DELL Technologies

Opracowanie techniczne

Kryptografia postkwantowa: Przygotowanie na erę kwantową

Opracowanie firmy Dell Technologies

Spis treści

przegląd dla kierownictwa 3

Terminologia 3

Obliczenia kwantowe i zagrożenie dla szyfrowania 4

Kryptografia postkwantowa i powstające standardy 4

Dlaczego czas na działanie jest teraz 7

O nas 11

Przegląd dla kierownictwa

Obliczenia kwantowe szybko przechodzą od badań teoretycznych do praktycznej rzeczywistości. Kiedyś uważano je za odległą perspektywę, ale postępy w sprzęcie, algorytmach i inwestycjach przyspieszają nadejście maszyn zdolnych do rozwiązywania problemów zbyt trudnych dla klasycznych komputerów. Konsekwencje dla branżyh są ogromne. Od odkrywania leków przez modelowanie klimatu po globalną logistykę — obliczenia kwantowe obiecują odblokowanie innowacji, które wcześniej były poza zasięgiem.

Jednak ten przełom wiąże się z poważnym wyzwaniem: komputery kwantowe osłabią fundamenty kryptograficzne, które chronią gospodarkę cyfrową. Kryptografia klucza publicznego — algorytmy takie jak RSA i kryptografia krzywych eliptycznych (ECC) — od dziesięcioleci chroni komunikację cyfrową, systemy finansowe, dane medyczne i bezpieczeństwo narodowe. Metody te opierają się na problemach matematycznych, które są zbyt trudne dla klasycznych komputerów. Jednak wraz z nadejściem kryptograficznie odpowiednich komputerów kwantowych (CRQC) te same problemy można skutecznie rozwiązywać, co czyni dzisiejsze zabezpieczenia przestarzałymi.

Nie jest to zagrożenie teoretyczne. Niektóre organizacje już stosują taktykę znaną jako „zbierz teraz, odszyfruj później" (HNDL) — zbierając zaszyfrowane dane teraz z nadzieją na ich złamanie, gdy komputery kwantowe osiągną dojrzałość. Informacje wrażliwe, które wydają się teraz bezpieczne, mogą być zagrożone w ciągu kilku lat. Czas na działanie to nie moment, gdy pojawią się komputery CRQC — to dziś.

Niniejsze opracowanie wyjaśnia pilność zagrożenia kwantowego, bada rozwijającą się dziedzinę kryptografii postkwantowej (PQC) i zawiera wskazówki, jak organizacje mogą się przygotować. Podkreśla zaangażowanie firmy Dell Technologies w budowanie przyszłości w zakresie bezpieczeństwa kwantowego — osadzania zabezpieczeń w naszym łańcuchu dostaw, sprzęcie, oprogramowaniu wewnętrznym, oprogramowaniu i ekosystemie partnerskim — poprzez dostosowanie się do standardów kryptografii postkwantowej (PQC) NIST (FIPS 203, FIPS 204 i FIPS 205) oraz wytycznych Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). Cel firmy Dell jest jasny: zadbajmy o to, aby innowacje mogły iść naprzód bez utraty bezpieczeństwa i zaufania.

Terminologia

W tym dokumencie znajdziesz kilka terminów. Próbowaliśmy przedstawić niektóre z tych terminów, aby pomóc w zrozumieniu dokumentu.

Kryptografia postkwantowa — nowe matematyczne podejście do kryptografii z nowymi algorytmami, które mają być bezpieczne przed atakami komputerów kwantowych. Algorytmy te działają na klasycznych komputerach i są odporne zarówno na ataki kwantowe, jak i na znane ataki kryptograficzne.

Odporność kwantowa — odporność kwantowa odnosi się do systemów, algorytmów lub infrastruktur, które zostały zaprojektowane tak, aby zachować bezpieczeństwo nawet w obecności kryptograficznie odpowiednich komputerów kwantowych (CRQC). System odporny kwantowo wykorzystuje kryptografię postkwantową (PQC) lub inne zabezpieczenia, które wytrzymują zarówno ataki klasyczne, jak i kwantowe, zapewniając poufność, integralność i autentyczność danych w przyszłości. Inne terminy, takie jak odporność kwantowa i bezpieczeństwo kwantowe, są również używane zamiennie.

Zdolność kryptograficzna — (czasami nazywana zwinnością kryptograficzną) to zdolność systemów i aplikacji organizacji do szybkiej i bezproblemowej zamiany algorytmów kryptograficznych, protokołów lub długości kluczy bez konieczności poważnych przeróbek czy zakłóceń operacyjnych.

„Zbierz teraz, odszyfruj później" („Harvest Now, Decrypt Later", HNDL) lub „Zapisz teraz, odszyfruj później" („Record Now, Decrypt Later") to praktyka polegająca na gromadzeniu i przechowywaniu zaszyfrowanych danych przez przeciwników z zamiarem ich odszyfrowania w przyszłości, gdy dostępne będą kryptograficznie istotne komputery kwantowe (CRQC).

Obliczenia kwantowe i zagrożenie dla szyfrowania

Rozwój obliczeń kwantowych

Jak opisaliśmy w naszym wpisie na blogu, Kryptografia postkwantowa: strategiczny imperatyw dla odporności przedsiębiorstw, opublikowanym niemal rok temu przez naszego dyrektora technicznego, Johna Roese'a, klasyczne komputery — niezależnie czy to notebooki, smartfony, czy serwery — przetwarzają informacje za pomocą bitów, które przyjmują wartość zero lub jeden. Ten model binarny przez dziesięciolecia stymulował postęp, ale ogranicza on sposób, w jaki informacje mogą być odzwierciedlane i obrabiane. Komputery kwantowe wykorzystują kubity, które mogą istnieć w wielu stanach jednocześnie poprzez zasady takie jak superpozycja i splątanie. Dzięki temu komputery kwantowe mogą równolegle badać ogromną liczbę możliwych rozwiązań, zapewniając przewagę obliczeniową w przypadku określonych rodzajów problemów.

