

Postkvantum- kryptografi

Kom i gång



Introduktion

Kvantberäkning driver en grundläggande omdesign av tekniken, vilket skapar både otroliga möjligheter och nya utmaningar. Den här framtiden är visserligen spännande, men den medför ett betydande hot mot de kryptografiska system som skyddar vår digitala värld.

Varför ökar kvantberäkning?

Klassiska datorer, oavsett om det är bärbara datorer, smartphones eller servrar, bearbetar information med hjälp av bitar, som är antingen nollor eller ettor. Den här binära modellen har drivit årtionden av framsteg, men den begränsar hur information kan representeras och manipuleras. Kvantdatorer använder kvantbitar (qubits), som kan representera flera tillstånd samtidigt genom principer som superposition och sammanflätning. Det gör det möjligt för kvantdatorer att utforska ett stort antal möjliga lösningar parallellt, vilket medför en beräkningsfördel för vissa typer av problem.

Vad är postkvantumkryptografi?

Postkvantumkryptografi (PQC) avser en ny generation algoritmer som utformats för att skydda digitala system mot både klassiska angrepp och kvantattacker. Till skillnad från kvantnyckeldistribution, som kräver specialiserad hårdvara, är PQC utformat för att köras på dagens klassiska infrastruktur – servrar, slutpunkter, nätverk – och är därför det mest praktiska och skalbara sättet att förbereda sig för kvanteran.

Vilka risker medför kvantberäkning i närtid för organisationer?

Konsekvenserna sträcker sig långt bortom teoretiska risker. Om organisationer misslyckas med att förbereda sig riskeras exponering av känslig immateriell egendom, störningar i finansiella system, intrång i hälso- och sjukvårdsdata och hot mot den nationella säkerheten.

Hotet "skörda nu, dekryptera senare" gör läget ännu mer brådskande: Angripare behöver bara samla in krypterade data idag och vänta på att de ska kunna dekryptera dem. När de kryptografiskt relevanta kvantdatorerna är här är skadan redan skedd.

"Skörda nu, dekryptera senare" (HNDL, harvest now, decrypt later) – Kallas även "record now, decrypt later" och innebär att angripare samlar in och lagrar krypterade data idag med avsikt att dekryptera dem i framtiden när kryptografiskt relevanta kvantdatorer finns tillgängliga.



Hur bör organisationer förbereda sig för övergången till PQC?

