DELL Technologies

WHITEPAPER

Post-Quanten-Kryptografie: Vorbereitung auf das Quantenzeitalter

Ein Whitepaper von Dell Technologies

Inhaltsverzeichnis

Übersicht für Führungskräfte

Quantencomputing entwickelt sich schnell von der theoretischen Forschung zur praktischen Realität. Die Technologie galt einst als Zukunftsvision, aber mittlerweile beschleunigen Fortschritte bei Hardware, Algorithmen und Investitionen das Aufkommen von Rechnern, die Probleme lösen können, die für herkömmliche Computer nicht lösbar sind. Die Auswirkungen auf die Branche sind tiefgreifend. Von der Arzneimittelforschung über die Klimamodellierung bis hin zur globalen Logistik verspricht Quantencomputing, Innovationen zu erschließen, die zuvor nicht erreichbar waren.

Aber dieser Durchbruch bringt eine disruptive Herausforderung mit sich: Quantencomputer werden die kryptografischen Grundlagen untergraben, die die digitale Wirtschaft schützen. Kryptografie mit öffentlichen Schlüsseln – Algorithmen wie RSA und Elliptic Curve Cryptography (ECC) – schützt seit Jahrzehnten die digitale Kommunikation, Finanzsysteme, Patientenakten und die nationale Sicherheit. Diese Methoden basieren auf mathematischen Problemen, die auf klassischen Computern nicht zu lösen sind. Doch mit dem Aufkommen von kryptografisch relevanten Quantencomputern (Cryptographically Relevant Quantum Computers, CRQCs) können diese Probleme effizient gelöst und heutige Sicherheitseinrichtungen überwunden werden.

Es handelt sich nicht nur um eine theoretische Bedrohung. Einige Organisationen nutzen bereits eine Taktik, die als „Harvest Now, Decrypt Later“ (HNDL) bezeichnet wird. Sie sammeln heute verschlüsselte Daten mit der Erwartung, sie zu entschlüsseln, sobald Quantencomputer ausgereift sind. Vertrauliche Informationen, die jetzt sicher erscheinen, können in wenigen Jahren anfällig sein. Die Zeit zum Handeln ist nicht der Zeitpunkt, an dem CRQCs Realität werden, sondern jetzt.

In diesem Whitepaper wird die Dringlichkeit der Quantenbedrohung erläutert, das aufkommende Feld der Post-Quanten-Kryptografie (Post-Quantum Cryptography, PQC) untersucht und Ratschläge dazu bereitgestellt, wie Unternehmen sich darauf vorbereiten können. Es unterstreicht das Engagement von Dell Technologies für den Aufbau einer quantensicheren Zukunft – die Integration von Sicherheit in unsere Lieferkette, Hardware, Firmware, Software und Partnernetzwerke – durch die Ausrichtung an den PQC-Standards von NIST – FIPS 203, FIPS 204 und FIPS 205 – sowie an den Richtlinien der Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). Das Ziel von Dell ist klar: sicherzustellen, dass Innovation voranschreiten kann, ohne Sicherheit oder Vertrauen zu opfern.

Terminologie

In diesem Whitepaper werden Sie auf eine Reihe von Begriffen stoßen. Wir haben versucht, einige dieser Begriffe zu erläutern, um das Verständnis des Artikels zu erleichtern.

Post-Quanten-Kryptografie: Ein neuer mathematischer Ansatz für die Kryptografie mit neuen Algorithmen, der vor Angriffen durch Quantencomputer geschützt sein soll. Diese Algorithmen können auf klassischen Computern ausgeführt werden und sind sowohl gegen Quantenangriffe als auch gegen bekannte klassische Kryptographieangriffe resistent.

Quantenresistent: Dieser Begriff bezieht sich auf Systeme, Algorithmen oder Infrastrukturen, die selbst bei Vorhandensein von kryptografisch relevanten Quantencomputern (CRQCs) sicher bleiben. Ein quantenresistentes System nutzt Post-Quanten-Kryptografie (PQC) oder andere Schutzmaßnahmen, die sowohl herkömmlichen als auch quantenbasierten Angriffen standhalten und die Vertraulichkeit, Integrität und Authentizität von Daten auch in Zukunft sicherstellen. Andere Begriffe wie quantenresilient und quantensicher werden außerdem austauschbar verwendet.

Kryptografische Agilität (manchmal auch als Krypto-Agilität bezeichnet): Dieser Begriff bezieht sich auf die Fähigkeit der Systeme und Anwendungen eines Unternehmens, kryptografische Algorithmen, Protokolle oder Schlüssellängen schnell und nahtlos zu wechseln, ohne dass größere Neuentwicklungen oder Betriebsunterbrechungen erforderlich sind.

„Harvest Now, Decrypt Later“ (HNDL): Mit dieser auch als „Record Now, Decrypt Later“ bezeichneten Aktivität erfassen und speichern AngreiferInnen heute verschlüsselte Daten mit der Absicht, sie in Zukunft zu entschlüsseln, sobald kryptografisch relevante Quantencomputer (CRQCs) verfügbar sind.

Quanten-Computing und die Bedrohung für die Verschlüsselung

Das Aufkommen von Quanten-Computing

Wie wir im Blogbeitrag Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience von unserem CTO John Roese vor fast einem Jahr beschrieben haben, verarbeiten herkömmliche Computer – ob Laptops, Smartphones oder Server – Informationen mithilfe von Bits, die den Zustand Null oder Eins annehmen. Dieses Binärmodell hat jahrzehntelang den Fortschritt vorangetrieben, aber es gibt hier Einschränkungen bei Darstellung und Bearbeitung von Informationen. Quantencomputer verwenden Qubits, die durch Prinzipien wie Überlagerung und Verschränkung in mehreren Zuständen gleichzeitig existieren können. Auf diese Weise können Quantenmaschinen eine große Anzahl möglicher Lösungen parallel erkunden, was einen Rechenvorteil für bestimmte Problemklassen bietet.

