenti agli attacchi quantistici.

Standard NIST - FIPS 203, 204, 205

Nell'agosto 2024 lo U.S. National Institute of Standards and Technology (NIST) ha finalizzato i primi algoritmi PQC:

- FIPS 203 (ML-KEM) - Basato sul meccanismo di incapsulamento delle chiavi CRYSTALS-Kyber, fornisce sicurezza IND-CCA2. Di conseguenza, il testo crittografato rimane indecifrabile anche in caso di attacco mirato.
- FIPS 204 (ML-DSA) - Algoritmo di firma digitale basato su CRYSTALS-Dilithium. Garantisce un'efficace sicurezza EUF-CMA (Existential UnForgeability Under Chosen-Message Attacks), il requisito standard per le firme digitali.
- FIPS 205 (SLH-DSA) - Schema di firma basato su hash, incentrato su SPHINCS+. È stato scelto come meccanismo di fallback prudenziale, indipendente dai problemi di reticolo.

Roadmap obbligatoria

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, ad esempio tramite il National Security Memorandum 10 (NSM-10), la Commercial National Security Algorithm Suite (CNSA 2.0), il National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547, l'Office of Management and Budget Memorandum 23-02 (OMB M-2302) e altro.

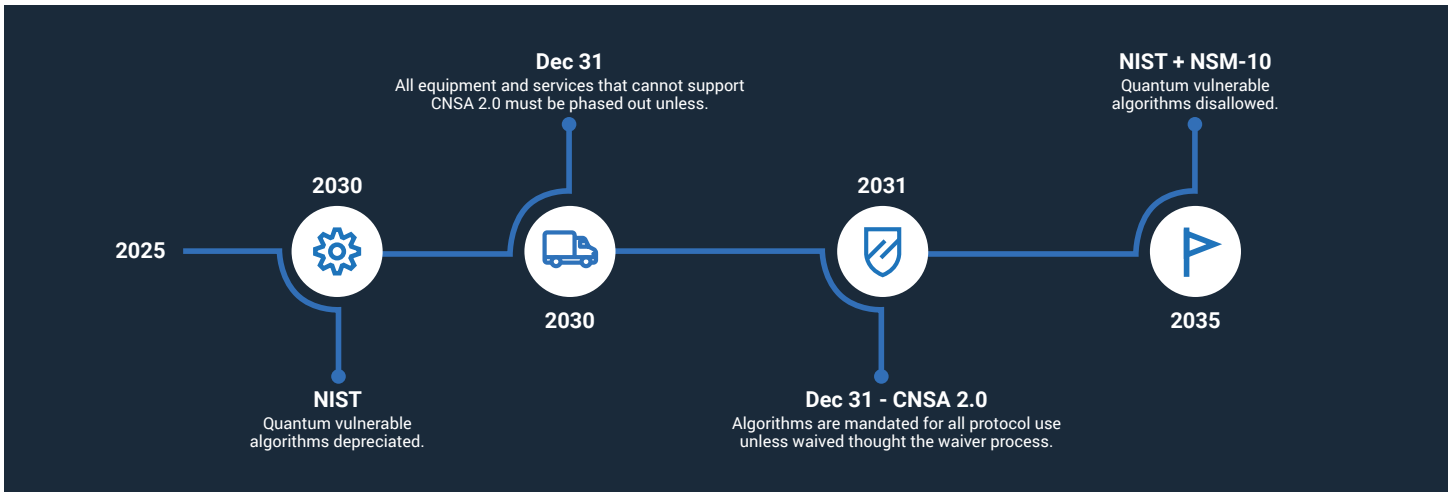
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodologies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