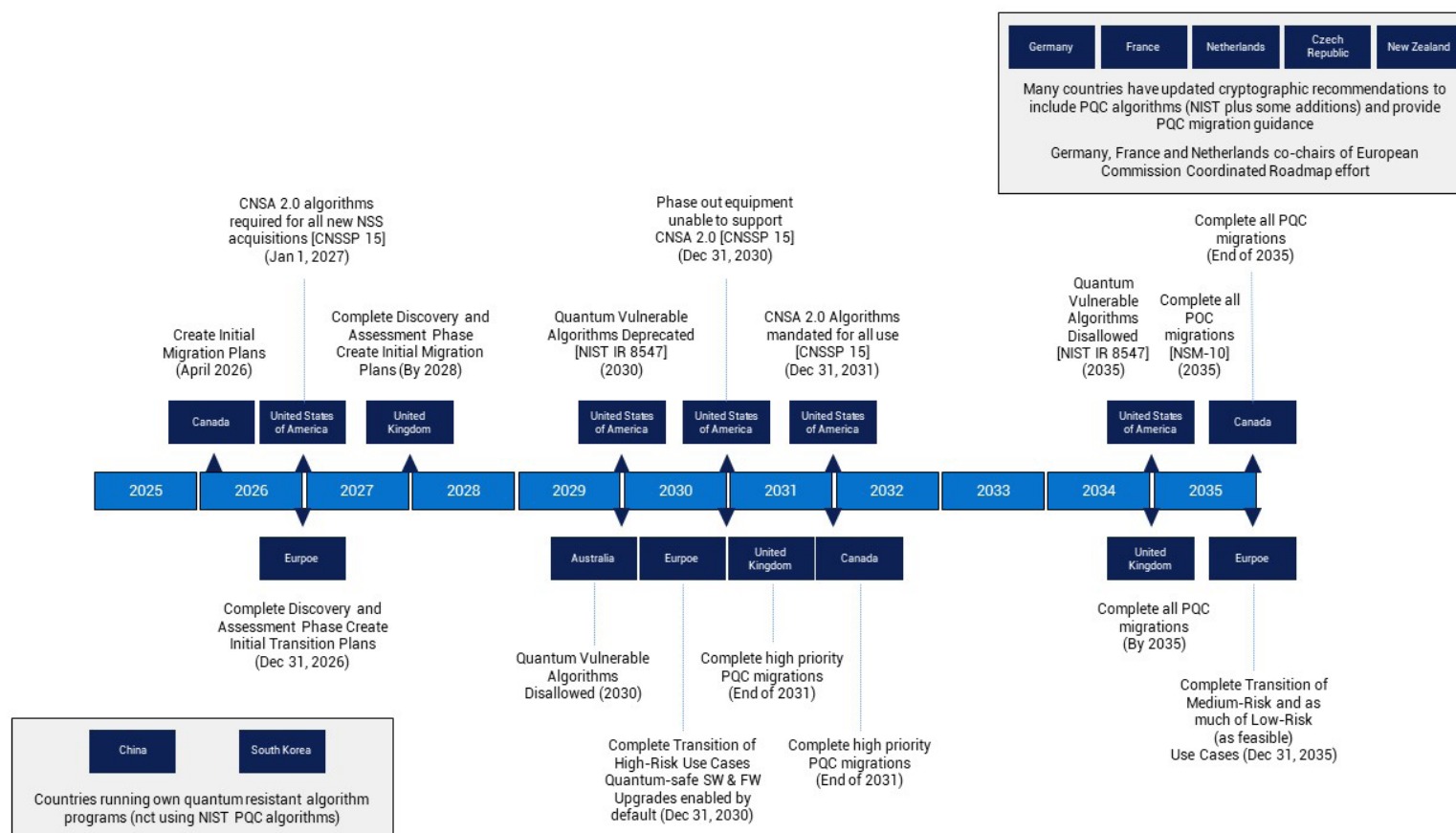
Resan mot en kvantsäker framtid är ett maraton, inte en sprint, och en resa som utvecklas. En proaktiv, skiktad och stegvis metod hjälper din organisation att hantera risker, anpassa resurser och bygga en motståndskraftig säkerhetsställning på lång sikt. Dell tillhandahåller den teknik och vägledning som behövs för att stödja dig i varje steg. Här är de viktigaste stegen för att vägleda din organisation när det gäller att skapa en PQC-övergångsplan.



Tidslinje för PQC-övergång

Eftersom hotet är så brådskande har regeringar och standardiseringsorgan gjort PQC till en global prioritet. USA:s federala regering inser vikten av att införa kvantresistenta kryptografiska algoritmer och har börjat utfärda PQC-krav till federala myndigheter. Dessa inkluderar National Security Memorandum 10 (NSM-10), Commercial National Security Algorithm Suite (CNSA 2.0), Office of Management and Budget Memorandum 23-02 (OMB M-2302) och National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547) och andra.

Andra organisationer runt om i världen har också utarbetat riktlinjer för PQC-övergången. De här datumen är inte slumpmässiga – de återspeglar de ledtider som krävs för att omarbeta, validera och distribuera kryptografi i komplexa IT-ekosystem. Företag bör inte betrakta dem som enbart myndighetskrav, utan som praktiska indikatorer på den globala övergången mot kvantresiliens. Här nedan anges några av de olika landskraven.



Inventera och granska kryptografiska hot

Den första prioriteringen är att förstå ditt nuvarande kryptografiska landskap. Det här grundläggande steget utformar hela din migreringsstrategi.

God säkerhetshygien

Det första steget i att förbereda sig för kvantteknikens framtid är att stärka de försvar som redan finns på plats. Organisationer bör använda bästa praxis för säkerhetshygien, till exempel att tillämpa åtkomst med minsta behörighet, implementera multifaktorautentisering och upprätthålla strikt korrigeringshantering. Det finns två ytterligare aspekter att ta hänsyn till. Det kan vara viktigt att inaktivera svagare kryptografi så att nya system med mer kraftfull kryptografi kan interagera med äldre system. För nyare system är det också viktigt att höja den minsta säkerhetsstyrkan – AES-256 för symmetrisk kryptografi, SHA-384 eller högre för digests – för att motverka de minskade marginalerna som införs av Grovers algoritm. Åtgärderna minskar inte bara riskerna idag utan minimerar också den kryptografiska eftersläpning som annars skulle försvåra morgondagens migrering.