Potencjalne zastosowania obliczeń kwantowych są niezwykłe. Naukowcy przewidują przełomowe dokonania w farmaceutykach, symulując precyzyjne interakcje molekularne, jakich nie mogą przeprowadzić klasyczne komputery. Naukowcy zajmujący się klimatem przewidują dokładniejsze modele systemów globalnych, podczas gdy sektor energetyczny dostrzega potencjał optymalizacji sieci elektroenergetycznych i magazynowania. Nawet logistyka i produkcja mogą skorzystać na technikach optymalizacji kwantowej. Korzyści są realne i w zasięgu ręki, podobnie jak zagrożenia.

Dlaczego szyfrowanie jest zagrożone

Szyfrowanie wzmacnia zaufanie w erze cyfrowej. Po wprowadzeniu numeru karty kredytowej, zalogowaniu się do bezpiecznej witryny internetowej albo otrzymaniu podpisanej aktualizacji oprogramowania kryptografia zapewnia poufność, autentyczność i integralność. Większość tej ochrony opiera się na kryptografii klucza publicznego — algorytmach takich jak RSA i ECC, które wykorzystują problemy matematyczne uważanych za niemożliwe do obliczenia dla klasycznych maszyn.

Obliczenia kwantowe zmieniają to równanie. Korzystając z **algorytmu Shora**, wystarczająco wydajny komputer kwantowy może rozwiązać problemy z faktoryzacją i logarytmem dyskretnym, które nadają RSA i ECC ich siłę. Gdy komputery CRQC zaistnieją, podpisy cyfrowe, które chronią aktualizacje oprogramowania, klucze, które ustanawiają sesje TLS i certyfikaty uwierzytelniające urządzenia, mogą zostać złamane. Wpływ ma charakter systemowy, zagrażający samym mechanizmom, które sprawiają, że transakcje cyfrowe są bezpieczne.

Kryptografia symetryczna — algorytmy takie jak AES używane do ochrony przechowywanych danych lub zabezpieczenia komunikacji — stoi przed innym, choć mniej poważnym wyzwaniem. **Algorytm Grovera** pozwala komputerowi kwantowemu zmniejszyć efektywną siłę symetrycznych kluczy, skutecznie zmniejszając o połowę ich bezpieczeństwo. Chociaż można ten efekt złagodzić, przechodząc na większe rozmiary kluczy, takie jak AES-256, regulacja podkreśla wszechobecny zasięg zagrożeń kwantowych

Pilność i konsekwencje

Konsekwencje wykraczają daleko poza teoretyczne ryzyko. Organizacje, które się nie przygotują, narażają na niebezpieczeństwo wrażliwe składniki własności intelektualnej oraz bezpieczeństwo narodowe, a także wystawiają się na ryzyko zakłóceń w systemach finansowych i naruszeń danych zdrowotnych. Strategia „Zbierz teraz, odszyfruj później" potęguje pilność: przeciwnicy muszą już dziś przechwycić zaszyfrowane dane i poczekać na środki do ich odszyfrowania. Do czasu nadejścia komputerów CRQC szkoda będzie już nieodwracalna.

Kryptografia postkwantowa i wschodzące standardy

Definiowanie kryptografii postkwantowej

Kryptografia postkwantowa (Post-Quantum Cryptography, PQC) odnosi się do nowej generacji algorytmów zaprojektowanych w celu zabezpieczenia systemów cyfrowych przed atakami klasycznymi i kwantowymi. W przeciwieństwie do dystrybucji kluczy kwantowych, która wymaga specjalistycznego sprzętu, kryptografia postkwantowa jest przeznaczona do pracy na współczesnej klasycznej infrastrukturze — serwerach, punktach końcowych, sieciach — dzięki czemu jest to najbardziej praktyczny i skalowalny sposób przygotowania się do ery kwantowej.

Podstawą PQC jest zestaw problemów matematycznych, które — zgodnie z najlepszą aktualną wiedzą — są odporne na techniki kwantowe, takie jak algorytmy Shora i Grovera. Kryptografia oparta na kratach, podpisy hashujące, schematy kodowe oraz równania wielowymiarowe to najbardziej obiecujące grupy rozwiązań. Podejścia te są starannie testowane i standaryzowane, aby zapewnić taką samą niezawodność i interoperacyjność jak niegdyś RSA i ECC.

Globalny wysiłek standaryzacji — wschodzące standardy branżowe

Uznając pilność tego zagrożenia, rządy i organy standaryzacyjne uznały PQC za globalny priorytet. Amerykański National Institute of Standards and Technology (NIST) uruchomił projekt PQC w 2016 roku, wzywając kryptograficzną społeczność badawczą do proponowania, analizowania i udoskonalania kandydujących algorytmów. Po latach testów NIST ogłosił pierwszą grupę zestandaryzowanych algorytmów w sierpniu 2024 roku:

- **CRYSTALS** —Kyber do szyfrowania z kluczem publicznym i ustalania klucza
- **CRYSTALS**-Dilithium i SPHINCS+ do podpisów cyfrowych

Dodatkowe algorytmy są nadal analizowane, aby zapewnić różnorodność i elastyczność dla różnych potrzeb wdrożeniowych, w tym dla systemów lekkich, takich jak oprogramowanie wewnętrzne. Ten ewoluujący proces standaryzacji zapewnia organizacjom na całym świecie wyraźną ścieżkę do przyjęcia rozwiązań odpornych na kwanty.

