DE QUANTUMREVOLUTIE: WAAROM CIO'S NU MOETEN HANDELEN

Van harvest-now-risico's tot strategische kansen: zo bereidt u uw organisatie voor op het post-quantum tijdperk

Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | info@mxi.nl | www.mxi.nl

Richard Sitters
Karin Zwiggelaar

Quantum computing ontwikkelt zich van academische belofte naar strategische realiteit. Hoewel grootschalige, foutgecorrigeerde quantum-computers waarschijnlijk nog enkele jaren op zich laten wachten, heeft de technologie nu al directe gevolgen voor organisaties. De belangrijkste reden: de beveiliging van digitale communicatie en digitale identiteit leunt zwaar op cryptografie die, zoals nu gerealiseerd, in een post-quantum wereld kwetsbaar wordt.

Voor CIO's, CISO's en IT-management verschuift de vraag daarom van 'of' naar 'wanneer' en 'wat betekent dit voor de technologieroadmap'. Tegenstanders hoeven immers niet te wachten tot quantumcomputers operationeel zijn: versleutelde data kan vandaag worden buitgemaakt om later te worden ontcijferd ('harvest now, decrypt later'). Vooral informatie met een lange houdbaarheid, zoals medische data, contracten, intellectueel eigendom en vitale infrastructuur, verdient nu prioriteit.

In deze whitepaper schetsen we:

- wat quantum computing inhoudt;
- de bestuurlijke impact op cybersecurity en compliance;
- wat de transitie naar post-quantum cryptografie (PQC) in de praktijk vraagt en;
- waar quantum computing op termijn waarde kan toevoegen in optimalisatie en R&D van de organisatie;
- hoe organisaties de eerste stappen kunnen nemen voor quantum readiness.

Het doel is om inzicht te geven in waarom voorbereiden jaren kost en dus nu al moet beginnen.

WAT IS QUANTUM COMPUTING?

Quantum computing is een manier van rekenen die gebruikmaakt van principes uit de quantumfysica. Waar gewone computers werken met bits die de waarde 0 of 1 hebben, werken quantumcomputers met zogenaamde qubits. Die kunnen, sterk vereenvoudigd gezegd, meerdere toestanden tegelijk meenemen in een berekening. Daardoor kunnen quantumcomputers bepaalde complexe rekenproblemen op termijn veel sneller aanpakken dan klassieke computers.

Dat betekent niet dat quantumcomputers gewone computers vervangen. Ze zijn vooral relevant voor specifieke vraagstukken met zeer veel mogelijke combinaties, zoals optimalisatie, simulatie van moleculen en bepaalde wiskundige problemen. Juist dat laatste is belangrijk voor digitale veiligheid: een deel van de huidige cryptografie is gebaseerd op berekeningen die voor gewone computers praktisch onhaalbaar zijn, maar voor voldoende krachtige quantumcomputers wel mogelijk zijn waardoor de huidige cryptografie kwetsbaar kan worden.

Voor organisaties is quantum computing daarom tegelijk een kans en een risico. De kans zit in nieuwe mogelijkheden voor optimalisatie, onderzoek en innovatie. Het risico zit vooral in de impact op bestaande beveiliging, digitale identiteit en versleutelde communicatie. Daarom is het onderwerp nu al relevant voor CIO's, CISO's en bestuurders, ook al zijn grootschalige quantumcomputers nog niet breed beschikbaar.

IMPACT OP CYBERSECURITY

Quantum computing kan op termijn een doorbraak betekenen voor aanvallen op bepaalde vormen van publieke-sleutelcryptografie (zoals RSA en elliptic curve cryptografie (ECC)). In theorie maken quantum-algoritmen (zoals Shor[1]) het mogelijk deze constructies te breken, mits er voldoende stabiele, foutgecorrigeerde qubits beschikbaar zijn. Het punt voor organisaties is echter dat het risicovenster al openstaat: data die vandaag wordt onderschept en opgeslagen, kan later alsnog leesbaar worden.

