

Post-kwantum- cryptografie

Aan de slag



Introductie

Kwantumcomputing is de drijvende kracht achter een fundamentele herziening van technologie, waardoor zorgt voor zowel ongelooflijke kansen als nieuwe uitdagingen. Hoewel deze toekomst spannend is, brengt het een aanzienlijke bedreiging met zich mee voor de cryptografische systemen die onze digitale wereld beschermen.

Waarom is kwantumcomputing in opkomst?

Klassieke computers, of ze nu in laptops, smartphones of servers zitten, verwerken informatie met behulp van bits, die de waarde van nul of één aannemen. Dit binaire model is al tientallen jaren de drijvende kracht achter vooruitgang, maar het beperkt de manier waarop informatie kan worden weergegeven en gemanipuleerd. Kwantumcomputers maken gebruik van qubits. Deze kunnen door principes als superpositie en verstrengeling tegelijkertijd meerdere waarden kunnen hebben. Hierdoor kunnen kwantummachines gelijktijdig enorme aantallen mogelijke oplossingen verkennen en dit biedt een computationeel voordeel voor specifieke soorten problemen.

Wat is post-kwantumcryptografie?

Post-kwantumcryptografie (PQC) verwijst naar een nieuwe generatie algoritmen die zijn ontworpen om digitale systemen te beveiligen tegen zowel klassieke als kwantumaanvallen. In tegenstelling tot kwantumsleuteldistributie, dat speciale hardware vereist, is PQC ontworpen om te worden uitgevoerd op de hedendaagse klassieke infrastructuur, zoals servers, eindpunten en netwerken. Dit maakt het tot de meest praktische en schaalbare manier om u voor te bereiden op het kwantumtijdperk.

Welke directe risico's lopen organisaties met kwantumcomputing?

De gevolgen gaan veel verder dan theoretische risico's. Organisaties die zich niet voorbereiden, kunnen worden geconfronteerd met de openbaarmaking van gevoelig intellectueel eigendom, verstoring van financiële systemen, inbreuken op data in de gezondheidszorg en bedreigingen voor de nationale veiligheid.

De dreiging 'Harvest Now, Decrypt Later' vergroot de urgentie: kwaadwillenden hoeven nu alleen maar versleutelde data te verzamelen en te wachten op de middelen om deze te decoderen. Tegen de tijd dat cryptografisch relevante kwantumcomputers beschikbaar komen, is de schade al onomkeerbaar.

'Harvest Now, Decrypt Later' (ook bekend als 'Record Now, Decrypt later') – het verzamelen en opslaan van versleutelde data door kwaadwillenden met de bedoeling deze in de toekomst te decoderen zodra cryptografisch relevante kwantumcomputers beschikbaar zijn.



Hoe moeten organisaties zich voorbereiden op de overgang naar PQC?

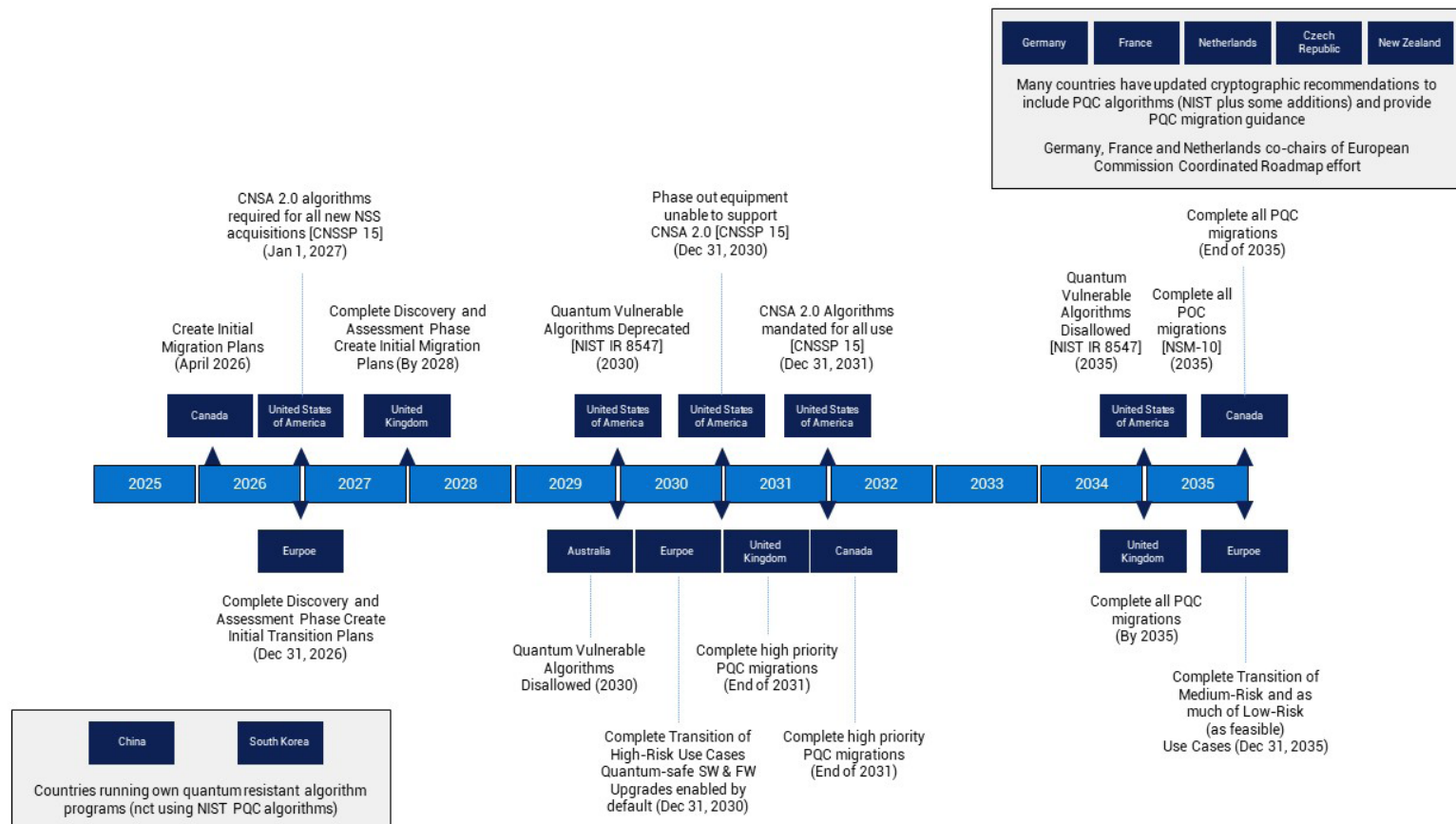
De reis naar een kwantumveilige toekomst is een marathon, geen sprint, en een steeds veranderend traject. Een proactieve, gelaagde en gefaseerde aanpak helpt uw organisatie bij het beheren van risico's, het afstemmen van resources en het opbouwen van een veerkrachtige beveiligingsmentaliteit voor de lange termijn. Dell biedt de technologieën en begeleiding om u in elke fase te ondersteunen. Hier volgen de belangrijkste stappen om uw organisatie te begeleiden bij het maken van een plan voor de overgang naar PQC.



Tijdlijn overgang naar PQC

Overheden en normalisatie-instellingen erkennen de urgentie van de dreiging en hebben PQC tot een wereldwijde prioriteit gemaakt. De Amerikaanse federale overheid beseft hoe belangrijk het is om kwantumbestendige cryptografische algoritmen te gebruiken en is daarom begonnen met het opstellen van PQC-vereisten voor federale instanties. Deze omvatten onder andere het National Security Memorandum 10 (NSM-10), de Commercial National Security Algorithm Suite (CNSA 2.0), het Office of Management and Budget Memorandum 23-02 (OMB M-2302) en het National Institute of Standards and Technology Interagency Report 8547 (NIST IR 8547).

Andere organisaties over de hele wereld hebben ook richtlijnen opgesteld voor de PQC-transitie. Deze deadlines zijn niet willekeurig: ze weerspiegelen de doorlooptijd die nodig is om cryptografie opnieuw te ontwerpen, te valideren en te implementeren in complexe IT-ecosystemen. Ondernemingen moeten ze zien als meer dan alleen overheidsmandaten; het zijn praktische aanwijzingen voor de wereldwijde verschuiving naar kwantumtolerantie. Hieronder vindt u enkele van de verschillende nationale voorschriften.



Inventariseer en audit cryptografische dreigingen

De topprioriteit is inzicht in uw huidige cryptografische landschap. Deze fundamentele stap vormt de basis voor uw gehele migratiestrategie.

Goede beveiligingshygiëne

De eerste stap in de voorbereiding op de kwantumtoekomst bestaat uit het versterken van de bestaande verdediging. Organisaties moeten gebruikmaken van sterke best practices op het gebied van beveiligingshygiëne, zoals het afdwingen van toegang met minimale bevoegdheden, het implementeren van meervoudige verificatie en het onderhouden van rigoureuus patchbeheer. Daarnaast zijn er twee andere zaken om te overwegen. Het kan belangrijk zijn om zwakkere cryptografie uit te schakelen, zodat nieuwe systemen met een hogere cryptografie kunnen samenwerken met verouderde systemen. Het is ook belangrijk voor nieuwere systemen om de minimale beveiligingssterkte te verhogen (AES-256 voor symmetrische cryptografie, SHA-384 of hoger voor digests) om de kleinere marges te compenseren die door het algoritme van Grover worden geïntroduceerd. Deze maatregelen verminderen niet alleen het risico nu, maar minimaliseren ook de achterstand in cryptografische vorderingen die anders de migratie in de toekomst kan bemoeilijken.

Inventariseer en audit cryptografische assets

Zichtbaarheid is de hoeksteen van elk migratieplan. Organisaties moeten een uitgebreide cryptografische inventaris uitvoeren, waarbij wordt vastgesteld waar en hoe cryptografie met openbare sleutels wordt gebruikt in applicaties, apparaten en workflows. Dit omvat TLS-certificaten, VPN's, e-mailsystemen, codeondertekeningsmechanismen, klantdata, gearchiveerde data en meer. Eenmaal geïdentificeerd, moeten assets prioriteit krijgen op basis van bedrijfskritikaliteit, gevoeligheid en levensduur. Data met een lange levensduur – zoals medische dossiers of vertrouwelijke archieven – moeten met de hoogste urgentie worden behandeld, omdat ze het meest kwetsbaar zijn voor de dreiging van 'Harvest Now, Decrypt Later'.



Test en experimenteer met PQC

Met een duidelijke inventaris kunt u praktische experimenten beginnen met PQC-ready technologieën om prestaties en integratie te valideren.

Zodra organisaties het cryptografische landschap begrijpen, moeten ze beginnen met het testen van PQC-oplossingen in gecontroleerde omgevingen. Door deze oplossingen in laboratoria te testen, kunnen IT-teams de prestaties, interoperabiliteit en beheerbaarheid controleren voordat oplossingen op grote schaal worden geïmplementeerd. Het opbouwen van deze cryptografische flexibiliteit – het vermogen om te schakelen tussen cryptografische algoritmen zonder hele systemen te hoeven reviseren – is cruciaal voor veerkracht op de lange termijn en een soepele migratie.



Implementeer een aanpak voor interoperabiliteit

Naarmate PQC-standaarden volledig ontwikkeld worden, kunt u beginnen met het plannen van productie-implementaties. Een hybride aanpak biedt een brug naar een volledig kwantumveilige omgeving.

Naarmate standaarden volwassen worden, biedt een hybride model een brug naar de toekomst. Veel leveranciers ondersteunen al hybride coderingssuites die klassieke en kwantumbestendige algoritmen combineren in één implementatie. Deze dubbele aanpak biedt continuïteit van bescherming, zelfs als één algoritme later wordt gecompromitteerd. Ondernemingen moeten nu beginnen met het implementeren van hybride strategieën en tegelijkertijd hun interne tijdlijnen afstemmen op de productroadmaps en mijlpalen van hun infrastructuurleverancier. Dit zorgt ervoor dat wanneer kwantumveilige algoritmen gestandaardiseerd worden, organisaties de implementatie zonder onderbrekingen kunnen opschalen.



Voer een volledige migratie en continue validatie uit

Het uiteindelijke doel is een volledig geïntegreerde en continu gevalideerde kwantumveilige onderneming.

Voer een volledige migratie en continue validatie uit

Het uiteindelijke doel is een volledige overgang naar PQC in de hele onderneming. Dit zal geen eenmalige gebeurtenis zijn maar een doorlopend proces van validatie en aanpassing. Organisaties moeten gedetailleerde migratieplannen uitvoeren, waarbij ze PQC in elke laag van hun IT-stack integreren en tegelijkertijd voortdurend nieuwe standaarden en implementaties testen. Met behulp van hybride laboratoria die zowel klassieke als kwantumcomputers bevatten, kunnen klanten aanvalsscenario's simuleren, de cryptografische integriteit valideren en ervoor zorgen dat hun systemen bestand blijven tegen veranderende dreigingen.



Samenwerken en delen van kennis

Geen enkele organisatie zou deze uitdaging alleen moeten aangaan.

Brancheorganisaties, onderzoekers uit de academische wereld en overheidsinstellingen bundelen kennis om de overgang naar PQC te versnellen. Door deel te nemen aan normalisatiegroepen, werkgroepen en proefprogramma's zorgen ondernemingen ervoor dat ze op de hoogte blijven van best practices en opkomende vereisten. De actieve betrokkenheid van Dell bij initiatieven zoals het NCCoE PQC-project van NIST zorgt ervoor dat onze klanten rechtstreeks profiteren van deze gezamenlijke expertise.



Conclusie

Het kwantumtijdperk is niet langer een minieme mogelijkheid; het is een dreigende realiteit waarvoor nu actie moet worden ondernomen. Voorbereiding op deze technologische verschuiving is een strategische noodzaak voor het beschermen van uw meest waardevolle asset: uw data. Zoals beschreven is een gefaseerde aanpak die overgaat van inventarisatie en controle naar volledige migratie de beste weg naar een kwantumveilige toekomst.

De overgang naar PQC zal een van de belangrijkste infrastructuurwijzigingen van de afgelopen decennia zijn. Deze overgang raakt bijna elk aspect van IT, van servers en storage tot eindpunten, cloudplatforms en netwerkprotocollen. Een succesvolle overgang vereist een vooruitziende blik, planning en een gedisciplineerde uitvoering. Bij Dell Technologies zien we de weg vooruit als een gefaseerd traject: een traject dat een evenwicht biedt tussen onmiddellijke beveiligingsverbeteringen en de gereedheid op lange termijn voor de implementatie van PQC.

Dell staat klaar om u te helpen met uw strategie voor het implementeren van PQC. We raden een gefaseerd migratieplan aan en hebben een reeks activiteiten beschreven die u helpen bij het opstellen van een strategie voor en het plannen, uitvoeren en bewaken van uw overgang naar PQC.