Standardy NIST — FIPS 203, 204, 205

W sierpniu 2024 roku amerykański National Institute of Standards and Technology (NIST) sfinalizował pierwsze algorytmy PQC:

- FIPS 203 (ML-KEM) — oparty na mechanizmie enkapsulacji kluczy CRYSTALS-Kyber. Zapewnia bezpieczeństwo IND-CCA2, co oznacza, że zaszyfrowane teksty pozostają nierozróżnialne nawet w przypadku ataków adaptacyjnych z wybranym tekstem zaszyfrowanym.
- FIPS 204 (ML-DSA) — oparty na algorytmie podpisu cyfrowego CRYSTALS-Dililithium. Zapewnia wysoki poziom bezpieczeństwa EUF-CMA (egzystencjalna niepodrabialność przy atakach z wybranym komunikatem), co stanowi standardowy wymóg dla podpisów cyfrowych.
- FIPS 205 (SLH-DSA) — oparty na SPHINCS+, schemacie podpisu opartego na haszowaniu. Wybrany jako ostrożna alternatywa, niezależna od problemów kratowych.

Obowiązkowy plan działania

Zdając sobie sprawę ze znaczenia przyjęcia algorytmów szyfrowania odpornego na kwanty, rząd federalny USA zaczął wydawać wymogi PQC agencjom federalnym. Należą do nich National Security Memoranum 10 (NSM-10), Commercial National Security Algorithm Suite (CNSA 2.0), The National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547 oraz Office of Management and Budget Memoranment 23-02 (OMB M-2302), ale nie tylko.

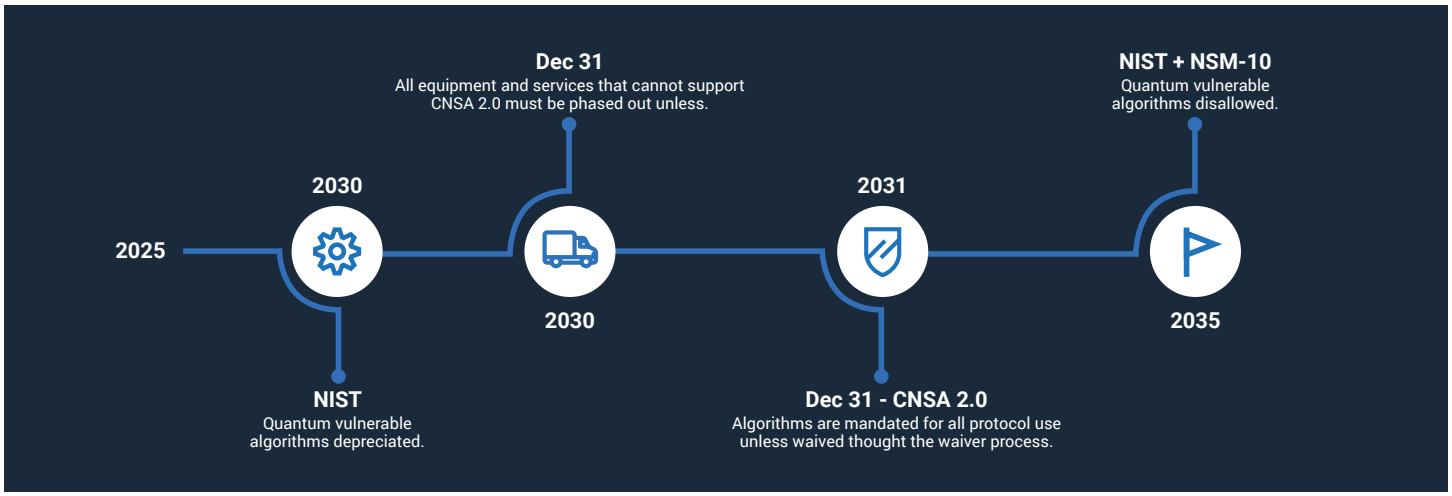
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

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

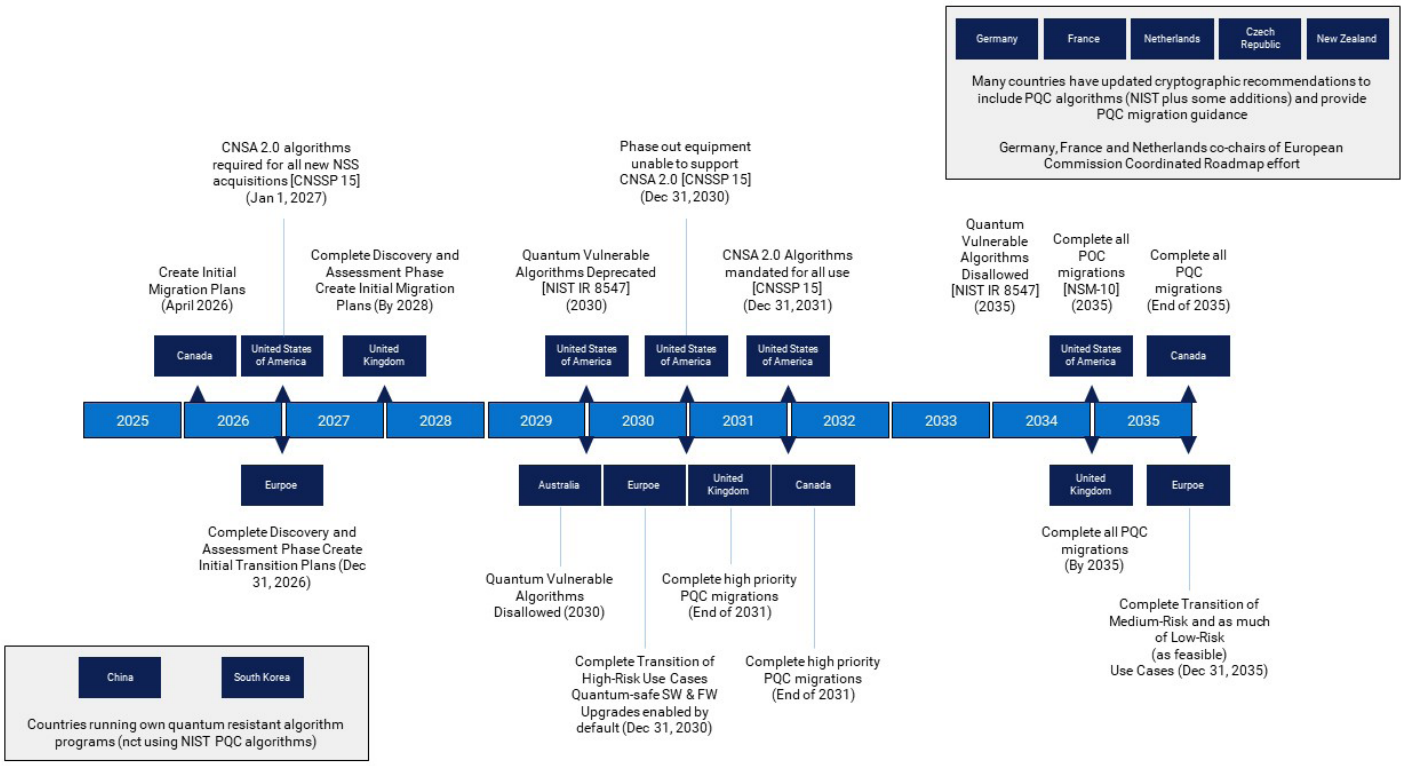
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