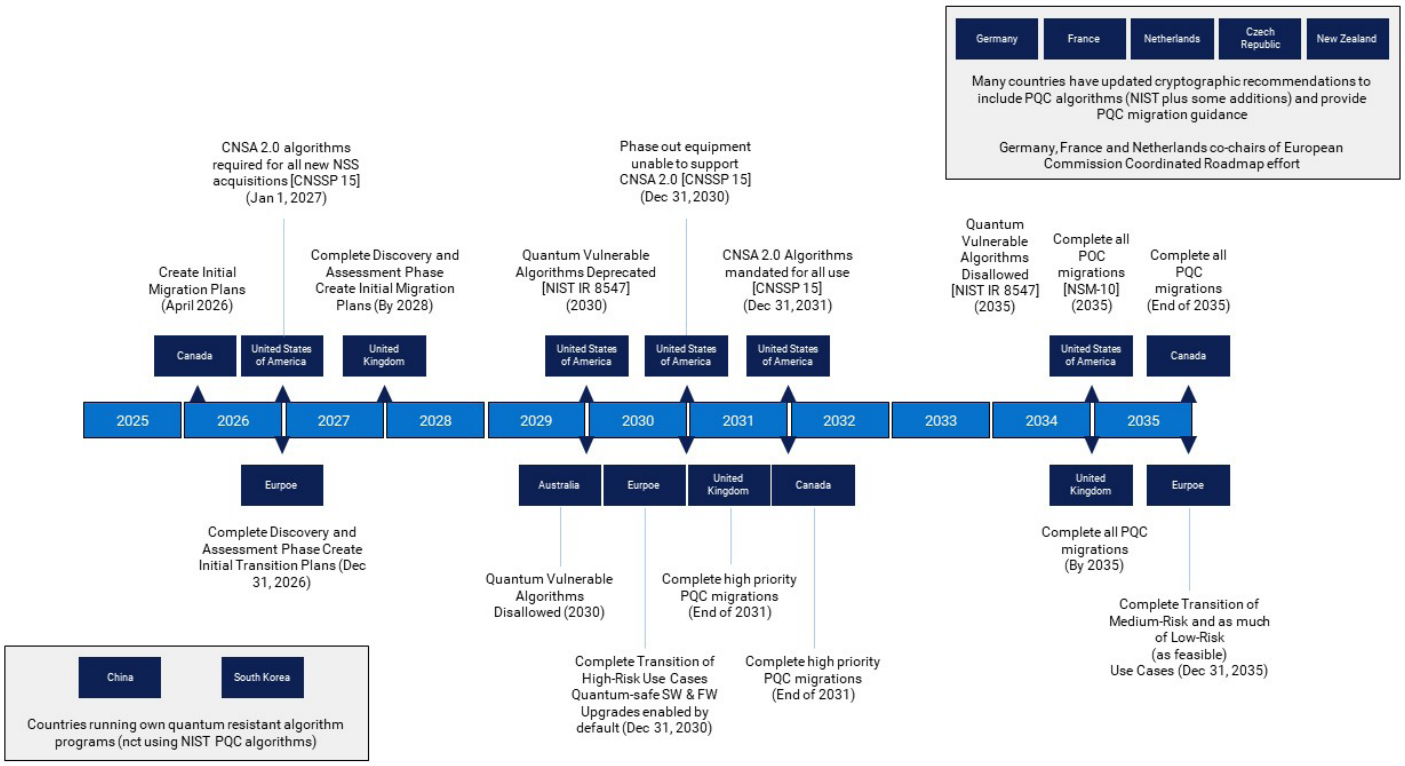
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detailed guidelines for federal agencies to how to comply with NSM-10

La suite CNSA 2.0, annunciata dall'NSA nel settembre 2022, introduce le prime raccomandazioni per gli algoritmi di crittografia post-quantistica, indicando esplicitamente le scadenze per l'adozione di algoritmi resistenti agli attacchi quantistici in tutti i sistemi di sicurezza nazionale (NSS, National Security System) e fornendo linee guida efficaci alle imprese che si preparano alla transizione.



Nel resto del mondo, anche altre organizzazioni hanno definito linee guida per la transizione alla crittografia PQC. Le scadenze obbligatorie per i vari Paesi sono riportate di seguito.



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.