Die potenziellen Anwendungen von Quantencomputing sind außergewöhnlich. ForscherInnen antizipieren bahnbrechende Fortschritte in der Pharmazeutik, indem sie molekulare Interaktionen mit einer Präzision simulieren, die klassische Computer nicht erreichen können. KlimawissenschaftlerInnen stellen sich präzisere Modelle globaler Systeme vor, während der Energiesektor Potenzial für die Optimierung von Stromnetzen und -speichern sieht. Auch Logistik und Fertigung profitieren von Quantenoptimierungstechniken. Die Vorteile sind real und in Reichweite – das gilt aber auch für die Risiken.

Warum die Verschlüsselung gefährdet ist

Verschlüsselung steht für Vertrauen im digitalen Zeitalter. Wenn Sie eine Kreditkartennummer eingeben, sich bei einer sicheren Website anmelden oder ein signiertes Softwareupdate erhalten, sorgt die Kryptografie für Vertraulichkeit, Authentizität und Integrität. Der größte Teil dieses Schutzes stützt sich auf Kryptographie mit öffentlichen Schlüsseln – Algorithmen wie RSA und ECC, die auf mathematischen Problemen basieren, welche für herkömmliche Maschinen als rechnerisch unausführbar gelten.

Das Quantencomputing stellt diese Gleichung um. Mithilfe des **Shor-Algorithmus** kann ein ausreichend leistungsstarker Quantencomputer die Faktorisierungs- und diskreten Logarithmusprobleme lösen, die RSA und ECC ihre Stärke verleihen. Sobald CRQCs vorhanden sind, können die digitalen Signaturen, die Softwareupdates schützen, die Schlüssel, die TLS-Sitzungen einrichten, und die Zertifikate, die Geräte authentifizieren, kompromittiert werden. Die Auswirkungen sind systemisch und bedrohen genau die Mechanismen, die digitale Transaktionen sicher machen.

Symmetrische Kryptografie: Algorithmen wie AES, die zum Schutz gespeicherter Daten oder sicherer Kommunikation verwendet werden – hier ergibt sich eine andere, wenn auch weniger schwerwiegende Herausforderung. **Der Grover-Algorithmus** ermöglicht es einem Quantencomputer, die effektive Stärke symmetrischer Schlüssel zu reduzieren und so die Sicherheit effektiv zu halbieren. Dies kann zwar durch die Umstellung auf größere Schlüsselgrößen wie AES-256 gemindert werden, die Anpassung unterstreicht jedoch die durchdringende Reichweite von Quantenbedrohungen.

Dringlichkeit und Konsequenzen

Die Folgen gehen weit über das theoretische Risiko hinaus. Unternehmen, die sich nicht entsprechend vorbereiten, müssen mit der Offenlegung von sensiblem geistigem Eigentum, Unterbrechungen von Finanzsystemen, Verstößen gegen Vorschriften zu Gesundheitsdaten und Bedrohungen für die nationale Sicherheit rechnen. Die Strategie „Harvest Now, Decrypt Later“ verschärft die Dringlichkeit: AngreiferInnen müssen heute nur verschlüsselte Daten erfassen und auf die Mittel warten, mit denen sie entschlüsselt werden können. Wenn CRQCs verfügbar sind, ist der Schaden bereits irreversibel.

Post-Quanten-Kryptografie und neue Standards

Definition der Post-Quanten-Kryptografie

Post-Quanten-Kryptografie (PQC) bezieht sich auf eine neue Generation von Algorithmen, die digitale Systeme sowohl vor herkömmlichen als auch vor Quantenangriffen schützen. Im Gegensatz zur Quantenschlüsselverteilung, die spezielle Hardware erfordert, ist PQC für die Ausführung auf der herkömmlichen Infrastruktur von heute – Servern, Endpunkten und Netzwerken – konzipiert und somit die praktischste und skalierbarste Möglichkeit, sich auf das Quantenzeitalter vorzubereiten.

Die Grundlage von PQC ist eine Reihe mathematischer Probleme, die nach bestem aktuellem Wissen resistent gegen Quantentechniken wie Shor- und Grover-Algorithmen sind. Gitterbasierte Kryptografie, hashbasierte Signaturen, codebasierte Schemata und multivariate Gleichungen stellen die vielversprechendsten Ansätze dar. Diese Ansätze werden rigoros getestet und standardisiert, um sicherzustellen, dass sie die gleiche Zuverlässigkeit und Interoperabilität bieten, die RSA und ECC einst geliefert haben.

Die globale Standardisierungsinitiative – neue Branchenstandards

Angesichts der Dringlichkeit der Bedrohung haben Regierungen und Normungsgremien PQC zu einer globalen Priorität erklärt. Das U.S. National Institute of Standards and Technology (NIST) startete 2016 sein PQC-Projekt und forderte die kryptografische Forschungsgemeinschaft auf, geeignete Algorithmen vorzuschlagen, zu analysieren und zu optimieren. Nach jahrelangen Tests kündigte NIST im August 2024 die erste Gruppe standardisierter Algorithmen an:

- **CRYSTALS**-Kyber für Verschlüsselung und Schlüsseleinrichtung mit öffentlichen Schlüsseln
- **CRYSTALS**-Dilithium und SPHINCS+ für digitale Signaturen

Weitere Algorithmen werden geprüft, um Diversität und Flexibilität für verschiedene Implementierungsanforderungen zu bieten, einschließlich unkomplizierter Systeme wie integrierte Firmware. Dieser sich weiterentwickelnde Standardisierungsprozess stellt sicher, dass Unternehmen weltweit ein klarer Weg zur Einführung quantenresistenter Lösungen offensteht.