Wymóg CNSA 2.0, ogłoszony przez NSA we wrześniu 2022 roku, zawiera pierwsze rekomendacje dotyczące algorytmów kryptograficznych odpornych na ataki kwantowe. CNSA 2.0 określa wyraźne terminy wdrażania algorytmów odpornych na kwanty w krajowych systemach bezpieczeństwa (NSS) i służy jako potężny przewodnik dla przedsiębiorstw przygotowujących własne zmiany:



Inne organizacje na całym świecie również ustaliły wytyczne dotyczące przejścia na PQC. Poniżej przedstawiono wybrane regulacje obowiązujące w różnych krajach.



Daty te nie są arbitralne — odzwierciedlają terminy realizacji potrzebne do przeprojektowania, zweryfikowania i wdrożenia kryptografii w złożonych ekosystemach IT. Przedsiębiorstwa powinny postrzegać je jako coś więcej niż nakazy rządowe; są to praktyczne wskaźniki globalnego przejścia na odporność kwantową.

Współpraca branżowa

Oprócz NIST i NSA również firma Dell aktywnie uczestniczy w konsorcjach branżowych i grupach standaryzacyjnych, które promują interoperacyjność i wdrażanie. Trusted Computing Group integruje PQC ze standardem TPM (Trusted Platform Module). IETF aktywnie wspiera wdrażanie algorytmów kryptografii postkwantowej (PQC) do protokołów branżowych, takich jak TLS czy certyfikaty X.509. Komitety OASIS ds. protokołu KMIP (Key Management Interoperability Protocol) umożliwiają integrację kryptografii postkwantowej z infrastrukturami zarządzania kluczami. FIDO Alliance bada wpływ PQC na standardy uwierzytelniania i wdrażania urządzeń, podczas gdy organizacje takie jak SAFECode pracują nad edukowaniem branży w zakresie gotowości do migracji.

National Cyber Security Center of Excellence (NCCoE) NIST to ośrodek, który umożliwia instytutowi NIST współpracę z przemysłem, środowiskiem akademickim i agencjami rządowymi przy projektach ukierunkowanych na domenę. Skupiają się na wielu rzeczach, takich jak:

- Odkrywanie kryptografii — określenie, które mechanizmy kryptograficzne wymagają migracji i jak ustalić priorytety migracji.
- Interoperacyjność — zapewnienie, że popularne funkcje i protokoły kryptograficzne są wyposażone w nowe algorytmy PQC i że wdrożenia od różnych dostawców współdziałają.
- Zwinność kryptograficzna — koncentracja na tworzeniu systemów informatycznych, które umożliwiają szybkie dostosowywanie nowych podstawowych elementów kryptograficznych i algorytmów bez znacznych zmian w infrastrukturze systemu, co jest nazywane zwinnością kryptograficzną.

Projekty te pomagają w informowaniu/[opracowywaniu wytycznych i standardów, które tworzą, oraz udostępniają przykładowe rozwiązania branżowe zgodne z tymi wytycznymi i standardami. Firma Dell bierze udział w projekcie NCCoE Migration to PQC od samego początku.

Obecnie PQC to nie tylko temat badawczy; jest to rozwijający się standard z konkretnymi algorytmami, harmonogramami i ścieżkami wdrażania. Organizacje, które rozpoczną przygotowania już teraz, mogą uniknąć kosztów, zakłóceń i ryzyka związanego z przygotowaniami w ostatniej chwili. Transformacja nie polega wyłącznie na zgodności z przepisami — chodzi o zapewnienie, że zaufanie, poufność i integralność pozostaną nienaruszone, ponieważ obliczenia kwantowe zmieniają krajobraz cyfrowy.