Die tactiek heet "harvest now, decrypt later": kwaadwillenden verzamelen nu al versleutelde data met de intentie deze later te ontcijferen zodra de benodigde rekenkracht beschikbaar komt. Voor organisaties met gegevens die jarenlang vertrouwelijk moeten blijven, zoals medische dossiers, financiële data, contracten, intellectueel eigendom en gegevens rond vitale infrastructuur, maakt dit quantum security tot een onderwerp dat niet kan wachten tot 'de techniek er is'.

Dit raakt nadrukkelijk ook sectoren die onder NIS2 als essentieel of belangrijk worden aangemerkt (zoals energie, transport, bankwezen, digitale infrastructuur en zorg). Daar gaat het niet alleen om datalekken, maar om continuïteit, vertrouwen en maatschappelijke veiligheid. Quantum readiness hoort daarom thuis in risicomanagement, architectuurprincipes en leverancierssturing, niet alleen in de technische backlog.

De transitie naar quantum-veilige cryptografie (post-quantum cryptografie, PQC) is complex en tijdrovend. Grote technologiebedrijven (zoals Google, Apple, Microsoft, IBM, Amazon) testen inmiddels hybride varianten (klassiek + PQC) in protocollen en producten. Tegelijkertijd worden ook andere benaderingen onderzocht, zoals Quantum Key Distribution (QKD) voor het veilig uitwisselen van sleutels in specifieke netwerken. QKD kan waardevol zijn in niche-scenario's, maar voor de meeste organisaties is PQC de schaalbare route omdat het softwarematig in bestaande infrastructuur kan worden ingevoerd.

---

[1] Het algoritme van Shor is in 1994 ontwikkeld door Peter Shor en heeft aanzienlijke gevolgen voor de cryptografie en de beveiliging van moderne communicatiesystemen. De implementatie van het algoritme is momenteel nog beperkt door de huidige capaciteiten van quantum-computers.

Ook in Nederland wordt gewerkt aan quantum security, onder meer via samenwerkingen tussen kennisinstellingen en marktpartijen (zoals SURF, Quantum Delta NL en Q*Bird) in testomgevingen voor nieuwe technieken (zie [16], [17] en [18]). De rode draad: migratie kost jaren, terwijl de gevolgen van het verlies van vertrouwelijkheid of integriteit (reputatie, compliance, financiële schade) groot zijn. Vroege voorbereiding is daarom rationeel risicobeheer.

TRANSITIE NAAR POST-QUANTUM CRYPTOGRAFIE (PQC) IS URGENT

De overgang naar quantum-veilige cryptografie is urgenter geworden door het “harvest now, decrypt later”-risico en het feit dat migraties doorgaans jaren duren. Tijdlijnen voor krachtige quantumcomputers blijven onzeker, maar ontwikkelingen gaan snel. Voor bestuurders is vooral de doorlooptijd van de transitie relevant: cryptografische technologieën worden toegepast in applicaties, integraties, certificaten, apparaten, logging en leverancierssketens. Wachten op ‘meer zekerheid’ schuift het probleem vaak alleen vooruit.

Nederland ondersteunt deze transitie met praktische hulpmiddelen. Zo publiceerden AIVD, CWI en TNO een PQC Migration Handbook [12] met richtlijnen voor beleid, techniek en implementatie. Daarnaast is er tooling beschikbaar, zoals de PQChoiceAssistant [13], om keuzes te structureren. Een terugkerend principe in deze aanpak is crypto-agility: ontwerp systemen zó dat cryptografische algoritmen en parameters beheersbaar en tijdig te vervangen zijn.

NIST publiceerde de eerste set post-quantum cryptografiestandaarden [14]. Deze algoritmen zijn ontworpen om bestand te zijn tegen aanvallen door zowel klassieke als (toekomstige) quantumcomputers. Voor organisaties betekent dit dat pilots en migratieplanning niet langer op ‘conceptniveau’ hoeven te blijven: er is nu een concreet referentiekader om leveranciers op aan te spreken wat hun visie is en plannen zijn voor hun systemen en applicaties, en om implementaties gecontroleerd te testen.