NIST-Standards – FIPS 203, 204, 205

Im August 2024 hat das U.S. National Institute of Standards and Technology (NIST) die ersten PQC-Algorithmen finalisiert:

- FIPS 203 (ML-KEM) – basierend auf CRYSTALS-Kyber, einem wichtigen Kapselungsmechanismus. Er bietet IND-CCA2-Sicherheit, was bedeutet, dass Chiffretexte auch bei adaptiven ausgewählten Chiffretextangriffen nicht unterscheidbar bleiben.
- FIPS 204 (ML-DSA) – basierend auf CRYSTALS-Dilithium, einem digitalen Signaturalgorithmus. Er bietet robuste EUF-CMA-Sicherheit (existenzielle Unfälschbarkeit unter ausgewählten Nachrichtenangriffen), die Standardanforderung für digitale Signaturen.
- FIPS 205 (SLH-DSA) – basierend auf SPHINCS+, einem hashbasierten Signaturschema. Dieser wurde als konservatives Reservesystem ausgewählt, das nicht von Gitterproblemen abhängig ist.

Eine vorgegebene Roadmap

Nachdem die US-Bundesregierung die Bedeutung der Einführung quantenresistenter Verschlüsselungsalgorithmen erkannte, hat sie begonnen, PQC-Anforderungen an Bundesbehörden auszustellen. Dazu gehören das National Security Memorandum 10 (NSM-10), die Commercial National Security Algorithm Suite (CNSA 2.0), der National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547 sowie das Office of Management and Budget Memorandum 23-02 (OMB M-2302) und andere.

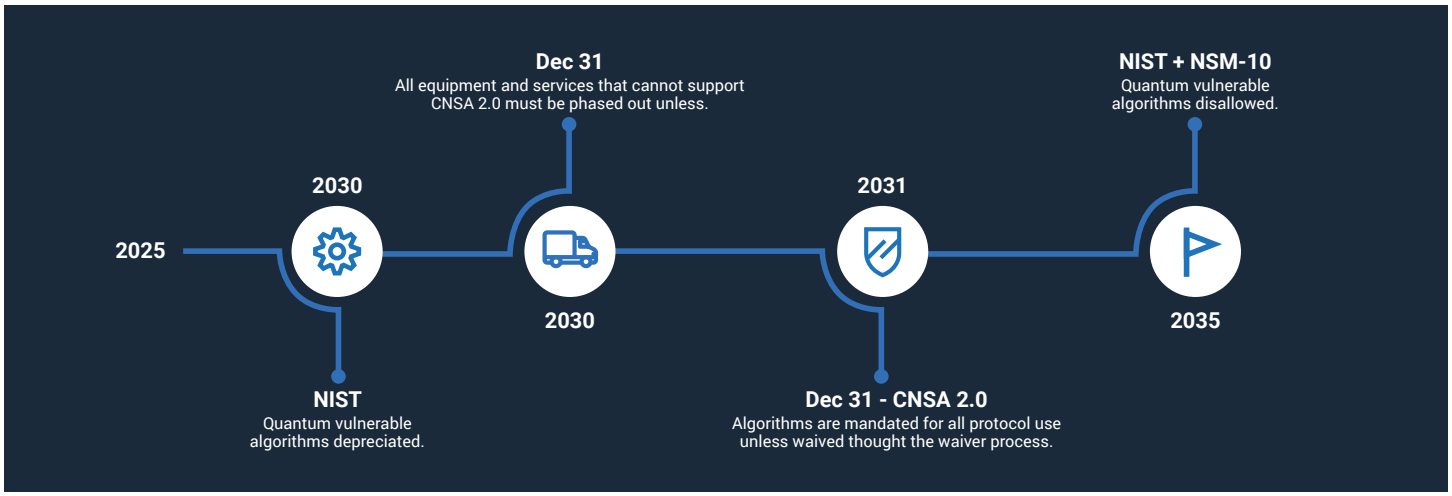
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

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

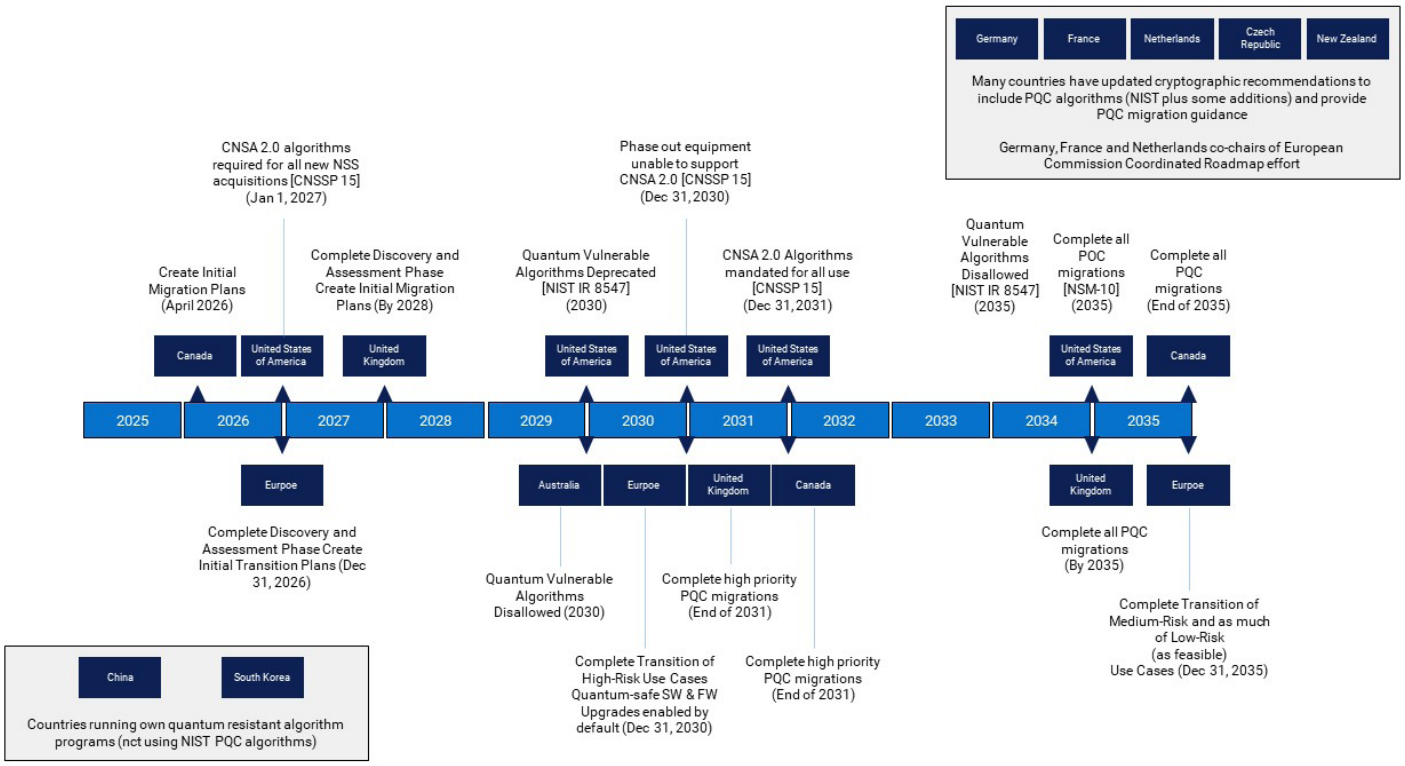
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