Dlaczego czas na działanie jest teraz

Bezpośredni charakter zagrożenia

Może być kuszące postrzeganie obliczeń kwantowych jako odległego ryzyka, którym można się zająć dopiero po pełnym wprowadzeniu technologii. W rzeczywistości zegar już zaczął odliczanie. Poufne informacje — transakcje finansowe, dokumentacja opieki zdrowotnej, własność intelektualna lub komunikacja rządowa — mogą być dziś bezpiecznie szyfrowane, ale gdy komputery kwantowe osiągną próg łamania RSA lub ECC, dane te mogą zostać odszyfrowane wstecznie. W rezultacie cały zbiór historycznych komunikatów i dokumentów może być nagle zagrożony.

Długie cykle technologiczne

Transformacja nowoczesnych ekosystemów IT nie jest łatwa ani szybka. W przeszłości wymiana pojedynczego algorytmu, na przykład przejście z SHA-1 na o SHA-2 lub z DES/3DES na AES, trwała ponad 10 lat. Algorytmy te są głęboko osadzone w systemach operacyjnych, aplikacjach, urządzeniach sieciowych i sprzęcie. Zastąpienie ich wymaga przeprojektowania, walidacji, testowania i wdrożenia w środowiskach, które obejmują centra danych, platformy chmurowe i urządzenia brzegowe. Wiele organizacji będzie potrzebowało wielu lat, aby się przygotować — znacznie więcej, niż pozostało czasu, zanim obliczenia kwantowe staną się realnym zagrożeniem. Dlatego organy regulacyjne, organy standaryzacyjne i liderzy ds. bezpieczeństwa kładą nacisk na natychmiastowe przygotowanie. Oczekiwanie na powszechną dostępność komputerów CRQC nie pozostawi czasu na uporządkowane przejście.

Ryzyko bezczynności

Konsekwencje opóźnienia migracji wykraczają poza narażenie techniczne:

- Ryzyko związane z bezpieczeństwem danych: dane o długim czasie eksploatacji, takie jak historie medyczne, dokumentacja finansowa lub informacje obronne, mogą zostać naruszone wstecznie, gdy komputery kwantowe osiągną odpowiedni poziom rozwoju.
- Ryzyko dla autentyczności i integralności oprogramowania: autentyczność i integralność oprogramowania mogą zostać naruszone przez złośliwy kod, jeśli podpisano je obecnymi metodami i nadal będzie używane po osiągnięciu dojrzałości przez komputery kwantowe.
- Ryzyko operacyjne: Systemy infrastruktury o znaczeniu krytycznym — takie jak media, sieci transportowe i usługi ratunkowe — są niezwykle trudne do unowocześnienia. Niedostateczne planowanie teraz może prowadzić do zakłóceń w działaniach operacyjnych w przyszłości.
- Ryzyko związane z przepisami i zgodnością: ramy, takie jak **CNSA 2.0**, określiły jasne terminy wdrożenia zgodności. Organizacje, które się nie przygotują, ryzykują nie tylko narażenie na zagrożenia, ale także brak zgodności z oczekiwaniami państwowymi lub branżowymi.
- Ryzyko reputacyjne i finansowe: Naruszenie wynikające z nieusuniętych luk w zabezpieczeniach kryptograficznych może prowadzić do trwałych szkód w zaufaniu do marki obok znacznych strat finansowych.

Argumenty za proaktywnym działaniem

Proaktywne przygotowanie to nie tylko ruch defensywny — to okazja do wzmocnienia długoterminowej odporności. Przeprowadzając inwentaryzacje kryptografii, uaktualniając długości kluczy symetrycznych, pilotując rozwiązania zgodne z PQC i angażując dostawców, którzy oferują oferty odporności kwantowej, organizacje mogą zapewnić ciągłość zaufania. Organizacje, które wcześnie wdrażają nowe rozwiązania, są lepiej przygotowane do zabezpieczenia swoich operacji na przyszłość, utrzymania zgodności z regulacjami oraz wykazania się przywództwem wobec klientów, partnerów i regulatorów.

Podejście firmy Dell do kryptografii postkwantowej

W firmie Dell wierzymy, że technologia stymuluje postęp ludzkości, a bezpieczeństwo jest podstawą tego postępu. Firma Dell Technologies dba o to, aby jej oferta, infrastruktura IT i systemy wsparcia cyklu eksploatacji były dobrze przygotowane do przejścia na algorytmy odporności kwantowej. Kroki podejmowane w celu przygotowania się do zmiany są następujące:

- Identyfikacja konkretnych obszarów i celów, w których kryptografia jest stosowana w produktach, usługach, infrastrukturze IT i systemach wsparcia w celu sformułowania kompleksowych planów zmiany.
- Poszerzenie wewnętrznej wiedzy na temat algorytmów kryptografii postkwantowej (Post Quantum Cryptography, PQC), uwzględnienie aspektów wdrożenia i zasad projektowania związanych ze zwinnością kryptograficzną w celu ułatwienia płynnego przejścia na algorytmy PQC.
- Ocena wydajności, przydatności i adekwatności algorytmów PQC w różnych zastosowaniach istotnych dla zróżnicowanej oferty Dell Technologies.

Ze względu na złożony charakter przejścia na PQC uaktualnienia zastosowań kryptograficznych mogą być stopniowo wprowadzane do oferty Dell Technologies. Na przykład, z perspektywy danych, priorytet przejścia jest przyznawany przypadkom użycia, które mogą być podatne na ataki typu „Zbierz teraz, odszyfruj później", takie jak szyfrowanie danych w ruchu lub w spoczynku.

Uwzględniając platformę technologiczną, zmiana kryptograficznego przypadku użycia może wymagać pełnego odświeżenia/wymiany produktu lub unowocześnienia produktu. Będzie to zależeć od danego produktu oraz miejsca i sposobu wdrożenia kryptografii w tym produkcie i otaczających go systemach.

W ciągu najbliższych 5+ lat priorytetem będzie wdrażanie rozwiązań odpornych na komputery kwantowe, aby klienci mogli dostosować się do harmonogramów przejścia na PQC, publikowanych przez rządy i organizacje branżowe na lata 2027–2035.