Collaborazione nel settore

Oltre al NIST e all'NSA, attraverso la sua partecipazione attiva Dell sta influenzando anche i consorzi settoriali e i gruppi per gli standard che promuovono l'interoperabilità e l'adozione. Trusted Computing Group lavora all'integrazione della crittografia PQC nello standard per i moduli TPM (Trusted Platform Module). L'IETF promuove attivamente l'integrazione degli algoritmi PQC nei protocolli settoriali, come TLS e i certificati X.509. I comitati OASIS Key Management Interoperability Protocol (KMIP) supportano la crittografia PQC per i framework di gestione principali. La FIDO Alliance studia l'impatto della crittografia PQC sugli standard di autenticazione e onboarding dei dispositivi, mentre organizzazioni come SAFECode si impegnano a educare il settore, nell'intento di preparare le aziende alla migrazione.

Al fine di collaborare con gli operatori del settore, gli istituti accademici e la Pubblica amministrazione, il NIST ha dato vita al National Cyber Security Center of Excellence (NCCoE), che gestisce vari progetti incentrati sul dominio e dedicati a una serie di aspetti diversi, quali:

- Rilevamento della crittografia - Ha lo scopo di identificare gli algoritmi crittografici da migrare, assegnando le giuste priorità a ciascuno di essi.
- Interoperabilità - Occorre assicurare l'integrazione dei nuovi algoritmi PQC nelle funzionalità e nei protocolli di crittografia più diffusi, verificando anche l'interoperabilità fra le implementazioni dei diversi fornitori.
- Crypto-agilità - Nota anche come agilità crittografica, punta a sviluppare sistemi informativi che promuovono il supporto di adattamenti rapidi dei nuovi algoritmi e primitive di crittografia, senza stravolgere l'infrastruttura del sistema preesistente.

Questi progetti hanno lo scopo di raccogliere le informazioni necessarie per lo sviluppo delle indicazioni e degli standard creati dalle organizzazioni in questione, assicurando anche la disponibilità di soluzioni settoriali esemplificative per gli standard e le indicazioni che forniscono. Dell partecipa al progetto NCCoE Migration to PQC fin dall'inizio.

Oggi la crittografia PQC non è solo un argomento di ricerca, ma uno standard in via di sviluppo, con algoritmi, tempistiche e percorsi di adozione concreti. Le aziende che cominciano a prepararsi ora possono evitare i costi, i disservizi e i rischi tipici di chi corre ai ripari all'ultimo minuto. La transizione non serve solo a garantire la conformità, ma ha anche lo scopo di continuare ad assicurare i giusti livelli di affidabilità, riservatezza e integrità mentre l'elaborazione quantistica ridefinisce il panorama digitale.

Perché è importante agire ora

La minaccia imminente

Anche se si può avere la tentazione di pensare all'elaborazione quantistica come a un rischio ancora lontano, un pericolo che dovremo affrontare solo quando lo sviluppo della tecnologia sarà completato, in realtà il conto alla rovescia è già partito. Oggi le informazioni sensibili, come transazioni finanziarie, cartelle sanitarie, proprietà intellettuale e comunicazioni governative, sembrano essere crittografate in modo sicuro, ma quando i sistemi quantistici arriveranno al punto di violare gli algoritmi RSA o ECC, tali dati risulteranno esposti retroattivamente, mettendo improvvisamente a rischio tutto il backlog delle comunicazioni e dei record storici.

Cicli tecnologici troppo lunghi

I moderni ecosistemi IT non possono essere trasformati in modo semplice e veloce. Storicamente la sostituzione di un singolo algoritmo, come la transizione da SHA-1 a SHA-2 o da DES/3DES a AES, ha sempre richiesto almeno 10 anni. Poiché questi algoritmi sono profondamente incorporati nei sistemi operativi, nelle applicazioni, nei dispositivi di rete e nell'hardware, per sostituirli è necessario riprogettare, convalidare, testare e implementare soluzioni in ambienti che vanno dai data center alle piattaforme cloud, fino ai dispositivi edge. In molte organizzazioni questo potrebbe richiedere anni, ovvero molto più del tempo rimanente prima che l'elaborazione quantistica possa trasformarsi in una minaccia reale. Proprio per questo, i legislatori, le organizzazioni per gli standard e gli esperti di sicurezza continuano a sottolineare l'importanza di prepararsi oggi stesso. Se si attende la disponibilità generale dei sistemi CRQC, non resterà più tempo per una transizione ordinata.

