

Post-kwantumcryptografie: voorbereiding op het kwantumtijdperk

—

Een whitepaper van Dell Technologies

Inhoudsopgave

Managementsamenvatting	3
Terminologie	3
Kwantumcomputing en de dreiging voor versleuteling	4
Post-kwantumcryptografie en opkomende standaarden	4
Waarom nu het moment is om actie te ondernemen	7
Over ons.....	11

Managementsamenvatting

Kwantumcomputing ontwikkelt zich snel van theoretisch onderzoek tot praktische realiteit. Wat ooit als een verre toekomst werd beschouwd, wordt door de vooruitgang op het gebied van hardware, algoritmen en investeringen steeds sneller werkelijkheid: machines die problemen kunnen oplossen die klassieke computers niet aankunnen. Dit heeft vergaande gevolgen voor de industrie. Van het ontdekken van nieuwe geneesmiddelen tot klimaatmodellering en wereldwijde logistiek: kwantumcomputing belooft innovaties mogelijk te maken die voorheen onbereikbaar waren.

Maar deze doorbraak brengt een ontwrichtende uitdaging met zich mee: kwantumcomputers zullen de cryptografische fundamenteën ondermijnen die de digitale economie beschermen. Cryptografie met openbare sleutels – algoritmen zoals RSA en elliptische curve-cryptografie (ECC) – beschermt al tientallen jaren digitale communicatie, financiële systemen, medische dossiers en de nationale veiligheid. Deze methoden vertrouwen op wiskundige problemen die klassieke computers niet kunnen oplossen. Maar met de komst van cryptografisch relevante kwantumcomputers (CRQC's) kunnen deze problemen efficiënt worden opgelost, waardoor de hedendaagse beveiliging achterhaald raakt.

Dit is geen theoretische bedreiging. Sommige organisaties maken al gebruik van een tactiek die bekend staat als 'harvest now, decrypt later' (HNDL). Dit betekent dat ze vandaag versleutelde data verzamelen met de verwachting dat deze kunnen worden gedecodeerd zodra kwantumcomputers verder ontwikkeld zijn. Gevoelige informatie die nu veilig lijkt, kan binnen enkele jaren kwetsbaar zijn. Het moment om actie te ondernemen is niet wanneer CRQC's beschikbaar komen, maar nu.

Deze whitepaper legt de urgentie van de kwantumdreiging uit, verkent het opkomende gebied van post-kwantumcryptografie (PQC) en biedt richtlijnen voor organisaties om zich voor te bereiden. Het benadrukt de inzet van Dell Technologies om een kwantumveilige toekomst op te bouwen door beveiliging in te bouwen in onze toeleveringsketen, hardware, firmware, software en partner-ecosysteem, door ons aan te sluiten bij de post-kwantumcryptografiestandaarden (PQC) van NIST – FIPS 203, FIPS 204 en FIPS 205 – en met de richtlijnen van de Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). Het doel van Dell is duidelijk: ervoor zorgen dat men kan blijven innoveren zonder dat dit ten koste gaat van de beveiliging of het vertrouwen.

Terminologie

In deze whitepaper worden een aantal termen gebruikt. We hebben een aantal van deze termen toegelicht, zodat u de whitepaper beter kunt begrijpen.

Post-kwantumcryptografie – een nieuwe wiskundige benadering van cryptografie, met nieuwe algoritmen die ontworpen zijn om bescherming te bieden tegen aanvallen van kwantumcomputers. Deze algoritmen worden uitgevoerd op klassieke computers en zijn bestand tegen zowel kwantumaanvallen als de bekende klassieke cryptografie-aanvallen.

Kwantumbestendig – kwantumbestendig verwijst naar systemen, algoritmen of infrastructuren die zijn ontworpen om veilig te blijven, zelfs in aanwezigheid van cryptografisch relevante kwantumcomputers (CRQC's). Een kwantumbestendig systeem maakt gebruik van post-kwantumcryptografie (PQC) of andere beveiligingen die zowel klassieke als kwantumaanvallen weerstaan, waardoor de vertrouwelijkheid, integriteit en authenticiteit van data in de toekomst worden gewaarborgd. Andere termen zoals kwantumresistent en kwantumveilig worden ook door elkaar gebruikt.

Cryptografische flexibiliteit – de mogelijkheid van systemen en applicaties van een organisatie om snel en naadloos te schakelen tussen cryptografische algoritmen, protocollen of sleutellengtes zonder omvangrijke herinrichtingen of operationele verstoringen.