Inventera och granska kryptografiska tillgångar

Hörnstenen i alla migreringsplaner är insyn. Organisationer måste genomföra en omfattande kryptografisk inventering där man identifierar var och hur kryptografi med offentlig nyckel används i applikationer, enheter och arbetsflöden. Det inkluderar TLS-certifikat, VPN, mejlssystem, kodsigneringsmekanismer, kunddata och arkiverade data. När tillgångarna har identifierats bör de prioriteras utifrån affärskritikalitet, känslighet och livslängd. Data med lång livslängd – som patientjournaler eller sekretessbelagda arkiv – bör behandlas med högsta prioritet, eftersom de är mest sårbara för "skörda nu, dekryptera senare"-hotet.



Testa och experimentera med PQC

Med en tydlig inventering kan du påbörja praktiska experiment med PQC-förberedd teknik för att validera prestanda och integrering.

När det kryptografiska landskapet har kartlagts bör organisationer börja testa PQC-lösningar i kontrollerade miljöer. Genom att testa de här lösningarna i labb kan IT-teamen validera prestanda, interoperabilitet och hanterbarhet före storskalig distribution. Att bygga upp den här kryptoagiliteten – förmågan att byta kryptografiska algoritmer utan att göra om hela system – är avgörande för långsiktig motståndskraft och smidig migrering.



Anta en interoperabilitetsstrategi

Allt eftersom PQC-standarderna mognar kan du börja planera för produktionsdriftsättningar. En hybridmetod ger en bro till en helt kvantsäker miljö.

Medan standarderna mognar erbjuder en hybridmodell en brygga till framtiden. Många leverantörer stöder redan hybridkrypteringssviter som kombinerar klassiska och kvantresistenta algoritmer i en enda implementering. En sådan dubbel strategi säkerställer kontinuerligt skydd även om en av algoritmerna senare komprometteras. Företag bör börja införa hybridstrategier nu och anpassa sina interna tidsplaner efter infrastrukturleverantörens produktplaner och milstolpar. På så sätt kan organisationer skala upp implementeringen utan störningar i takt med att kvantsäkra algoritmer når standardisering.



Utför fullständig migrering och kontinuerlig validering

Slutmålet är ett helt integrerat och kontinuerligt validerat kvantsäkert företag.

Utför fullständig migrering och kontinuerlig validering

Slutmålet är en fullständig övergång till postkvantumkryptografi (PQC) i hela företaget. Det är ingen engångshändelse utan en pågående validerings- och anpassningsprocess. Organisationer bör genomföra detaljerade migreringsplaner där PQC införlivas i varje lager av IT-stacken samtidigt som nya standarder och implementeringar testas löpande. Med en hybridmodell som kombinerar klassiska och kvantbaserade datorer kan kunder simulera attackscenarier, validera kryptografisk integritet och säkerställa att deras system förblir motståndskraftiga mot nya hot.



Samarbete och kunskapsdelning

Ingen organisation bör stå ensam inför denna utmaning.

Branschkonsortier, akademiska forskare och statliga myndigheter samlar sin kunskap för att påskynda PQC-övergången. Genom att delta i standardiseringsgrupper, arbetsgrupper och pilotprogram kan företag hålla jämna steg med bästa praxis och nya krav. Dells aktiva engagemang i initiativ som NIST NCCoE PQC-projektet säkerställer att våra kunder kan dra direkt nytta av denna samlade expertis.



Sammanfattning

Kvanteran är inte längre en avlägsen möjlighet, utan en överhängande verklighet som kräver proaktiva åtgärder idag. Att förbereda sig för det här teknikskiftet är en strategisk nödvändighet för att skydda din mest värdefulla tillgång – dina data. Som vi har beskrivit är en stegvis metod som går från inventering och granskning till fullständig migrering den tydligaste vägen till en kvantsäker framtid.

Övergången till PQC blir en av de största infrastrukturförändringarna på årtionden. Övergången berör nästan alla aspekter av IT, från servrar och lagring till slutpunkter, molnplattformar och nätverksprotokoll. För att lyckas krävs förutseende, planering och ett disciplinerat genomförande. På Dell Technologies ser vi vägen framåt som en stegvis resa, där omedelbara säkerhetsförbättringar balanseras med långsiktig beredskap för PQC-implementering.

Dell är redo att hjälpa dig med din strategi för implementering av PQC. Vi rekommenderar en fasad migreringsplan och vi har skisserat en uppsättning aktiviteter som hjälper dig att planera, genomföra och övervaka PQC-övergången.