Il rischio dell'inazione

Per le aziende che scelgono di posticipare la migrazione, le conseguenze andranno ben oltre la semplice esposizione tecnica:

- Rischio per la sicurezza dei dati: quando i computer quantistici saranno maturi, i dati storici, come le cartelle cliniche, le registrazioni finanziarie o le informazioni della difesa, potranno essere compromessi retroattivamente.
- Rischio per l'autenticità e l'integrità del software: l'autenticità e l'integrità del software firmato con i metodi attuali, che saranno ancora in uso quando i computer quantistici saranno maturi, rischiano di essere compromesse dal codice nocivo.
- Rischio operativo: come tutti sanno le infrastrutture critiche, come le utenze, le reti di trasportati e i servizi di emergenza, sono difficili da modernizzare. Se non si pianifica l'aggiornamento ora, si rischia un'interruzione delle operazioni future.
- Rischio di violazione dei requisiti di legge e conformità: framework come **CNSA 2.0** hanno stabilito tempistiche chiare per la conformità. Oltre all'esposizione, le organizzazioni che non si preparano rischiano anche di non risultare conformi alle norme di legge o ai regolamenti settoriali.
- Rischio reputazionale e finanziario: una violazione dovuta a vulnerabilità crittografiche non gestite può causare danni permanenti all'immagine del brand, oltre a notevoli perdite finanziarie.

Business case per l'azione proattiva

La preparazione proattiva non è una semplice misura difensiva, ma un'opportunità per aumentare la resilienza a lungo termine. Le aziende che effettuano un inventario della crittografia, aggiornano la lunghezza delle chiavi simmetriche, sperimentano soluzioni predisposte per la crittografia PQC e consultano i fornitori di prodotti resistenti agli attacchi quantistici possono mantenere la loro immagine di affidabilità. I pionieri si troveranno in una posizione di vantaggio per affrontare il futuro, garantire la conformità e dimostrare la loro leadership a clienti, partner e legislatori.

L'approccio di Dell alla crittografia post-quantistica

Noi di Dell riteniamo che la tecnologia sia alla base del progresso dell'umanità e che la sicurezza costituisca il fondamento di tale progresso. Come azienda, Dell Technologies deve assicurarsi che il suo portafoglio prodotti, la sua infrastruttura IT e i suoi sistemi di supporto del ciclo di vita siano adeguatamente preparati per la transizione agli algoritmi resistenti agli attacchi quantistici. A tale scopo, ha adottato la procedura seguente:

- Identificazione delle aree e delle finalità specifiche per cui viene utilizzata la crittografia, nei prodotti, nei servizi, nell'infrastruttura IT e nei sistemi di supporto, allo scopo di formulare piani di transizione esaustivi.
- Miglioramento delle competenze interne in materia di algoritmi di crittografia post-quantistica, tenendo conto degli aspetti implementativi e dei principi di progettazione correlati all'agilità crittografica per garantire una transizione senza problemi agli algoritmi PQC.
- Valutazione delle prestazioni, dell'applicabilità e dell'idoneità degli algoritmi PQC nei vari casi d'uso rilevanti per il portafoglio diversificato dei prodotti Dell Technologies.

Vista la complessità intrinseca della transizione agli algoritmi PQC, gli upgrade dei casi d'uso della crittografia nei prodotti Dell Technologies avverranno probabilmente in più fasi. Ad esempio, per quanto riguarda i dati, viene considerata prioritaria la transizione degli scenari di utilizzo che potrebbero essere vulnerabili agli attacchi HNDL, come i data in flight o la crittografia at-rest.

Nel caso di una piattaforma tecnologica, la transizione di uno scenario di utilizzo della crittografia potrebbe comportare l'aggiornamento o la sostituzione di un intero prodotto o un semplice upgrade. Tutto dipende dal prodotto in questione, oltre che dalla posizione e dalla modalità di implementazione della crittografia in tale prodotto e nei sistemi circostanti.