Klienci powinni współpracować z działem obsługi klienta firmy Dell w celu uzyskania szczegółowych informacji dotyczących konkretnych produktów (np. planów wydań i harmonogramów) w celu uwzględnienia ich w planach migracji. Bądź na bieżąco, ponieważ w nadchodzących miesiącach firma Dell będzie informować o bardziej szczegółowych terminach integracji PQC z liniami produktowymi i produktami.

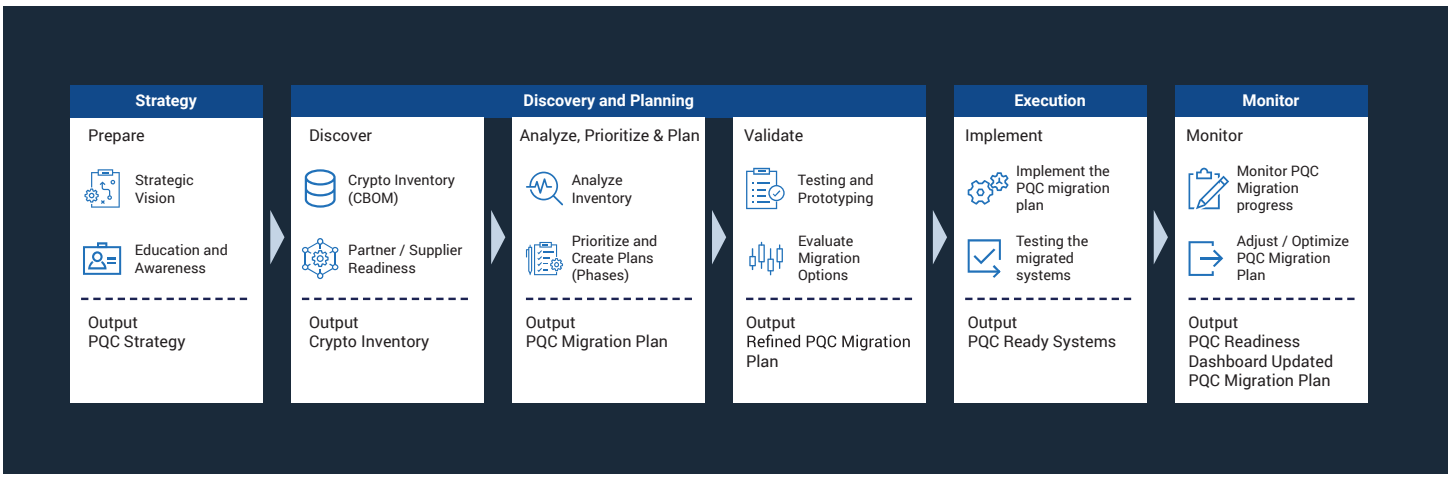
Przygotowanie do innowacji odpornych na kwanty

Celem firmy Dell jest nie tylko pomaganie klientom w stosowaniu się do wschodzących standardów, ale także umożliwienie im bezpiecznego wprowadzania innowacji w erze kwantowej. Niezależnie od tego, czy wdrażasz obciążenia robocze związane ze sztuczną inteligencją, zarządzasz środowiskami chmury hybrydowej, czy modernizujesz infrastrukturę brzegową, klienci mogą mieć pewność, że rozwiązania firmy Dell są zaprojektowane z myślą o odporności. Bezpieczeństwo nie jest budowane po fakcie — jest ono projektowane w każdej warstwie portfolio firmy Dell, dzięki czemu organizacje mogą bez obaw przejść na kryptografię postkwantową.

Przygotowanie do zmiany

Przejście na kryptografię postkwantową będzie jedną z najważniejszych zmian w infrastrukturze od dziesięcioleci. Ta zmiana dotyczy niemal każdego aspektu IT, od serwerów i pamięci masowej po punkty końcowe, platformy chmurowe i protokoły sieciowe. Sukces wymaga przewidywania, planowania i zdyscyplinowanej realizacji. W firmie Dell Technologies widzimy, że droga składa się z etapów i równoważy natychmiastowe udoskonalenia zabezpieczeń z długoterminową gotowością do wdrożenia PQC.

Firma Dell jest gotowa pomóc w realizacji strategii wdrożenia PQC. Rekomendujemy plan stopniowej migracji i przedstawiliśmy zestaw działań, które pomogą Ci w strategii, planowaniu, realizacji i monitorowaniu migracji PQC.



Przygotowanie obecnego stanu bezpieczeństwa

Dobra higiena bezpieczeństwa

Pierwszym krokiem w przygotowaniu się na kwantową przyszłość jest wzmocnienie już istniejących zabezpieczeń. Organizacje powinny stosować najlepsze praktyki w zakresie higieny bezpieczeństwa, takie jak egzekwowanie zasady najmniejszych uprawnień, wdrażanie uwierzytelniania wieloskładnikowego i utrzymywanie rygorystycznego zarządzania poprawkami. Istnieją również dwie inne kwestie. Ważne może być wyłączenie słabszej kryptografii, tak aby nowe systemy z wyższą kryptografią mogły współdziałać ze starszymi systemami. Ważne jest również, aby kryptografia symetryczna, w przypadku nowszych systemów, została uaktualniona pod kątem dłuższych kluczy — AES-256 i SHA-384 lub nowszych — w celu przeciwdziałania zmniejszonym marginesom bezpieczeństwa wprowadzonym przez algorytm Grovera. Środki te nie tylko zmniejszają ryzyko dzisiaj, ale także minimalizują dług kryptograficzny, który inaczej utrudniłby przyszłą migrację.