CNSA 2.0, die von der NSA im September 2022 angekündigt wurde, führt die ersten Empfehlungen für Post-Quanten-kryptografische Algorithmen ein. CNSA 2.0 legt explizite Fristen für die Einführung quantenresistenter Algorithmen in nationalen Sicherheitssystemen (NSS) fest und dient als leistungsstarker Leitfaden für Unternehmen, die ihre eigenen Umstellungen vorbereiten:



Andere Organisationen auf der ganzen Welt haben ebenfalls Richtlinien für die PQC-Umstellung festgelegt. Im Folgenden finden Sie einige der verschiedenen länderspezifischen Bestimmungen.



Diese Termine sind nicht willkürlich – sie spiegeln die Vorlaufzeiten wider, die für die Neugestaltung, Validierung und Bereitstellung von Kryptografie in komplexen IT-Ökosystemen erforderlich sind. Unternehmen sollten sie nicht nur als behördliche Vorgaben betrachten; sie sind praktische Indikatoren für den globalen Wandel hin zu Quantenresilienz.

Zusammenarbeit in der Branche

Über NIST und NSA hinaus nimmt Dell aktiv Einfluss und beteiligt sich an Branchenkonsortien und Standardgruppen, die Interoperabilität und Einführung vorantreiben. Die Trusted Computing Group integriert PQC in den TPM-Standard (Trusted Platform Module). Die IETF bringt einen Großteil der Integration von PQC-Algorithmen in Branchenprotokolle wie TLS und X.509-Zertifikate voran. Die OASIS-KMIP-Ausschüsse (Key Management Interoperability Protocol) ermöglichen PQC für wichtige Management-Frameworks. Die FIDO Alliance untersucht die Auswirkungen von PQC auf Authentifizierungs- und Geräteintegrationsstandards, während Unternehmen wie SAFECode daran arbeiten, die Branche über die Migrationsbereitschaft zu informieren.

Das NIST National Cyber Security Center of Excellence (NCCoE) ist das Konstrukt, mit dem NIST über bereichsspezifische Projekte mit der Industrie, der Wissenschaft und den Behörden zusammenarbeiten kann. Der Fokus liegt unter anderem auf folgenden Themen:

- Kryptografische Erkennung, mit der identifiziert wird, welche Kryptografie migriert werden muss und wie priorisiert wird, was zuerst migriert werden soll
- Interoperabilität, die sicherstellt, dass beliebte kryptografische Funktionen und Protokolle die neuen PQC-Algorithmen enthalten und die Implementierung von verschiedenen Anbietern interoperabel ist
- Krypto-Agilität, wobei der Schwerpunkt auf der Entwicklung von Informationssystemen liegt, die Unterstützung für schnelle Anpassungen neuer kryptografischer Primitive und Algorithmen bieten, ohne wesentliche Änderungen an der Systeminfrastruktur vorzunehmen – dies wird auch als kryptografische Agilität bezeichnet

Diese Projekte tragen dazu bei, die erarbeiteten Leitlinien und Standards zu prägen/entwickeln, und stellen sicher, dass es beispielhafte Branchenlösungen für die von ihnen bereitgestellten Standards und Leitlinien gibt. Dell ist am Projekt NCCoE Migration to PQC seit seiner Gründung beteiligt.

Heute ist PQC nicht nur ein Forschungsthema, sondern ein sich entwickelnder Standard mit konkreten Algorithmen, Zeitplänen und Einführungspfaden. Unternehmen, die jetzt mit der Vorbereitung beginnen, können die Kosten, Unterbrechungen und Risiken einer Last-Minute-Krise vermeiden. Bei der Umstellung geht es nicht nur um Compliance – vielmehr muss sichergestellt werden, dass Vertrauen, Vertraulichkeit und Integrität intakt bleiben, wenn Quantencomputing die digitale Landschaft neu gestaltet.

Warum Sie jetzt handeln müssen

Die unmittelbare Bedrohung

Es mag verlockend sein, Quantencomputing als entferntes Risiko zu betrachten, etwas, das angegangen werden kann, sobald die Technologie vollständig realisiert ist. In Wirklichkeit tickt die Uhr bereits jetzt. Sensible Informationen – Finanztransaktionen, Patientenakten, geistiges Eigentum oder Behördenkommunikation – können heute sicher verschlüsselt werden. Sobald Quantencomputer aber die Schwelle erreichen, RSA oder ECC zu überwinden, können diese Daten rückwirkend offengelegt werden. Das Ergebnis ist, dass ein umfangreicher Bestand an historischen Kommunikationen und Aufzeichnungen plötzlich gefährdet sein könnte.

Lange Technologiezyklen

Moderne IT-Ökosysteme lassen sich nicht einfach oder schnell transformieren. In der Vergangenheit hat der Austausch einzelner Algorithmen, wie z. B. der Übergang von SHA-1 zu SHA-2 oder DES/3DES zu AES, mehr als 10 Jahre in Anspruch genommen. Diese Algorithmen sind tief in Betriebssysteme, Anwendungen, Netzwerkgeräte und Hardware integriert. Der Austausch erfordert ein neues Design, eine Validierung, Tests und eine Bereitstellung über Umgebungen hinweg, die von Rechenzentren über Cloud-Plattformen bis hin zu Edge-Geräten reichen. Für viele Unternehmen wird dies Jahre dauern – weit länger als das verbleibende Zeitfenster, bevor Quantencomputing eine reale Bedrohung darstellt. Regulierungsbehörden, Normungsgremien und Sicherheitsvorreiter betonen daher die Notwendigkeit einer sofortigen Vorbereitung. Wenn Sie warten, bis CRQCs weithin verfügbar sind, bleibt Ihnen keine Zeit für eine geordnete Umstellung.

Risiken der Untätigkeit

Die Folgen einer verzögerten Migration gehen über die technische Gefährdung hinaus:

- Risiken in Bezug auf die Datensicherheit: Langlebige Daten wie Patientenakten, Finanzdaten oder Verteidigungsinformationen können rückwirkend kompromittiert werden, sobald Quantencomputer ausgereift sind.
- Risiken in Bezug auf die Softwareauthentizität und -integrität: Softwareauthentizität und -integrität können durch bösartigen Code gefährdet werden, wenn sie mit aktuellen Signaturmethoden signiert und immer noch verwendet werden, nachdem Quantencomputer ausgereift sind.
- Betriebliches Risiko: Bei kritischen Infrastruktursystemen wie Versorgungsunternehmen, Transportnetzwerken und Notfalldiensten stellen Aktualisierungsvorgänge bekanntermaßen eine große Herausforderung dar. Wenn Sie jetzt nicht planen, kann dies später zu einer Betriebsunterbrechung führen.
- Regulatorische und Compliancerisiken: Frameworks wie **CNSA 2.0** haben klare Zeitrahmen für die Compliance festgelegt. Unternehmen, die sich nicht auf Risiken vorbereiten, riskieren nicht nur die Offenlegung, sondern auch die Nichteinhaltung von Behörden- oder Branchenerwartungen.
- Reputations- und Finanzrisiko: Eine Sicherheitsverletzung, die auf nicht behobene kryptografische Sicherheitslücken zurückzuführen ist, kann zu einem dauerhaften Schaden des Markenvertrauens und erheblichen finanziellen Verlusten führen.

Der Grund für proaktive Maßnahmen

Proaktive Vorbereitung ist nicht nur eine Verteidigungsmaßnahme, sondern eine Chance, die langfristige Widerstandsfähigkeit zu stärken. Durch kryptografische Bestandsaufnahmen, eine Aktualisierung symmetrischer Schlüssellängen, Pilotprojekte für PQC-fähige Lösungen und die Zusammenarbeit mit Anbietern, die quantenresistente Lösungen anbieten, können Unternehmen kontinuierliches Vertrauen sicherstellen. Early Adopters sind besser positioniert, zukunftssichere Betriebsabläufe zu gewährleisten, die Compliance aufrechtzuerhalten sowie gegenüber Kunden, Partnern und Aufsichtsbehörden eine führende Rolle einzunehmen.

Der Ansatz von Dell für die Post-Quanten-Kryptografie

Wir bei Dell glauben, dass Technologie den menschlichen Fortschritt vorantreibt und Sicherheit die Grundlage für diesen Fortschritt ist. Als Unternehmen stellt Dell Technologies sicher, dass sein Portfolio, seine IT-Infrastruktur und seine Lebenszyklusunterstützungssysteme gut auf den Übergang zu quantenresistenten Algorithmen vorbereitet sind. Die Schritte zur Vorbereitung auf die Umstellung umfassen:

- Identifizieren der spezifischen Bereiche und Zwecke, in denen Kryptografie in Produkten, Services, IT-Infrastruktur und Supportsystemen eingesetzt wird, um umfassende Übergangspläne zu formulieren
- Erweitern des internen Wissens über PQC-Algorithmen (Post-Quanten-Kryptografie) unter Berücksichtigung von Implementierungsaspekten und Designprinzipien im Zusammenhang mit Krypto-Agilität, um eine reibungslose Umstellung auf PQC-Algorithmen zu erleichtern
- Bewerten der Leistung, Anwendbarkeit und Eignung von PQC-Algorithmen in verschiedenen Anwendungsfällen, die für das vielfältige Portfolio von Dell Technologies relevant sind

Angesichts der Komplexität der PQC-Umstellung werden Upgrades der kryptografischen Anwendungsfälle in Dell Technologies Angeboten möglicherweise schrittweise eingeführt. Aus Datensicht wird die Umstellung beispielsweise für Anwendungsfälle priorisiert, die anfällig für Angriffe mit dem Ansatz „Harvest Now, Decrypt Later“ auf In-Flight-Daten oder Data-at-Rest-Verschlüsselung sein könnten.

Wenn Sie Ihre Technologieplattform in Betracht ziehen, kann die Umstellung eines kryptografischen Anwendungsfalls das vollständige Erneuern/Austauschen von Produkten oder ein Produktupgrade umfassen. Dies hängt vom fraglichen Produkt ab und davon, wo und wie die Kryptografie in diesem Produkt und den umgebenden Systemen implementiert wird.

Die Veröffentlichung quantenresistenter Angebote wird in etwa den nächsten 5 Jahren ein Schwerpunkt sein, um sicherzustellen, dass Kunden die PQC-Umstellungstermine einhalten können, die von Regierungsbehörden und Branchenverbänden veröffentlicht und zwischen 2027 und 2035 liegen werden.

