DELL Technologies

Post-Quanten-Kryptografie

Erste Schritte

Einführung

Quantencomputing treibt eine grundlegende Neugestaltung der Technologie voran und eröffnet sowohl enorme Chancen als auch neue Herausforderungen. So spannend diese Zukunft ist, sie bringt zugleich eine erhebliche Bedrohung für die kryptografischen Systeme mit sich, die unsere digitale Welt schützen.

Warum ist Quantencomputing auf dem Vormarsch?

Klassische Computer, ob in Laptops, Smartphones oder Servern, verarbeiten Informationen mithilfe von Bits, die sich in einem Zustand von Null oder eins befinden. 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.

Was ist Post-Quantenkryptografie?

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.

Welche unmittelbaren Risiken sind Unternehmen durch Quantencomputing ausgesetzt?

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 kryptografisch relevante Quantencomputer auf den Markt kommen, wird der Schaden bereits irreversibel sein.

„Harvest Now, Decrypt Later“: 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 verfügbar sind.

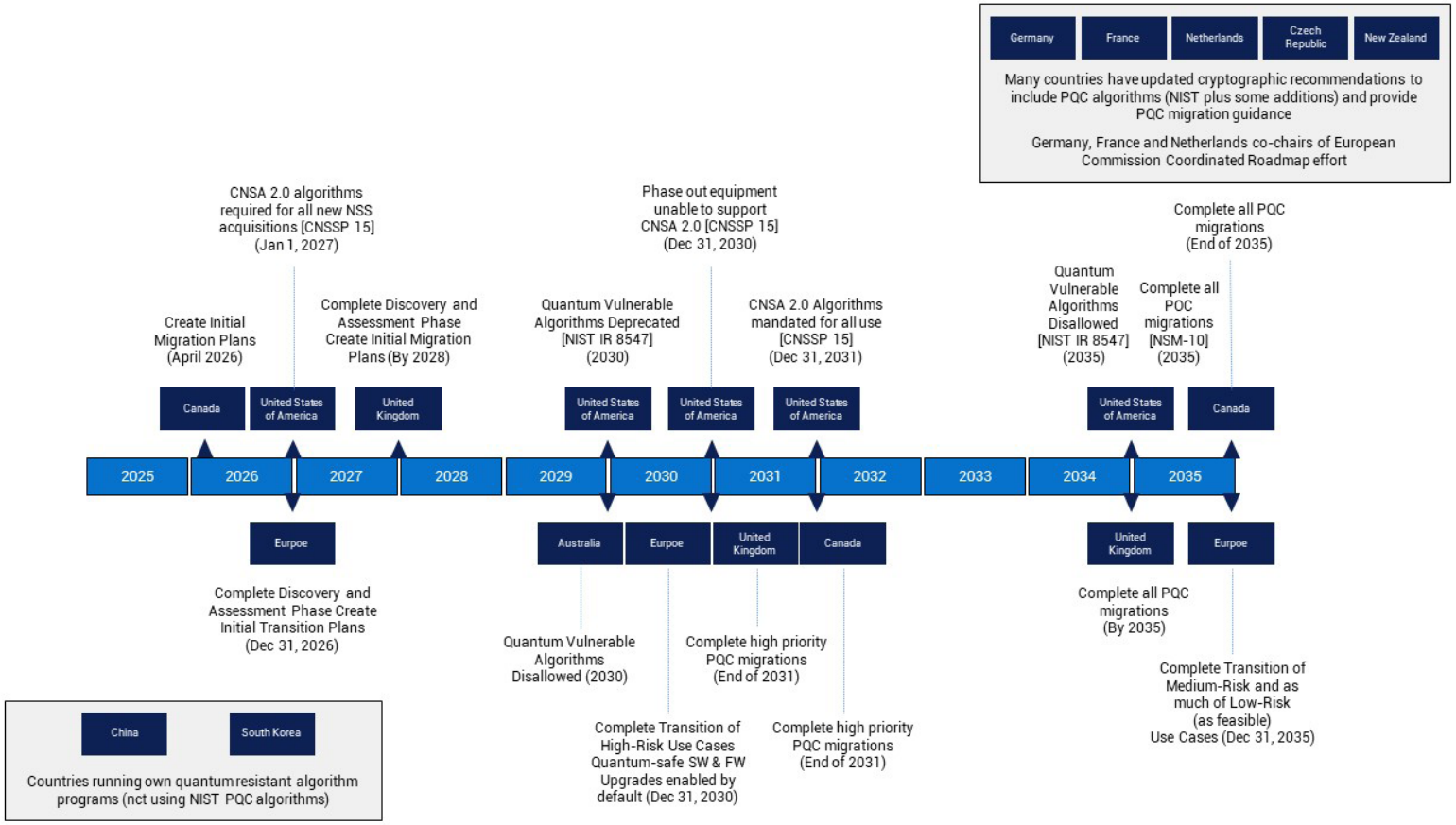
Wie sollten sich Unternehmen auf die Umstellung auf PQC vorbereiten?

Der Weg zu einer quantensicheren Zukunft ist ein Marathon, kein Sprint und ein Weg, der sich weiterentwickelt. Ein proaktiver, mehrschichtiger und stufenweiser Ansatz hilft Ihrem Unternehmen, Risiken zu managen, Ressourcen auszurichten und langfristig einen ausfallsicheren Sicherheitsstatus aufzubauen. Dell bietet die Technologien und Anleitungen, um Sie in jeder Phase zu unterstützen. Hier finden Sie die wichtigsten Schritte, die Ihr Unternehmen bei der Erstellung eines PQC-Übergangsplans unterstützen.

PQC-Übergangszeitplan

Angesichts der Dringlichkeit der Bedrohung haben Regierungen und Normungsgremien PQC zu einer globalen Priorität erklärt. Nachdem die US-Bundesregierung die Bedeutung der Einführung quantenresistenter Kryptografie-Algorithmen erkannte, hat sie begonnen, PQC-Anforderungen an Bundesbehörden zu stellen. Dazu gehören das National Security Memorandum 10 (NSM-10), die Commercial National Security Algorithm Suite (CNSA 2.0), das Office of Management and Budget Memorandum 23-02 (OMB M-2302) und der National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547) und weitere.

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



Bestandsaufnahme und Audit kryptografischer Ressourcen

Die erste Priorität besteht darin, Ihre aktuelle kryptografische Landschaft zu verstehen. Dieser grundlegende Schritt bildet die Grundlage für Ihre gesamte Migrationsstrategie.

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. Bei neueren Systemen ist es außerdem wichtig, die Mindestsicherheitsstärke zu erhöhen – AES-256 für symmetrische Kryptografie, SHA-384 oder höher für Digests –, 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, Kundendaten, archivierte Daten und weitere. 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

Mit einer klaren Bestandsaufnahme können Sie mit PQC-fähigen Technologien praxisnahe Experimente beginnen, um Performance und Integration zu validieren.

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 PQC-Standards ausgereift sind, können Sie mit der Planung für Produktions-Rollouts beginnen. Ein hybrider Ansatz bietet eine Brücke zu einer vollständig quantensicheren Umgebung.

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 ein vollständig integriertes und kontinuierlich validiertes Unternehmen, das auf Quantensicherheit basiert.

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 Labors aus Quanten- und klassischen Computern können Kunden Angriffsszenarien simulieren, die kryptografische Integrität validieren und sicherstellen, dass ihre Systeme gegen sich entwickelnde Bedrohungen resilient bleiben.

Zusammenarbeit und Wissensaustausch

Kein Unternehmen sollte sich dieser Herausforderung allein stellen müssen.

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.

Fazit

Das Quantenzeitalter ist keine weit entfernte Möglichkeit mehr. Es ist eine bevorstehende Realität, die heute vorausschauende Maßnahmen erfordert. Die Vorbereitung auf diesen technologischen Wandel ist eine strategische Notwendigkeit für den Schutz Ihrer wertvollsten Ressource – Ihrer Daten. Wie bereits beschrieben, ist ein stufenweiser Ansatz von der Bestandsaufnahme und dem Auditing bis zur vollständigen Migration der klarste Weg zu einer quantensicheren Zukunft.

Die Umstellung auf PQC 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.