Inwentaryzacja i audyt zasobów kryptograficznych

Podstawą każdego planu migracji jest widoczność. Organizacje muszą przeprowadzić kompleksową inwentaryzację kryptograficzną, określającą, gdzie i w jaki sposób kryptografia klucza publicznego jest używana w aplikacjach, urządzeniach i przepływach pracy. Obejmuje to certyfikaty TLS, VPN, systemy poczty e-mail, mechanizmy podpisywania kodu i zarchiwizowane dane. Po zidentyfikowaniu zasoby powinny być traktowane priorytetowo na podstawie krytyczności dla działalności biznesowej, wrażliwości i cyklu życia. Dane o długim okresie przechowywania — takie jak dokumentacja medyczna lub tajne archiwa — powinny być traktowane z najwyższą pilnością, ponieważ są najbardziej narażone na zagrożenie typu „Zbierz teraz, odszyfruj później”.

Pilotuj i eksperymentuj z PQC

Po zorientowaniu się w krajobrazie kryptograficznym organizacje powinny rozpocząć testowanie rozwiązań PQC w środowiskach kontrolowanych. Pilotując te rozwiązania w laboratoriach, zespoły IT mogą weryfikować wydajność, interoperacyjność i łatwość zarządzania przed wdrożeniem na szeroką skalę. Budowanie takiej zwinności kryptograficznej — zdolności do przełączania algorytmów kryptograficznych bez konieczności przeprowadzania przeglądu całych systemów — ma kluczowe znaczenie dla długoterminowej odporności i łatwości migracji.

Przyjęcie podejścia interoperacyjnego

W miarę dojrzewania standardów model hybrydowy tworzy pomost ku przyszłości. Wielu dostawców już obsługuje hybrydowe zestawy szyfrów, które łączą algorytmy klasyczne i odporne na kwanty w jednej implementacji. Takie podwójne podejście zapewnia ciągłość ochrony nawet w przypadku późniejszego naruszenia jednego algorytmu. Przedsiębiorstwa powinny już teraz zacząć wdrażać strategie hybrydowe, dostosowując swoje wewnętrzne harmonogramy czasowe do planów i kamieni milowych dostawców infrastruktury. Dzięki temu, gdy algorytmy bezpieczne kwantowo osiągną standaryzację, organizacje mogą skalować wdrażanie bez zakłóceń.

Wykonuj pełną migrację i ciągłą weryfikację

Ostatecznym celem jest całkowite przejście na PQC w całym przedsiębiorstwie. Nie będzie to jednorazowe zdarzenie, ale ciągły proces weryfikacji i adaptacji. Organizacje powinny realizować szczegółowe plany migracji, włączając PQC do każdej warstwy swojego stosu IT, jednocześnie stale testując nowe standardy i wdrożenia. Korzystając z hybrydowych laboratoriów kwantowo-klasycznych, klienci mogą symulować scenariusze ataków, weryfikować integralność kryptograficzną i zapewnić odporność systemów na zmieniające się zagrożenia.

Współpraca i wymiana wiedzy

Wreszcie żadna organizacja nie powinna stawiać czoła temu wyzwaniu w pojedynkę. Konsorcja branżowe, akademicy i agencje rządowe łączą wiedzę, aby przyspieszyć transformację PQC. Uczestnictwo w grupach standaryzacji, grupach roboczych i programach pilotażowych umożliwia przedsiębiorstwom utrzymywanie zgodności z najlepszymi praktykami i wschodzącymi wymaganiami. Aktywne zaangażowanie firmy Dell w inicjatywy takie jak NIST NCCoE PQC zapewnia naszym klientom bezpośrednie korzyści z tej zbiorowej wiedzy eksperckiej.

Przygotowanie do PQC to maraton, a nie sprint. Dzięki stopniowemu podejściu — wzmacnianiu dzisiejszych zabezpieczeń, audytowi zasobów kryptograficznych, pilotażowi PQC, przyjęciu strategii hybrydowych i pełnej migracji — organizacje mogą pewnie zmierzać ku odporności kwantowej. Dzięki firmie Dell jako partnerowi ten proces jest nie tylko realistyczny, ale także stanowi okazję do wzmocnienia zaufania i umożliwienia innowacji w przyszłości.

Zastosowania i korzyści w praktyce

Przejście na kryptografię postkwantową to coś więcej niż tylko ćwiczenie dotyczące zgodności z przepisami — jest to imperatyw biznesowy, który bezpośrednio wpływa na zaufanie, odporność i długoterminową konkurencyjność. W przypadku dostawców usług telekomunikacyjnych, instytucji finansowych, organizacji opieki zdrowotnej i agencji rządowych przyjęcie algorytmów odpornych na kwanty zapewnia bezpieczeństwo krytycznej infrastruktury cyfrowej zarówno przed obecnymi, jak i przyszłymi zagrożeniami.

Telekomunikacja

Sieci telekomunikacyjne są podstawą globalnej digitalizacji. Umożliwiają wszystko — od akcji ratunkowych i łączności IoT po bezpieczną komunikację z klientami. Naruszenie kwantowe w tym sektorze może zagrozić przydzieleniu karty SIM, wdrożeniu karty eSIM lub procesom uwierzytelniania, które są podstawą sieci 4G i 5G. Dzięki wdrożeniu hybrydowej i bezpiecznej kryptografii kwantowej operatorzy mogą utrzymać zaufanie klientów, ochronić prywatność danych i zapewnić bezproblemową ciągłość usług w generacjach technologii mobilnych.