Kunden sollten mit ihrem Dell Account-Team zusammenarbeiten, um produktspezifische Details (z. B. Roadmaps und Zeitrahmen für Veröffentlichungen) zu erhalten und sie in ihre Migrationspläne einzubinden. Bleiben Sie auf dem Laufenden, wenn Dell in den kommenden Monaten genauere Termine für die PQC-Integration in seine Produktlinien und Produkte bereitstellen wird.

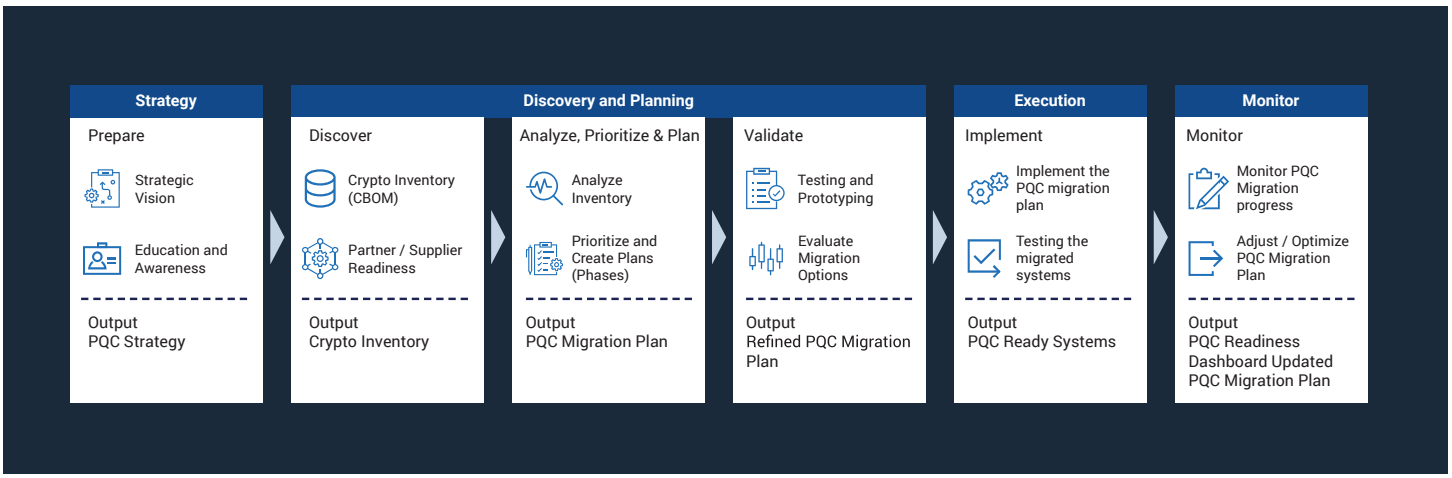
Vorbereitung auf quantenresiliente Innovationen

Dell möchte seine Kunden nicht nur bei der Einhaltung neuer Standards unterstützen, sondern ihnen auch helfen, Innovationen im Quantenzeitalter auf sichere Weise zu entwickeln. Ganz gleich, ob sie KI-Workloads bereitstellen, Hybrid-Cloud-Umgebungen managen oder die Edge-Infrastruktur modernisieren – Kunden können darauf vertrauen, dass die Lösungen von Dell auf Resilienz ausgelegt sind. Sicherheit wird nicht nachträglich aufgesetzt, sondern in jede Ebene des Dell Portfolios integriert, damit Unternehmen die Umstellung auf die Post-Quanten-Kryptografie souverän bewältigen können.

Vorbereitung auf die Umstellung

Die Umstellung auf die Post-Quanten-Kryptografie wird eine der bedeutendsten Infrastrukturänderungen seit Jahrzehnten sein. Diese Umstellung berührt nahezu alle Bereiche der IT, von Servern und Speichern über Endpunkte und Cloud-Plattformen bis hin zu Netzwerkprotokollen. Erfolg erfordert Voraussicht, Planung und disziplinierte Ausführung. Wir bei Dell Technologies sehen einen schrittweisen Weg in die Zukunft: einen Weg, der sofortige Sicherheitsverbesserungen mit langfristiger Bereitschaft für die PQC-Einführung in Einklang bringt.

Dell ist bereit, Sie bei Ihrer Strategie für die Implementierung von PQC zu unterstützen. Wir empfehlen einen schrittweisen Migrationsplan und haben eine Reihe von Aktivitäten erarbeitet, die Sie bei der Strategieerstellung, Planung, Ausführung und Überwachung Ihrer PQC-Migration unterstützen.



Vorbereitung des heutigen Sicherheitsstatus

Gute Sicherheitshygiene

Der erste Schritt zur Vorbereitung auf die Quantenzukunft besteht darin, die bereits vorhandenen Abwehrmaßnahmen zu verstärken. Unternehmen müssen strenge Best Practices für die Sicherheitshygiene nutzen, z. B. die Durchsetzung des Zugriffs mit geringsten Berechtigungen, die Implementierung einer Multi-Faktor-Authentifizierung und die Aufrechterhaltung eines strikten Patchmanagements. Zwei weitere Punkte sind zu bedenken. Es kann wichtig sein, schwächere Kryptografie zu deaktivieren, damit neue Systeme mit stärkerer Kryptografie mit Legacy-Systemen zusammenarbeiten können. Wichtig ist auch, dass die symmetrische Kryptografie für neuere Systeme auf längere Schlüssellängen – AES-256 und SHA-384 oder höher – aktualisiert wird, um die durch den Grover-Algorithmus eingeführten reduzierten Margen auszugleichen. Diese Maßnahmen verringern nicht nur das heutige Risiko, sondern minimieren auch den Rückstand kryptografischer Schulden, die andernfalls die Migration von morgen erschweren würden.

Bestandsaufnahme und Audit kryptografischer Ressourcen

Der Eckpfeiler jedes Migrationsplans ist die Transparenz. Unternehmen müssen eine umfassende kryptografische Bestandsaufnahme durchführen, um zu ermitteln, wo und wie Kryptografie mit öffentlichen Schlüsseln für Anwendungen, Geräte und Workflows verwendet wird. Dazu gehören TLS-Zertifikate, VPNs, E-Mail-Systeme, Codesignaturmechanismen und archivierte Daten. Nach der Identifizierung müssen Ressourcen basierend auf der geschäftlichen Bedeutung, Sensibilität und Lebensdauer priorisiert werden. Langlebige Daten wie Patientenakten oder klassifizierte Archive müssen mit höchster Dringlichkeit behandelt werden, da sie am anfälligsten für die „Harvest Now, Decrypt Later“-Bedrohung sind.

Pilotprojekt und Experimente mit PQC

Sobald ein Überblick über die kryptografische Landschaft geschaffen ist, sollten Unternehmen mit dem Testen von PQC-Lösungen in kontrollierten Umgebungen beginnen. Durch die Pilotphase dieser Lösungen in Laboren können IT-Teams Performance, Interoperabilität und Verwaltbarkeit vor einer umfassenden Bereitstellung validieren. Der Aufbau dieser Krypto-Agilität – die Möglichkeit, kryptografische Algorithmen zu wechseln, ohne ganze Systeme zu überholen – ist für langfristige Resilienz und eine einfache Migration von entscheidender Bedeutung.

Einführung eines Interoperabilitätsansatzes

Wenn Standards ausgereift sind, ebnet ein hybrides Modell den Weg in die Zukunft. Viele Anbieter unterstützen bereits hybride Verschlüsselungssuiten, die klassische und quantenresistente Algorithmen in einer einzigen Implementierung kombinieren. Diese duale Herangehensweise bietet eine Kontinuität des Schutzes, selbst wenn ein Algorithmus später kompromittiert wird. Unternehmen sollten jetzt mit der Einführung hybrider Strategien beginnen und gleichzeitig ihre internen Zeitpläne an den Produktroadmaps und -meilensteinen ihres Infrastrukturanbieters ausrichten. Dadurch wird sichergestellt, dass Unternehmen die Einführung unterbrechungsfrei skalieren können, wenn quantensichere Algorithmen standardisiert werden.

Vollständige Migration und kontinuierliche Validierung durchführen

Das ultimative Ziel ist eine vollständige Umstellung auf PQC im gesamten Unternehmen. Dies ist kein einmaliges Ereignis, sondern ein fortlaufender Validierungs- und Anpassungsprozess. Unternehmen sollten detaillierte Migrationspläne ausführen, mit denen PQC in jede Ebene ihres IT-Stacks integriert wird, und gleichzeitig kontinuierlich neue Standards und Implementierungen testen. Mithilfe von hybriden Quanten- und klassischen Labors können Kunden Angriffsszenarien simulieren, die kryptografische Integrität validieren und sicherstellen, dass ihre Systeme gegen sich entwickelnde Bedrohungen resilient bleiben.

Zusammenarbeit und Wissensaustausch

Schließlich sollte sich kein Unternehmen dieser Herausforderung allein stellen. Branchenkonsortien, akademische ForscherInnen und Regierungsbehörden bündeln Wissen, um die PQC-Umstellung zu beschleunigen. Durch die Teilnahme an Standardgruppen, Arbeitsgruppen und Pilotprogrammen können sich Unternehmen an Best Practices und neuen Anforderungen orientieren. Die aktive Beteiligung von Dell an Initiativen wie dem NIST NCCoE PQC-Projekt stellt sicher, dass unsere Kunden direkt von diesem kollektiven Fachwissen profitieren.

Die Vorbereitung auf PQC ist ein Marathon, kein Sprint. Durch einen schrittweisen Ansatz – eine Verstärkung der heutigen Abwehrmaßnahmen, Audits der kryptografischen Ressourcen, PQC-Pilotprojekte, die Einführung hybrider Strategien und die Durchführung einer vollständigen Migration – können Unternehmen souverän auf Quantenresilienz umsteigen. Mit Dell als Partner ist dieser Weg nicht nur gangbar, sondern auch eine Chance, das Vertrauen zu stärken und Innovationen weit in die Zukunft hinaus zu ermöglichen.

Reale Anwendungen und Vorteile

Bei der Umstellung auf Post-Quanten-Kryptografie geht es um mehr als nur um Compliance. Sie ist eine geschäftliche Notwendigkeit, die sich direkt auf Vertrauen, Resilienz und die langfristige Wettbewerbsfähigkeit auswirkt. Für Telekommunikationsanbieter, Finanzinstitute, Gesundheitseinrichtungen und Behörden sorgt die Einführung quantenresistenter Algorithmen dafür, dass kritische digitale Infrastruktur sowohl vor aktuellen als auch zukünftigen Bedrohungen geschützt bleibt.

Telekommunikation

Telekommunikationsnetzwerke sind das Rückgrat der globalen Digitalisierung. Sie ermöglichen alles von Notfalldiensten über IoT-Konnektivität bis hin zu sicherer Kundenkommunikation. Eine Quantensicherheitsverletzung in diesem Sektor könnte die SIM-Bereitstellung, das eSIM-Onboarding oder die Authentifizierungsprozesse beeinträchtigen, die 4G und 5G zugrunde liegen. Wenn Betreiber jetzt hybride und quantensichere Kryptografie bereitstellen, können sie das Vertrauen der Kunden wahren, Datenschutz sicherstellen und eine nahtlose Kontinuität des Service über Generationen mobiler Technologie hinweg gewährleisten.

Finanzdienstleister

Die Finanzbranche ist einer der am häufigsten von CyberangreiferInnen angegriffenen Sektoren, und die Integrität von Transaktionen hängt stark von der Kryptographie ab. Die Post-Quanten-Bereitschaft schützt digitale Zahlungen, Onlinebanking und Überweisungen zwischen Banken vor quantenbasiertem Betrug. Die frühzeitige Einführung überzeugt auch Regulierungsbehörden und Kunden davon, dass sich Institutionen für den Schutz von Ressourcen und die Aufrechterhaltung der systemischen Stabilität einsetzen. Eine zukunftssichere Kryptografie in diesem Sektor reduziert sowohl das Risiko der Verletzung behördlicher Auflagen als auch Reputationsrisiken.

Gesundheitswesen

Patientenakten, genetische Daten sowie vernetzte medizinische Geräte sind von Angriffen gefährdet, bei denen die Daten zunächst gesammelt und später entschlüsselt werden. Das Gesundheitswesen steht vor einer zusätzlichen Herausforderung: Die langen Aufbewahrungsfristen, die für sensible medizinische Daten erforderlich sind. Wenn sie heute mit der Umstellung auf PQC beginnen, stellen Krankenhäuser und Anbieter sicher, dass Gesundheitsdaten nicht nur jetzt, sondern auch in künftigen Jahrzehnten privat bleiben. Dies ist unerlässlich, um das Vertrauen der Patienten zu wahren und gleichzeitig die sich ändernden Datenschutzbestimmungen zu erfüllen.

Behörden und kritische Infrastruktur

Von der Verteidigungskommunikation bis hin zu Energieverteilungssystemen – Regierungen und Infrastrukturbetreiber verlassen sich auf Kryptografie für Kontinuität des Betriebs und nationale Sicherheit. Post-Quanten-Kryptografie schützt nicht nur vor zeitnahen Angriffen, sondern auch vor der strategischen Erfassung verschlüsselter Kommunikation für künftige Exploits. Die Ausrichtung an Frameworks wie CNSA 2.0 sorgt dafür, dass Regierungssysteme im Quantenzeitalter interoperabel, sicher und vertrauenswürdig bleiben.

Erweiterte geschäftliche Vorteile

Die technische Notwendigkeit von PQC ist klar, aber auch der Business Case überzeugt:

- Vertrauen und Markenimage: Übernahme einer Führungsrolle beim Schutz von Kunden- und Partnerdaten
- Compliance: Ausrichtung an NIST-Standards und behördlichen Auflagen wie CNSA 2.0
- Betriebliche Ausfallsicherheit: Reduziert das Risiko schwerwiegender Ausfälle, die durch entschlüsselte Kryptografie verursacht werden
- Wettbewerbsdifferenzierung: Positionierung von Unternehmen als proaktive Innovatoren statt als reaktive Mitläufer

Wer jetzt handelt, erzielt Vorteile, die weit über die technische Resilienz hinausgehen. Unternehmen, die PQC frühzeitig einführen, reduzieren nicht nur Risiken, sondern stärken auch ihre Fähigkeit, in einer auf Vertrauen angewiesenen digitalen Wirtschaft innovativ zu sein, für Compliance zu sorgen und wettbewerbsfähig zu bleiben.

Machen Sie die nächsten Schritte

Die Einführung von Quantencomputing stellt sowohl eine Generationschance als auch eine beispiellose Sicherheitsherausforderung dar. Der genaue Zeitrahmen für kryptografisch relevante Quantencomputer bleibt unsicher – sicher ist jedoch, dass die Vorbereitung mit viel Aufwand verbunden sein wird. Die Umstellung auf Post-Quanten-Kryptografie wird Jahre koordinierter Planung, Investitionen und Ausführung erfordern. Zu warten, bis Quantencomputer betriebsbereit sind, ist keine praktikable Option.

Der erste Schritt für jedes Unternehmen ist die Sensibilisierung: Sie müssen verstehen, wo und wie Kryptografie in ihrer Umgebung verwendet wird. Anschließend müssen Unternehmen mit der Inventarisierung, Priorisierung und Pilotierung quantensicherer Lösungen beginnen. Die hybride Kryptografie, die klassische und Post-Quanten-Algorithmen kombiniert, bietet einen unmittelbaren Weg zur Resilienz, während sich die Standards weiterentwickeln. Durch die Ausrichtung interner Roadmaps an globalen Frameworks wie den PQC-Standards von NIST und den Zeitrahmen von CNSA 2.0 können Unternehmen souverän auf Compliance und Interoperabilität umstellen.

Dell Technologies ist bestrebt, Kunden bei dieser Umstellung zu unterstützen. Unser Ansatz bietet eine Grundlage für die Integrität der Lieferkette, hardwareintegrierte Sicherheitsvorkehrungen und softwarebasierte Anpassungsfähigkeit. Unsere Partnerschaften mit führenden Sicherheitsanbietern und unsere aktive Rolle bei Branchenstandards sorgen dafür, dass Dell Lösungen nicht nur an den neuesten Anforderungen ausgerichtet sind, sondern auch auf reale Performance und Interoperabilität getestet werden.

Beginnen Sie noch heute mit der Vorbereitung. Beginnen Sie mit der Erkennung und Risikoanalyse, arbeiten Sie mit vertrauenswürdigen Anbietern zusammen und testen Sie quantensichere Technologien. Jeder Schritt, der jetzt unternommen wird, reduziert das Risiko von künftigen Unterbrechungen. Unternehmen, die frühzeitig handeln, sichern nicht nur ihre Daten und Systeme, sondern gewinnen auch das Vertrauen von Kunden, Regulierungsbehörden und Partnern in einem Zeitalter, in dem digitales Vertrauen oberstes Gebot ist.

Über uns

Dell Technologies setzt sich dafür ein, fortschrittliche Technologie bereitzustellen, die für alle zugänglich, vertrauenswürdig und befähigend ist. Wir helfen MitarbeiterInnen und Unternehmen, Innovationen sicher zu nutzen und den Weg in eine sicherere, integrativere und vernetzte Zukunft zu ebnen.