'Harvest Now, Decrypt Later' (HNDL) (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 (CRQC's) beschikbaar zijn.

Kwantumcomputing en de dreiging voor versleuteling

De opkomst van kwantumcomputing

Zoals we bijna een jaar geleden in ons blogbericht [Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience](#) van onze CTO John Roese hebben beschreven, verwerken klassieke computers, of ze nu in laptops, smartphones of servers zitten, 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.

De potentiële toepassingen van kwantumcomputing zijn ongekend. Onderzoekers verwachten doorbraken op het gebied van geneesmiddelen door moleculaire interacties te simuleren met een precisie die klassieke computers niet kunnen evenaren. Klimaatwetenschappers voorzien nauwkeurigere modellen van wereldwijde systemen, terwijl de energiesector mogelijkheden ziet voor het optimaliseren van elektriciteitsnetten en opslag. Zelfs de logistiek en productiesector kunnen profiteren van kwantumoptimalisatietechnieken. De voordelen zijn echt en binnen bereik, maar datzelfde geldt voor de risico's.

Waarom versleuteling gevaar loopt

In het digitale tijdperk vormt versleuteling de basis van vertrouwen. Wanneer u een creditcardnummer invoert, inlogt op een beveiligde website of een ondertekende software-update ontvangt, garandeert cryptografie de vertrouwelijkheid, authenticiteit en integriteit. Het grootste deel van deze bescherming is gebaseerd op cryptografie met openbare sleutels: algoritmen zoals RSA en ECC die zijn gebaseerd op wiskundige problemen die voor klassieke machines computationeel onhaalbaar worden geacht.

Kwantumcomputing maakt hier een einde aan. Met **het algoritme van Shor** kan een voldoende krachtige kwantumcomputer de factorisatie- en discrete logaritme-problemen oplossen die de basis vormen van RSA en ECC. Zodra CRQC's bestaan, kunnen de digitale handtekeningen die software-updates beschermen, de sleutels die TLS-sessies tot stand brengen en de certificaten die apparaten verifiëren, allemaal worden gecompromitteerd. Dit heeft een systemische impact en bedreigt juist die mechanismen die de veiligheid van digitale transacties waarborgen.

Symmetrische cryptografie, waarbij algoritmen zoals AES worden gebruikt om opgeslagen data of beveiligde communicatie te beschermen, wordt geconfronteerd met een andere, minder ernstige uitdaging. **Met het algoritme van Grover** kan een kwantumcomputer de effectieve sterkte van symmetrische sleutels verminderen, waardoor de beveiliging wordt gehalveerd. Hoewel dit kan worden ondervangen door over te stappen op grotere sleutelgroottes, zoals AES-256, onderstreept deze aanpassing de wijdverbreide aanwezigheid van kwantumdreigingen.

Urgentie en gevolgen

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 strategie '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 CRQC's beschikbaar komen, is de schade al onomkeerbaar.

Post-kwantumcryptografie en opkomende standaarden

Definitie van 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.

De basis van PQC is een reeks wiskundige problemen die, voor zover nu bekend, bestand zijn tegen kwantumtechnieken zoals de algoritmen van Shor en Grover. De meest veelbelovende opties zijn op lattice gebaseerde cryptografie, op hash gebaseerde handtekeningen, op code gebaseerde schema's en multivariate vergelijkingen. Deze opties worden grondig getest en gestandaardiseerd om ervoor te zorgen dat ze dezelfde betrouwbaarheid en interoperabiliteit bieden die RSA en ECC eerder boden.

De wereldwijde inspanning op het gebied van standaardisatie – opkomende industriestandaarden

Overheden en normalisatie-instellingen erkennen de urgentie van de dreiging en hebben PQC tot een wereldwijde prioriteit gemaakt. In 2016 lanceerde het Amerikaanse National Institute of Standards and Technology (NIST) zijn PQC-project, waarin het de cryptografische onderzoeksgemeenschap oproep om kandidaat-algoritmen in te dienen, te analyseren en te verfijnen. Na jaren van testen kondigde NIST in augustus 2024 de eerste groep gestandaardiseerde algoritmen aan:

- **CRYSTALS-Kyber** voor versleuteling met openbare sleutels en sleutelvaststelling
- **CRYSTALS-Dilithium** en **SPHINCS+** voor digitale handtekeningen

Er worden nog steeds aanvullende algoritmen beoordeeld om diversiteit en flexibiliteit te bieden voor verschillende implementatiebehoeften, waaronder lichtgewicht systemen zoals ingebouwde firmware. Dit zich ontwikkelende standaardisatieproces zorgt ervoor dat organisaties wereldwijd een duidelijk pad hebben voor de implementatie van kwantumbestendige oplossingen.