Usługi finansowe

Branża finansowa jest jedną z najbardziej atakowanych przez cyberprzestępców, a integralność transakcji zależy od kryptografii. Gotowość na erę postkwantową chroni płatności cyfrowe, bankowość internetową i transfery międzybankowe przed oszustwami wykorzystującymi komputery kwantowe. Wczesne wdrożenie gwarantuje również organom regulacyjnym i klientom, że instytucje są zaangażowane w ochronę aktywów i utrzymanie stabilności systemowej. Przyszłościowa kryptografia w tym sektorze ogranicza ryzyko regulacyjne oraz ryzyko utraty reputacji.

Opieka zdrowotna

Dane pacjentów, dane genomowe i podłączone urządzenia medyczne są zagrożone atakami typu „Zbierz teraz, odszyfruj później”. Sektor opieki zdrowotnej stoi przed dodatkowym wyzwaniem: długimi okresami przechowywania danych wymaganych w przypadku wrażliwych danych medycznych. Rozpoczynając dziś przejście na PQC, szpitale i usługodawcy gwarantują, że dane medyczne pozostaną prywatne nie tylko teraz, ale także w ciągu najbliższych dziesięcioleci. Ma to kluczowe znaczenie dla zachowania zaufania pacjentów przy jednoczesnym spełnieniu zmieniających się przepisów dotyczących ochrony danych.

Administracja publiczna i infrastruktura krytyczna

Od komunikacji obronnej po systemy dystrybucji energii organy władzy i operatorzy infrastruktury polegają na kryptografii w celu zapewnienia ciągłości działania i bezpieczeństwa narodowego. Kryptografia postkwantowa chroni nie tylko przed dzisiejszymi przeciwnikami, ale także przed strategicznym przechwytywaniem zaszyfrowanych informacji z myślą o ich wykorzystaniu w przyszłości. Dostosowanie do struktur takich jak CNSA 2.0 daje pewność, że systemy publiczne pozostają interoperacyjne, bezpieczne i zaufane w erze kwantowej.

Większe korzyści biznesowe

Chociaż techniczna konieczność PQC jest oczywista, uzasadnienie biznesowe jest równie silne:

- Zaufanie i reputacja marki: Wykazuje czołową pozycję w zakresie ochrony danych klientów i partnerów.
- Zgodność z przepisami: Zgodność ze standardami NIST i wymogami rządowymi, takimi jak CNSA 2.0.
- Odporność operacyjna: Zmniejsza ryzyko katastrofalnych awarii spowodowanych uszkodzoną kryptografią.
- Zróżnicowanie konkurencyjne: Pozycjonuje organizacje jako proaktywnych innowatorów, a nie reaktywnych naśladowców.

Korzyści płynące z działania wykraczają teraz znacznie poza odporność techniczną. Organizacje, które wdrożą PQC wcześnie, nie tylko ograniczą ryzyko, ale także wzmocnią swoją zdolność do wprowadzania innowacji, przestrzegania przepisów i konkurowania w gospodarce cyfrowej, która zależy od zaufania.

Dalsze działania

Pojawienie się obliczeniowych systemów kwantowych stanowi zarówno szansę dla generacji, jak i bezprecedensowe wyzwanie w zakresie bezpieczeństwa. Chociaż dokładny harmonogram wprowadzenia kryptograficznie odpowiednich komputerów kwantowych pozostaje niepewny, to pewne jest, że należy podjąć wysiłek, aby się do tego przygotować. Przejście na kryptografię postkwantową będzie wymagało lat skoordynowanego planowania, inwestycji i realizacji. Oczekiwanie na wdrożenie komputerów kwantowych nie jest praktyczną opcją.

Pierwszym krokiem dla każdej organizacji jest uświadomienie: zrozumienie, gdzie i w jaki sposób kryptografia jest używana w całym środowisku. Od tego momentu przedsiębiorstwa muszą rozpocząć proces inwentaryzacji, nadawania priorytetów i pilotażu bezpiecznych rozwiązań kwantowych. Kryptografia hybrydowa, łącząca algorytmy klasyczne i postkwantowe, zapewnia natychmiastową odporność, podczas gdy standardy wciąż się rozwijają. Dostosowując wewnętrzne plany działania do globalnych struktur, takich jak standardy PQC NIST i harmonogramy CNSA 2.0, organizacje mogą pewnie zmierzać do zgodności z przepisami i interoperacyjności.

Firma Dell Technologies jest zaangażowana w pomoc klientom w przejściu na ten nowy etap. Dzięki naszemu podejściu zapewniamy solidne podstawy w zakresie integralności łańcucha dostaw, zabezpieczeń sprzętowych i możliwości dostosowywania oprogramowania. Nasze relacje partnerskie z czołowymi dostawcami zabezpieczeń i nasza aktywna rola w organach standaryzacyjnych w branży dają pewność, że rozwiązania firmy Dell są nie tylko zgodne z najnowszymi wymaganiami, ale także przetestowane pod kątem rzeczywistej wydajności i interoperacyjności.

Zacznij się przygotowywać już dziś. Zacznij od zauważenia i analizy ryzyka, zaangażuj zaufanych dostawców i pilotuj technologie odporne na kwantowe zagrożenia. Każdy podjęty krok zmniejsza ryzyko zakłóceń w przyszłości. Organizacje, które zadziałają wcześnie, nie tylko zabezpieczą swoje dane i systemy, ale także zyskają zaufanie klientów, organów regulacyjnych i partnerów w epoce, w której zaufanie cyfrowe jest najważniejsze.

Informacje o programie

Firma Dell Technologies dokłada wszelkich starań, aby zaawansowana technologia była dostępna i godna zaufania, a przy tym zapewniała wszystkim większe możliwości. Pomagamy ludziom i organizacjom bezpiecznie wykorzystywać innowacje, tworząc bezpieczniejszą, bardziej inkluzywną i połączoną przyszłość.

Dowiedz się więcej o rozwiązaniach Dell [product name]

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies