

Kryptografia postkwantowa

Rozpocznij



Wprowadzenie

Obliczenia kwantowe powodują fundamentalną przebudowę technologii, stwarzając zarówno niesamowite możliwości, jak i nowe wyzwania. Chociaż przyszłość ta rysuje się ekscytująco, to stanowi poważne zagrożenie dla systemów kryptograficznych chroniących nasz cyfrowy świat.

Dlaczego obliczenia kwantowe zyskują na popularności?

Komputery klasyczne, niezależnie od tego, czy są to laptopy, smartfony czy serwery, przetwarzają informacje za pomocą bitów, które mogą przyjmować wartości 0 lub 1. 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.

Co to jest kryptografia postkwantowa?

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.

Jakie bezpośrednie zagrożenia dla organizacji wiążą się z obliczeniami kwantowymi?

Konsekwencje wykraczają daleko poza teoretyczne ryzyko. Organizacje, które się nie przygotowują, narażają na niebezpieczeństwo wrażliwe składniki własności intelektualnej oraz bezpieczeństwo narodowe, a także wystawiają się na ryzyko zakłóceń w systemach finansowych i naruszeń danych zdrowotnych.

Zagrożenie typu „Zbierz teraz, odszyfruj później” potęguje pilność problemu: adwersarze muszą już dziś przechwycić zaszyfrowane dane i poczekać na środki do ich odszyfrowania. Zanim pojawią się komputery kwantowe mające znaczenie dla kryptografii, szkody będą już nieodwracalne.

„Zbierz teraz, odszyfruj później” (Harvest Now, Decrypt Later) — znane również jako „Zapisz teraz, odszyfruj później” („Record Now, Decrypt Later”) — to praktyka polegająca na gromadzeniu i przechowywaniu zaszyfrowanych danych przez adwersarzy z zamiarem ich odszyfrowania w przyszłości, gdy dostępne będą kryptograficznie odpowiednie komputery kwantowe.



Jak organizacje powinny przygotować się do przejścia na PQC?

—

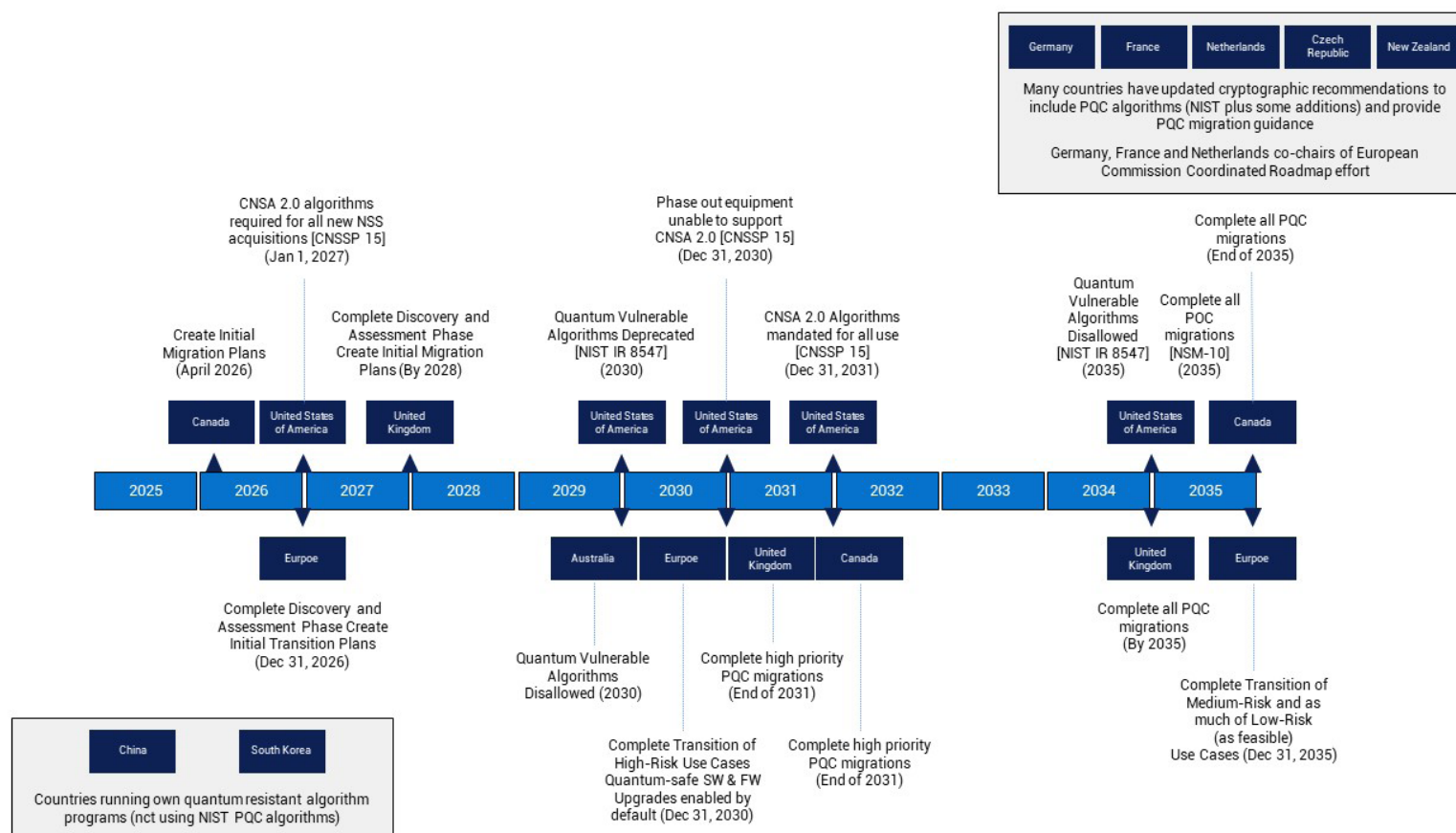
Droga do przyszłości bezpiecznej pod względem kwantowym to maraton, a nie sprint — i jest to droga wciąż ewoluująca. Proaktywne, warstwowe i etapowe podejście pomoże Twojej organizacji zarządzać ryzykiem, dostosowywać zasoby i budować odporność na zagrożenia w dłuższej perspektywie. Firma Dell zapewnia technologie i wskazówki, które pomogą Ci na każdym etapie. Oto najważniejsze kroki, które pomogą Twojej organizacji w tworzeniu planu przejścia na PQC.



Harmonogram przejścia PQC

Uznając pilność tego zagrożenia, rządy i organy standaryzacyjne uznały PQC za globalny priorytet. Zdając sobie sprawę ze znaczenia przyjęcia algorytmów kryptograficznych odpornego na kwanty, rząd federalny USA zaczął wydawać wymogi PQC agencjom federalnym. Należą do nich National Security Memorandum 10 (NSM-10), The Commercial National Security Algorithm Suite (CNSA 2.0), The Office of Management and Budget Memorandum 23-02 (OMB M-2302) oraz National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547), ale nie tylko.

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



Inwentaryzacja i audyt zagrożeń kryptograficznych

Pierwszym priorytetem jest zrozumienie obecnego krajobrazu kryptograficznego. Ten podstawowy krok będzie stanowił o całej strategii migracji.

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. W przypadku nowszych systemów ważne jest również podniesienie minimalnego poziomu bezpieczeństwa – AES-256 dla kryptografii symetrycznej, SHA-384 lub wyższy dla skrótów – aby przeciwdziałać zmniejszeniu marginesów wprowadzonych 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, dane klientów, zarchiwizowane dane i nie tylko. 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”.



Pilotowanie i eksperymenty z PQC

Dzięki wyraźnym zasobom możesz rozpocząć praktyczne eksperymenty z technologiami gotowymi do PQC, aby zweryfikować wydajność i integrację.

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 PQC można rozpocząć planowanie wdrożeń produkcyjnych. Podejście hybrydowe stanowi pomost do środowiska w pełni bezpiecznego kwantowo.

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.



Wykonywanie pełnej migracji i ciągła weryfikacja

Ostatecznym celem jest w pełni zintegrowane i stale weryfikowane przedsiębiorstwo bezpieczne pod względem kwantowym.

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 rozwiązań składających się z komputerów klasycznych i kwantowych, klienci mogą symulować scenariusze ataków, weryfikować integralność kryptograficzną i zapewnić odporność systemów na zmieniające się zagrożenia.



Współpraca i wymiana wiedzy

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.



Wnioski

Era kwantowa nie jest już odległą możliwością; jest to nieuchronna rzeczywistość, która wymaga dziś dalekowzrocznych działań. Przygotowanie się na tę zmianę technologiczną jest strategicznym imperatywem w zakresie ochrony najcenniejszych zasobów – danych. Jak już wspomnieliśmy, najbardziej oczywistą drogą do przyszłości bezpiecznej pod względem kwantowym jest podejście etapowe, przechodzące od inwentaryzacji i audytu do pełnej migracji.

Przejście na PQC 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 przejściu na PQC.