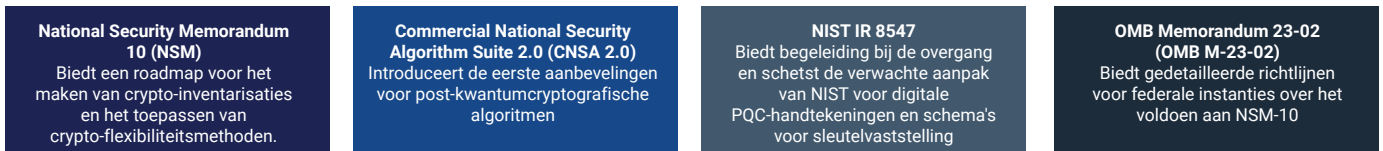
NIST-standaarden – FIPS 203, 204, 205

In augustus 2024 heeft het Amerikaanse National Institute of Standards and Technology (NIST) de eerste PQC-algoritmen afgerond:

- **FIPS 203 (ML-KEM)** – gebaseerd op CRYSTALS-Kyber, een sleutelinkapselingsmechanisme. Biedt IND-CCA2-beveiliging, wat betekent dat cijferteksten zelfs bij adaptief gekozen cijfertekst-aanvallen niet te onderscheiden zijn.
- **FIPS 204 (ML-DSA)** – gebaseerd op CRYSTALS-Dilithium, een algoritme voor digitale handtekeningen. Biedt sterke EUF-CMA-beveiliging (existentiële onvervalsbaarheid bij gekozen bericht-aanvallen), de standaardvereiste voor digitale handtekeningen.
- **FIPS 205 (SLH-DSA)** – gebaseerd op SPHINCS+, een op hash gebaseerd handtekeningschema. Geselecteerd als conservatieve fallback die niet afhankelijk is van lattice-problemen.

Een verplichte roadmap

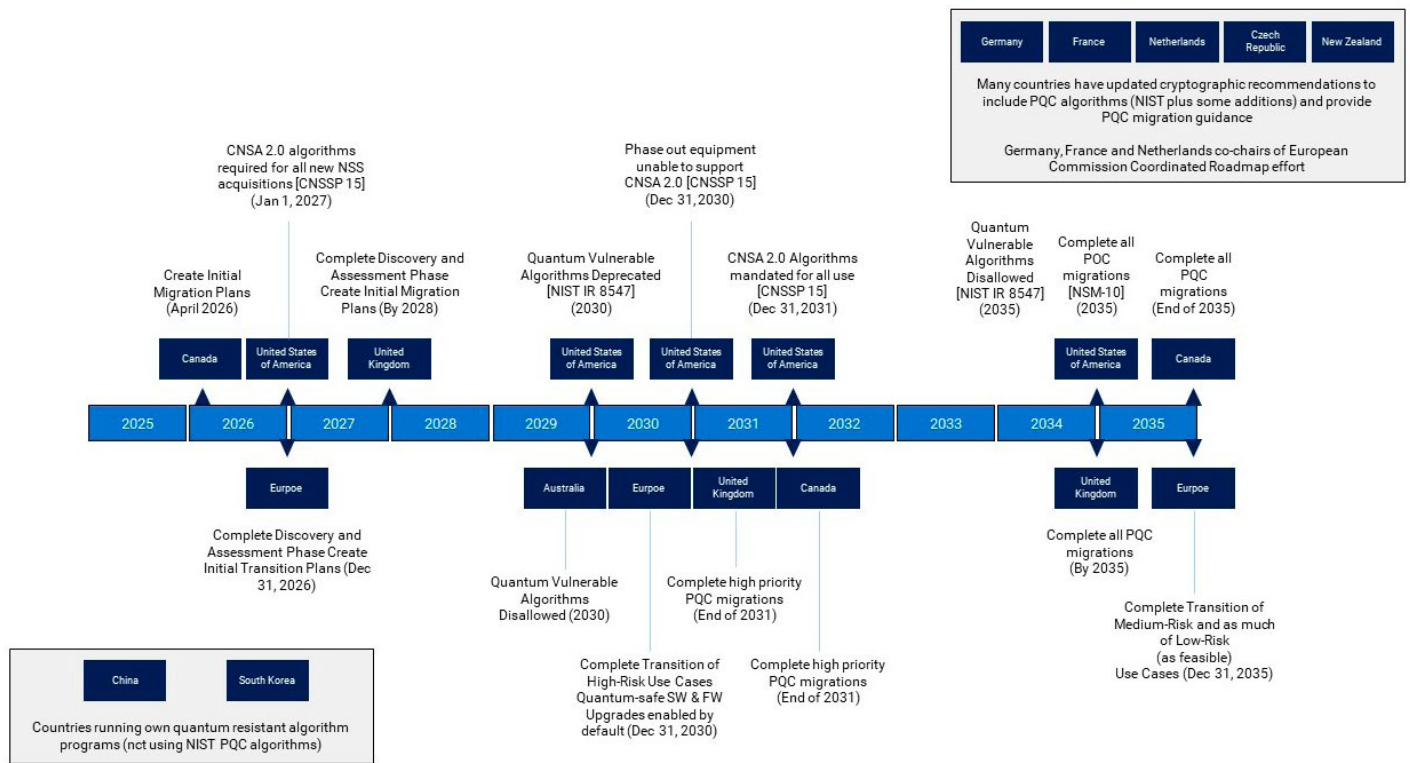
De Amerikaanse federale overheid beseft hoe belangrijk het is om kwantumbestendige versleutelingsalgoritmen te gebruiken en is daarom begonnen met het opstellen van PQC-vereisten voor federale instanties. Deze omvatten onder meer het National Security Memorandum 10 (NSM-10), de Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), het Interagency Report (IR) 8547 van het National Institute of Standards and Technology (NIST) en het Office of Management and Budget Memorandum 23-02 (OMB M-2302).



CNSA 2.0, aangekondigd door de NSA in september 2022, introduceert de eerste aanbevelingen voor post-quantumcryptografische algoritmen. CNSA 2.0 stelt expliciete deadlines vast voor de invoering van kwantumbestendige algoritmen in alle nationale veiligheidssystemen (NSS) en dient als een krachtig richtpunt voor ondernemingen die hun eigen transitie voorbereiden:



Andere organisaties over de hele wereld hebben ook richtlijnen opgesteld voor de PQC-transitie. Hieronder vindt u enkele van de verschillende nationale voorschriften.



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.

Samenwerking in de branche

Naast NIST en NSA oefent Dell actief invloed uit op en nemen we deel aan brancheorganisaties en normalisatiegroepen die interoperabiliteit en implementatie stimuleren. De Trusted Computing Group integreert PQC in de Trusted Platform Module (TPM)-standaard. De IETF stimuleert de integratie van PQC-algoritmen in industriële protocollen zoals TLS en X.509-certificaten. De OASIS Key Management Interoperability Protocol (KMIP)-commissies ondersteunen het gebruik van PQC voor sleutelbeheerframeworks. De FIDO Alliance bestudeert de impact van PQC op verificatie en de standaarden voor onboarding van apparaten, terwijl organisaties zoals SAFECODE de branche informeren over de voorbereiding op de migratie.

Dankzij het NIST National Cyber Security Center of Excellence (NCCoE) kan NIST via domeingerichte projecten samenwerken met de industrie, de academische wereld en overheidsinstellingen. Ze hebben zich gericht op verschillende zaken zoals:

- Cryptografische detectie – vaststellen welke cryptografie moet worden gemigreerd en hoe prioriteiten te stellen voor wat eerst moet worden gemigreerd.
- Interoperabiliteit – zorgen dat populaire cryptografische functies en protocollen de nieuwe PQC-algoritmen integreren en dat de oplossingen van verschillende leveranciers samenwerken.
- Cryptografische flexibiliteit – gericht op het ontwikkelen van informatiesystemen die snelle aanpassing aan nieuwe cryptografische primitieven en algoritmen ondersteunen zonder dat grote aanpassingen van de infrastructuur van het systeem nodig zijn.

Deze projecten dragen bij aan het ontwikkelen en opstellen van de richtlijnen en standaarden en zorgen ervoor dat er voorbeelden van industriële oplossingen zijn voor de standaarden en richtlijnen die ze bieden. Dell neemt sinds de oprichting deel aan het NCCoE Migration to PQC-project.

Vandaag de dag is PQC niet alleen een onderzoeksonderwerp; het is een zich ontwikkelende standaard met concrete algoritmen, tijdlijnen en implementatietrajecten. Organisaties die nu beginnen met de voorbereidingen, kunnen de kosten, verstoringen en risico's vermijden die ontstaan wanneer alles op het laatste moment snel moet worden geregeld. De transitie gaat niet alleen over naleving. Het gaat erom dat vertrouwen, betrouwbaarheid en integriteit gewaarborgd blijven terwijl kwantumcomputing het digitale landschap opnieuw vorm geeft.

Waarom nu het moment is om actie te ondernemen

De urgentie van de dreiging

Het kan verleidelijk zijn om kwantumcomputing te zien als een risico in de verre toekomst, iets dat kan worden aangepakt zodra de technologie volledig tot wasdom is gekomen. De werkelijkheid is dat de klok al tikt. Gevoelige informatie – denk aan financiële transacties, medische dossiers, intellectueel eigendom of overheidscommunicatie – is vandaag veilig versleuteld, maar zodra kwantumcomputing op de drempel staat om RSA of ECC te decoderen, kunnen die data alsnog openbaar worden gemaakt. Het gevolg is dat historische communicatie en documenten plotseling gevaar lopen.

Lange technologiecycli

Moderne IT-ecosystemen kunnen niet eenvoudig of snel worden getransformeerd. In het verleden duurde het meer dan tien jaar om één algoritme te vervangen. Denk aan de overgang van SHA-1 naar SHA-2 of van DES/3DES naar AES. Deze algoritmen zijn verregaand geïntegreerd in besturingssystemen, applicaties, netwerkapparaten en hardware. Om ze te vervangen, zijn een nieuw ontwerp, validatie, testen en implementatie nodig in omgevingen die variëren van datacenters tot cloudplatforms en edge-apparaten. Bij veel organisaties duurt dit jaren – veel langer dan de tijd die nog resteert voordat kwantumcomputing een reële bedreiging vormt. Daarom benadrukken regelgevers, normalisatie-instellingen en leiders op het gebied van beveiliging hoe belangrijk het is dat we direct beginnen om ons voor te bereiden. Als we wachten tot CRQC's op grote schaal beschikbaar zijn, blijft er geen tijd over voor een soepele overgang.

Risico's van afwachten

De gevolgen van het vertragen van de migratie gaan verder dan technische blootstelling:

- **Databeveiligingsrisico's:** data met een lange levensduur, zoals medische dossiers, financiële gegevens of militaire informatie, kunnen met terugwerkende kracht worden gecompromitteerd zodra kwantumcomputers volledig tot wasdom komen.
- **Risico's voor authenticiteit en integriteit van software:** de authenticiteit en integriteit van software kunnen worden aangetast door schadelijke code als deze wordt ondertekend met de huidige ondertekeningsmethoden en nog steeds wordt gebruikt zodra kwantumcomputers volledig zijn ontwikkeld.
- **Operationele risico's:** kritieke infrastructuursystemen, zoals nutsvoorzieningen, transportnetwerken en hulpdiensten, zijn enorm lastig te upgraden. Wanneer dit niet nu wordt gepland, kan dit later leiden tot een operationele verstoringen.
- **Risico's op het gebied van regelgeving en naleving:** kaders zoals **CNSA 2.0** hebben duidelijke tijdlijnen voor naleving vastgesteld. Organisaties die zich niet voorbereiden, lopen niet alleen het risico op blootstelling, maar ook dat ze niet voldoen aan de vereisten van de overheid of sector.
- **Reputatieschade en financiële risico's:** een inbreuk als gevolg van onopgeloste cryptografische kwetsbaarheden kan het merkvertrouwen blijvend schaden en resulteren in aanzienlijke financiële verliezen.

De casus voor proactieve actie

Proactieve voorbereiding is niet alleen een verdedigende zet. Het is een kans om de veerkracht op de lange termijn te versterken. Door cryptografische inventarisaties uit te voeren, symmetrische sleutellengtes te upgraden, PQC-ready oplossingen te testen en samen te werken met leveranciers die kwantumbestendige producten aanbieden, kunnen organisaties de continuïteit van vertrouwen waarborgen. Early adopters zijn beter in staat om hun activiteiten toekomstbestendig te maken, naleving te waarborgen en leiderschap te tonen aan klanten, partners en regelgevende instanties.

De aanpak van Dell ten aanzien van post-kwantumcryptografie

Bij Dell geloven we dat technologie de motor achter menselijke vooruitgang is en dat beveiliging de basis vormt van die vooruitgang. Als bedrijf zorgt Dell Technologies ervoor dat zijn portfolio, IT-infrastructuur en levenscyclusondersteunende systemen goed voorbereid zijn op de overgang naar kwantumbestendige algoritmen. We nemen onder andere de volgende stappen om de overgang voor te bereiden:

- Het identificeren van de specifieke gebieden en doelen waarvoor cryptografie wordt gebruikt in producten, services, IT-infrastructuur en supportsystemen om uitgebreide transitieplannen te formuleren.
- Het verbeteren van de interne kennis over post-kwantumcryptografische algoritmen (PQC), waarbij wordt gekeken naar implementatieaspecten en ontwerpprincipes op het gebied van cryptografische flexibiliteit om een soepele overgang naar PQC-algoritmen te ondersteunen.
- Het evalueren van de prestaties, toepasbaarheid en geschiktheid van PQC-algoritmen in verschillende gebruiksscenario's die relevant zijn voor het veelzijdige portfolio van Dell Technologies.

Gezien de complexe aard van de overgang naar PQC, worden upgrades van de cryptografische gebruiksscenario's gefaseerd doorgevoerd in het aanbod van Dell Technologies. Vanuit het perspectief van data wordt bijvoorbeeld prioriteit gegeven aan gebruiksscenario's die kwetsbaar kunnen zijn voor 'harvest now, decrypt later'-aanvallen, zoals de versleuteling van actieve data of van data-at-rest.

Bij het herzien van uw technologieplatform kan de overgang van een cryptografisch gebruiksscenario een volledige productvernieuwing/-vervanging of een productupgrade inhouden. Dit is afhankelijk van het betreffende product en waar en hoe de cryptografie in het product en de omliggende systemen wordt geïmplementeerd.

De release van een kwantumbestendig aanbod zal de komende vijf jaar een belangrijk aandachtspunt zijn om ervoor te zorgen dat klanten kunnen voldoen aan de tijdlijnen – die tussen 2027 en 2035 liggen – die overheden en brancheorganisaties hebben vastgesteld voor de overgang naar PQC.

Klanten moeten samenwerken met hun Dell accountteam om productspecifieke informatie te verkrijgen (bijv. roadmaps en tijdlijnen voor releases) die ze in hun migratieplannen kunnen opnemen. Houd de ontwikkelingen in de gaten, want Dell zal de komende maanden meer specifieke tijdlijnen bekendmaken voor de integratie van PQC in hun productlijnen en producten.

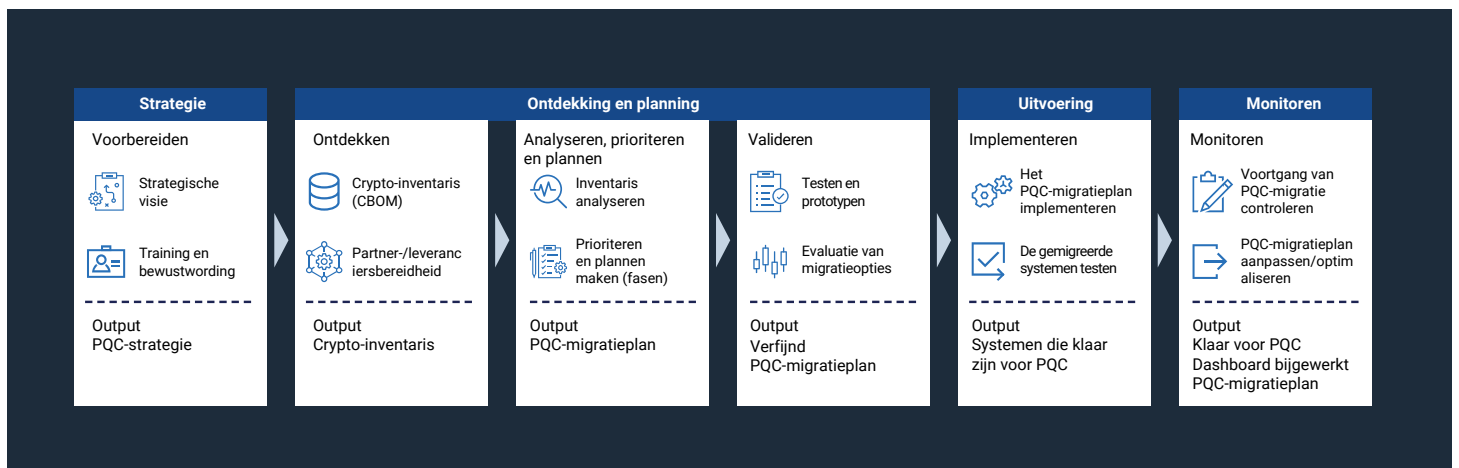
Vorbereiding op kwantumbestendige innovatie