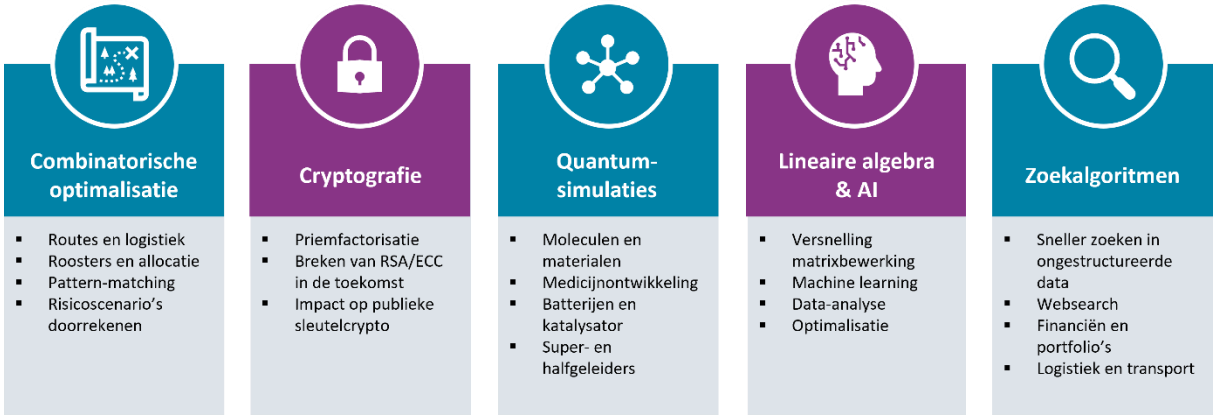
Een pragmatische implementatieaanpak bevat doorgaans de volgende bouwstenen:

- Start met een crypto-inventaris: waar worden encryptie, digitale handtekeningen, certificaten en key management gebruikt (ook in IAM en integraties)?
- Introduceer waar mogelijk hybride verbindingen (klassiek + PQC) en test performance, compatibiliteit en fallback-scenario’s in ketens.
- Maak certificaat- en sleutelbeheer PQC-ready: levenscycli, rotatie, HSM/KMS-ondersteuning, en eisen richting leveranciers en outsourcers.

Voor organisaties met gevoelige data, zoals zorg en vitale infrastructuur, loont het om nu te starten met prioritering op basis van ‘data-houdbaarheid’. Het “harvest now, decrypt later”-principe maakt immers dat uitstel vooral het risico naar de toekomst groter maakt. Gebruik beschikbare handreikingen en standaarden om de migratie naar quantum-veilige cryptografie beheersbaar te maken (zie o.a. [1], [12], [13], [15]): klein beginnen (kroonjuwelen en externe koppelingen), maar wel met een expliciete eindstaat en governance.

Type informatie	Benodigde vertrouwelijkheid	Implicatie
Identiteits- en certificaatdata (PKI, keys, signing)	Lang (5–20 jaar)	PQC-migratie vroeg starten; keten/leveranciers betrekken
Medische dossiers / sociaal domein	Zeer lang (10–30+ jaar)	Kroonjuwelen; encryptie én archieven beoordelen
Contracten / M&A / IP	Lang (5–15 jaar)	Bescherm 'nu' tegen later ontcijferen; prioriteer uitwisseling met derden
Operationele telemetrie/logging	Kort tot middellang	Focus op integriteit, herleidbaarheid en incidentrespons

Niet alleen bedreigingen maar ook kansen voor organisaties
De opkomst van quantum computing biedt organisaties ook mogelijkheden voor innovatie en optimalisatie, vaak via clouddiensten en experimenteerplatforms zoals D-Wave, waar we later bij de toepassingsgebieden nog op terugkomen. Het is daarbij verstandig om verwachtingen te managen: de eerste zakelijke waarde ontstaat vooral bij specifieke klassen problemen (optimalisatie, simulatie, bepaalde vormen van machine learning) en veelal in hybride combinaties met klassieke rekenkracht.