Nei prossimi cinque anni e oltre ci focalizzeremo sul rilascio di prodotti resistenti agli attacchi quantistici, per consentire ai clienti di rispettare le tempistiche della transizione a PQC pubblicate dai governi e dalle associazioni settoriali, che vanno dal 2027 al 2035.

I clienti sono invitati a contattare il proprio Account Team Dell per ottenere i dettagli specifici (come roadmap e tempistiche di rilascio) dei prodotti che intendono incorporare nei loro piani di migrazione. Nei prossimi mesi, Dell fornirà tempistiche più specifiche per l'integrazione degli algoritmi PQC nei suoi prodotti e linee commerciali.

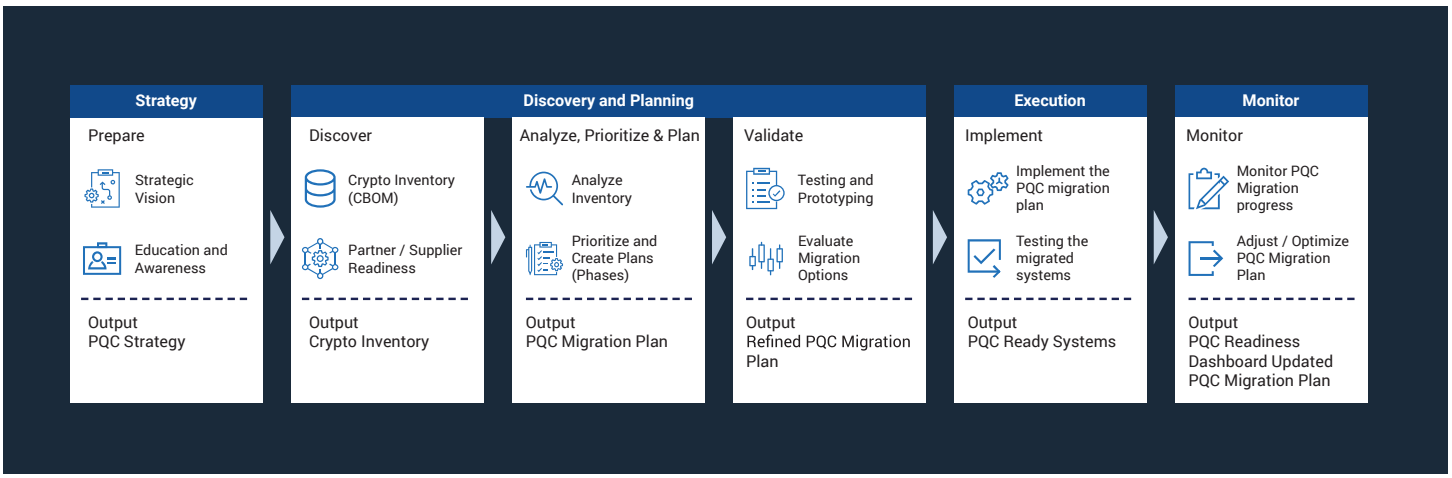
Innovazioni predisposte per la resilienza quantistica

Oltre ad aiutare i clienti a rispettare gli standard emergenti, Dell intende anche fornire loro tutto il supporto necessario per innovare in sicurezza nell'era quantistica. Dal deployment dei carichi di lavoro AI alla gestione degli ambienti hybrid cloud, fino alla modernizzazione dell'infrastruttura edge, i clienti hanno la certezza che le soluzioni Dell sono espressamente concepite per la resilienza. La sicurezza non viene aggiunta a posteriori, ma integrata per progettazione in ogni singolo livello del portafoglio Dell, per consentire alle aziende di affrontare con fiducia la transizione alla crittografia post-quantistica.

Preparazione per la transizione

La transizione alla crittografia post-quantistica 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.



Preparazione del profilo di sicurezza attuale

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. Inoltre, è importante aggiornare la lunghezza delle chiavi per la crittografia a chiave simmetrica sui nuovi sistemi, come AES-256 e SHA-384 o versioni successive, in modo da compensare la riduzione dei margini dovuta all'introduzione dell'algoritmo 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 crittografici

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 e i dati archiviati. 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 urgenza, perché sono i più vulnerabili alle minacce HNDL.

Progetti pilota per la sperimentazione della crittografia PQC

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.

Approccio all'adozione e all'interoperabilità

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 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 laboratori ibridi, che combinano tecnologie tradizionali e quantistiche, 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

Infine, 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.

La preparazione per la crittografia PQC non è una gara di velocità, ma una maratona. L'adozione di un approccio graduale, che prevede il consolidamento delle difese attuali, l'audit degli asset crittografici, la sperimentazione delle soluzioni PQC, l'adozione di strategie ibride e l'esecuzione di una migrazione completa permette alle aziende di procedere in tutta sicurezza verso la resilienza quantistica. E scegliendo Dell come partner, questo percorso non è solo fattibile, ma offre anche l'opportunità di aumentare l'affidabilità e supportare adeguatamente l'innovazione in vista del futuro.

Applicazioni e vantaggi reali

La transizione alla crittografia post-quantistica non è solo un esercizio di conformità, ma un imperativo di business che produce conseguenze dirette sui livelli di affidabilità, resilienza e competitività a lungo termine. L'adozione di algoritmi resistenti agli attacchi quantistici garantisce ai provider di servizi di telecomunicazioni, agli istituti finanziari, alle organizzazioni sanitarie e alla pubblica amministrazione che l'infrastruttura digitale critica rimarrà sicura anche a fronte delle minacce future, oltre che di quelle attuali.

Telecomunicazioni

Le reti di telecomunicazione sono la spina dorsale della digitalizzazione globale, poiché svolgono un ruolo essenziale per qualunque attività, dai servizi di emergenza alla connettività IoT, fino alle comunicazioni con i clienti. Un attacco quantistico in questo settore rischia di compromettere il provisioning delle SIM, l'onboarding delle eSIM o i processi di autenticazione alla base della connettività 4G e 5G. Gli operatori che implementano ora una soluzione di crittografia ibrida protetta dagli attacchi quantistici riusciranno a mantenere la fiducia dei clienti, a proteggere la riservatezza dei dati e a garantire la continuità dei servizi in modo trasparente, mentre la tecnologia mobile passa da una generazione all'altra.

Servizi finanziari

Il settore finanziario è uno dei più bersagliati dai criminali informatici, e l'integrità delle transazioni dipende dalla crittografia. La preparazione per la crittografia post-quantistica protegge i pagamenti digitali, i servizi bancari online e i trasferimenti interbancari dalle frodi che sfruttano le tecnologie quantistiche. Inoltre, l'adozione precoce dimostra a legislatori e clienti che gli istituti si impegnano a proteggere gli asset e a mantenere la stabilità dei sistemi. In questo settore, l'adozione di una crittografia futuristica riduce sia l'esposizione ai rischi reputazionali, sia il rischio di violare le normative.

Settore sanitario

Le cartelle cliniche dei pazienti, i dati genomici e i dispositivi medicali connessi sono tutti esposti agli attacchi HNDL. Rispetto agli altri, il settore sanitario deve affrontare una difficoltà in più, perché i dati sanitari sensibili devono essere conservati per periodi di tempo molto lunghi. Gli ospedali e gli operatori sanitari che cominciano ora la transizione alla crittografia PQC possono garantire la riservatezza delle cartelle cliniche sia nel presente che nei decenni futuri. Questo aspetto è essenziale per mantenere la fiducia dei pazienti e al tempo tesso continuare a rispettare le normative in materia di protezione dei dati, che sono in continua evoluzione.

Pubblica amministrazione e infrastruttura critica

Dalle comunicazioni della difesa ai sistemi di distribuzione dell'energia, le aziende che operano nei settori della pubblica amministrazione e delle infrastrutture dipendono dalla crittografia per garantire la continuità operativa e la sicurezza nazionale. Oltre a proteggerci dai malintenzionati nel breve termine, la crittografia post-quantistica fornisce anche una tutela contro le strategie che prevedono la raccolta delle comunicazioni crittografate nell'intento di sfruttarle in futuro. L'allineamento con framework quali CNSA 2.0 garantisce l'interoperabilità, la sicurezza e l'affidabilità dei sistemi della pubblica amministrazione anche nell'era dell'elaborazione quantistica.

Vantaggi generali per le aziende

Come abbiamo visto, la transizione alla PQC è chiaramente un'esigenza tecnica, ma anche il business case è altrettanto solido:

- Affidabilità e reputazione del brand: dimostra la leadership dell'azienda nel campo della tutela dei dati di clienti e partner.
- Conformità alle normative: garantisce l'allineamento agli standard NIST e agli obblighi di legge, come CNSA 2.0.
- Resilienza operativa: riduce il rischio di disservizi catastrofici dovuti alla violazione della crittografia.
- Distinzione dalla concorrenza: permette all'azienda di presentarsi come un innovatore proattivo, anziché come un seguace reattivo.

Ma i vantaggi dell'adozione precoce vanno ben oltre la resilienza tecnica. Oltre a ridurre i rischi, le aziende che adottano precocemente la crittografia PQC aumentano anche la loro capacità di innovare, rispettare le normative e competere in un'economia digitale incentrata sulla fiducia.

Fai le prossime mosse

L'avvento dell'elaborazione quantistica costituisce sia un'opportunità generazionale, sia una problematica di sicurezza senza precedenti. Anche se non conosciamo ancora le tempistiche esatte dell'introduzione dei computer quantistici crittograficamente rilevanti, sappiamo per certo che dobbiamo prepararci. La transizione alla crittografia post-quantistica richiederà anni di pianificazione, esecuzione e investimenti coordinati, e non conviene aspettare che i computer quantistici diventino operativi.

Le organizzazioni devono innanzitutto acquisire consapevolezza della situazione, comprendere dove e come viene utilizzata la crittografia in tutto il loro ambiente. Fatto questo, devono cominciare a stilare un inventario degli asset, assegnare le giuste priorità e sperimentare soluzioni protette dagli attacchi quantistici. La crittografia ibrida, che combina algoritmi classici e post-quantistici, fornisce un percorso immediato verso la resilienza, mentre gli standard continuano a evolversi. Le aziende che allineano le roadmap interne con i framework globali, come gli standard PQC del NIST e le tempistiche CNSA 2.0, possono procedere in tutta sicurezza verso la conformità e l'interoperabilità.

Dell Technologies rimane a disposizione dei clienti per aiutarli durante la transizione. Il nostro approccio garantisce una base solida, assicurando l'integrità della supply chain, misure di protezione incorporate nell'hardware e adattabilità supportata dal software. Grazie alle nostre partnership con i migliori provider di soluzioni di sicurezza e alla nostra partecipazione attiva alle organizzazioni per gli standard settoriali, oltre a garantire il rispetto dei requisiti più recenti le soluzioni Dell vengono anche testate in condizioni reali, per convalidarne prestazioni e interoperabilità.

Le imprese devono cominciare a prepararsi fin da ora con una fase di indagine e analisi del rischio, per poi contattare fornitori affidabili e sperimentare nuove tecnologie protette dagli attacchi quantistici. Tutto quello che viene fatto ora riduce il rischio di subire disservizi in futuro. Oltre a garantire la protezione dei loro dati e sistemi, le aziende che si preparano in anticipo riusciranno anche a conquistare la fiducia di clienti, legislatori e partner, in un'era in cui la fiducia nel digitale riveste la massima importanza.

Chi siamo

Dell Technologies si impegna a realizzare tecnologie avanzate accessibili, affidabili e al servizio di tutti. Aiutiamo persone singole e organizzazioni a sfruttare l'innovazione in tutta sicurezza, preparando la strada per un futuro più protetto, inclusivo e connesso.

Ulteriori informazioni sulle soluzioni [nome prodotto] Dell

Contatta un esperto Dell Technologies

Visualizza altre risorse

Partecipa alla conversazione con #HashTag