Het doel van Dell is niet alleen om klanten te helpen te voldoen aan opkomende standaarden, maar ook om klanten in staat te stellen veilig te innoveren in het kwantumtijdperk. Of het nu gaat om het inzetten van AI-workloads, het beheren van hybride cloudomgevingen of het moderniseren van edge-infrastructuur, klanten kunnen erop vertrouwen dat de oplossingen van Dell zijn ontworpen met het oog op veerkracht. Beveiliging wordt niet achteraf toegevoegd, maar is ingebouwd in elke laag van het portfolio van Dell, zodat organisaties met vertrouwen de overstap naar post-kwantumcryptografie kunnen maken.

Vorbereiding op de overgang

De overgang naar post-kwantumcryptografie 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 migratie naar PQC.



Vorbereiding op de moderne beveiligingsmentaliteit

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 rigoureuze 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 dat symmetrische cryptografie voor nieuwere systemen wordt geüpgraded naar langere sleutellengtes – AES-256 en SHA-384 of hoger – 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 en gearchiveerde data. 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

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 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 tijdslijnen 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 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 kwantum-klassieke laboratoria 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

Tot slot zou geen enkele organisatie 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.

De voorbereiding op PQC is een marathon, geen sprint. Door een gefaseerde aanpak te kiezen waarbij achtereenvolgens de bestaande verdediging wordt versterkt, cryptografische assets worden geaudit, PQC wordt getest, hybride strategieën worden geïmplementeerd en een volledige migratie wordt uitgevoerd, kunnen organisaties vol vertrouwen de stap maken naar kwantumtolerantie. Met Dell als partner is dit traject niet alleen haalbaar, maar ook een kans om het vertrouwen te versterken en innovatie tot ver in de toekomst mogelijk te maken.

Praktische toepassingen en voordelen

De overgang naar post-kwantumcryptografie is meer dan alleen een kwestie van naleving. Het is een zakelijke noodzaak die rechtstreeks van invloed is op het vertrouwen, de veerkracht en het concurrentievermogen op de lange termijn. Voor telecommunicatieproviders, financiële instellingen, organisaties in de gezondheidszorg en overheidsinstanties zorgt de implementatie van kwantumbestendige algoritmen ervoor dat kritieke digitale infrastructuur beschermd blijft tegen zowel huidige als toekomstige dreigingen.

Telecommunicatie

Telecomnetwerken vormen de ruggengraat van wereldwijde digitalisering. Ze maken alles mogelijk, van de inzet van hulpdiensten en IoT-connectiviteit tot de veilige communicatie met klanten. Een kwantuminbreuk in deze sector zou de SIM-provisioning, eSIM-onboarding of de verificatieprocessen die ten grondslag liggen aan 4G en 5G in gevaar kunnen brengen. Door nu hybride en kwantumveilige cryptografie te implementeren, kunnen providers het vertrouwen van de klant behouden, de dataprivacy beschermen en naadloze continuïteit van de service garanderen voor generaties mobiele technologie.

Financiële dienstverlening

De financiële sector is een van de meest kwetsbare sectoren voor cyberaanvallen, en de integriteit van transacties is afhankelijk van cryptografie. De gereedheid voor het post-kwantumtijdperk beschermt digitale betalingen, online bankieren en interbancaire overschrijvingen tegen fraude met behulp van kwantumtechnologie. Door een vroegtijdige implementatie kunnen instellingen toezichthouders en klanten bovendien geruststellen dat ze zich inzetten voor het beschermen van assets en het waarborgen van systemische stabiliteit. Toekomstbestendige cryptografie in deze sector vermindert zowel wettelijke blootstelling als het risico op reputatieschade.

Gezondheidszorg

Patiëntendossiers, genomdata en verbonden medische apparaten lopen allemaal risico bij 'harvest now, decrypt later'-aanvallen. De gezondheidszorg wordt daarnaast geconfronteerd met een extra uitdaging: de vereiste lange bewaartermijnen voor gevoelige medische data. Door vandaag te beginnen met de overstap naar PQC, zorgen ziekenhuizen en zorgverleners ervoor dat medische dossiers niet alleen nu, maar ook over tientallen jaren privé zijn en blijven. Dit is essentieel om het vertrouwen van patiënten te behouden en tegelijkertijd te voldoen aan de veranderende regelgeving inzake databescherming.

Overheid en kritieke infrastructuur

Van militaire communicatiesystemen tot energiedistributiesystemen, overheden en infrastructuurbeheerders vertrouwen op cryptografie voor de continuïteit van activiteiten en de nationale veiligheid. Post-kwantumcryptografie biedt niet alleen bescherming tegen kwaadwillenden op korte termijn, maar ook tegen het strategisch verzamelen van versleutelde communicatie voor toekomstig gebruik. Afstemming op kaders zoals CNSA 2.0 garandeert de interoperabiliteit, veiligheid en betrouwbaarheid van overheidssystemen in het kwantumtijdperk.

Bredere bedrijfsvoordelen

Hoewel de technische noodzaak van PQC duidelijk is, is de businesscase net zo sterk:

- Vertrouwen en merkreputatie: toont leiderschap in het beschermen van data van klanten en partners.
- Naleving van regelgeving: is afgestemd op NIST-standaarden en overheidsmandaten zoals CNSA 2.0.
- Operationele veerkracht: vermindert het risico op catastrofale storingen als gevolg van gebroken cryptografie.
- Onderscheiding ten opzichte van concurrentie: positioneert organisaties als proactieve innovators in plaats van reactieve volgers.

De voordelen van nu handelen reiken veel verder dan technische veerkracht. Organisaties die PQC vroegtijdig omarmen, beperken niet alleen risico's, maar versterken ook hun vermogen om te innoveren, te voldoen aan de regelgeving en te concurreren in een digitale economie die afhankelijk is van vertrouwen.

Zet de volgende stappen

De komst van kwantumcomputers biedt zowel een unieke kans als een ongekende uitdaging op het gebied van beveiliging. Hoewel het nog onzeker is wanneer kwantumcomputers cryptografisch relevant zullen worden, is het wel duidelijk dat er veel voorbereidingen nodig zijn. De overgang naar post-kwantumcryptografie zal jaren van gecoördineerde planning, investeringen en uitvoering vergen. Wachten totdat kwantumcomputers operationeel zijn, is geen praktische optie.

De eerste stap voor elke organisatie is bewustzijn: begrijpen waar en hoe cryptografie in hun omgeving wordt gebruikt. Vervolgens moeten ondernemingen beginnen met het inventariseren, prioriteren en testen van kwantumveilige oplossingen. Hybride cryptografie – een combinatie van klassieke en post-kwantumalgoritmen – biedt een snelle manier om veerkracht te creëren terwijl de standaarden zich blijven ontwikkelen. Door interne stappenplannen af te stemmen op wereldwijde kaders zoals de PQC-standaarden van NIST en de tijdlijnen in CNSA 2.0, kunnen organisaties vol vertrouwen werken aan naleving en interoperabiliteit.

Dell Technologies zet zich in om klanten te helpen bij deze overgang. Met onze aanpak bieden we een basis voor integriteit van de leveringsketen, in de hardware geïntegreerde beveiliging en aanpassingsvermogen met behulp van software. Onze partnerschappen met toonaangevende leveranciers van beveiligingsoplossingen en onze actieve rol in instanties voor industriestandaarden zorgen ervoor dat de oplossingen van Dell niet alleen voldoen aan de nieuwste vereisten, maar ook in de praktijk worden getest op prestaties en interoperabiliteit.

Begin vandaag nog met de voorbereiding. Begin met detectie en risicoanalyse, werk samen met vertrouwde leveranciers en test kwantumveilige technologieën. Elke stap die nu wordt genomen, vermindert het risico op verstoringen in de toekomst. Organisaties die in een vroeg stadium in actie komen, beveiligen niet alleen hun data en systemen, maar verdienen ook het vertrouwen van klanten, toezichhouders en partners in een tijdperk waarin digitaal vertrouwen van het grootste belang is.

Over ons

Dell Technologies streeft ernaar om geavanceerde technologie voor iedereen toegankelijk en betrouwbaar te maken en ervoor te zorgen dat iedereen dit kan benutten. We helpen mensen en organisaties om innovatie veilig te benutten en lopen voorop op weg naar een veiligere, inclusievere en meer verbonden toekomst.



Meer informatie over
Dell beveiligingsoplossingen



Neem contact op met een
Dell Technologies expert



Bekijk meer
informatiebronnen



Neem deel aan het
gesprek via #HashTag

Copyright © Dell Inc. Alle rechten voorbehouden. Dell Technologies, Dell en andere handelsmerken zijn handelsmerken van Dell Inc. of haar dochterondernemingen. Andere handelsmerken kunnen handelsmerken zijn van de desbetreffende eigenaren.