Figuur 1: Voor welk soort vraagstukken levert quantum computing een oplossing waar klassieke computers dat niet kunnen?

We bespreken hierna een aantal voorbeelden van ontwikkelingen op het gebied van quantum computing in verschillende sectoren en toepassingsgebieden.

Financiële sector

De financiële sector experimenteert relatief vroeg met quantum-algoritmen voor portfolio-optimalisatie, risico-modellering en fraudedetectie, vaak in samenwerking met grote technologie- en onderzoeksplatforms. Diverse banken en verzekeraars verkennen proof-of-concepts om rekenintensieve scenario-analyses te versnellen. De belangrijkste les voor CIO's: beoordeel claims kritisch, maar volg de ontwikkelingen bij kernleveranciers en onderzoeksconsortia, omdat de eerste toepasbare inzichten vaak juist daar ontstaan.

Toeleveringsketen en logistiek

In logistiek en supply chain ligt een van de meest genoemde toepassingsgebieden: optimalisatie van routes, planning en voorraden. In binnen- en buitenland lopen pilots waarin quantum- en quantum-inspired technieken worden verkend voor verkeersstromen, capaciteitsplanning en ketenoptimalisatie. Voor veel organisaties is dit een logisch startpunt: de waarde van enkele procenten efficiëntiewinst is vaak direct meetbaar in kosten, doorlooptijd en CO2-uitstoot.
Voorbeelden zijn routeplanning (ambulance-spreiding en prioritering, wijkzorg, afvalinzameling), maar ook bredere resource-allocatie: OK- en beddencapaciteit, personeelsroostering, wachtlijst-optimalisatie, ruimtelijke ordening en energiebeheer (smart grids, laadpaallocaties). De rode draad is steeds hetzelfde: veel variabelen, harde beperkingen en een grote impact van kleine verbeteringen.

Onderzoek en ontwikkeling

Quantum computing transformeert nu al R&D-processen in verschillende sectoren:

- versnelling van medicijnontwikkeling en gepersonaliseerde behandelingen in de farmaceutische industrie;
- op het gebied van materiaalonderzoek zoals de ontwikkeling van nieuwe batterijen en halfgeleiders en nanotechnologie;
- simulatie van moleculaire structuren in de chemische industrie.

Machine learning en AI

Onderzoek naar quantum machine learning richt zich op versnelling van specifieke berekeningen (vaak lineaire algebra) en op nieuwe modelvormen. De praktische relevantie verschilt per use-case en staat nog vroeg in ontwikkeling. Voor CIO's is het vooral een signaal om R&D-roadmaps te volgen en om te toetsen of leveranciers 'quantum-ready' innovaties vooral marketing zijn, of passen binnen een realistische uitvoeringsstrategie.
Vroeg experimenteren kan zinvol zijn, maar koppel het aan duidelijke selectiecriteria:

- Het probleem is aantoonbaar een optimalisatie- of simulatievraagstuk met veel variabelen,.
- Er is meetbare businesswaarde bij kleine verbeteringen, en.
- De organisatie kan de resultaten veilig en herhaalbaar integreren in bestaande processen.

Zet pilots daarom onder governance (architectuur, security, privacy) en voorkom 'quantum-hype' zonder businesscase.

Ontwikkeling van nieuwe beveiligingsmethoden

De ontwikkeling van quantum-veilige beveiligingsmethoden versnelt. Met de publicatie van NIST-standaarden en de opkomst van hybride implementaties in gangbare protocollen (zoals TLS) zetten meerdere leveranciers stappen richting PQC. Steeds meer producten en diensten bieden experimentele of gefaseerde ondersteuning. Voor organisaties is dit het moment om uit te vragen wat leveranciers ondersteunen, migratiepaden te plannen en te voorkomen dat security afhankelijk wordt van ad-hoc uitzonderingen.

Quantum annealing

Een specifieke vorm van quantum computing die al langer beschikbaar is, is quantum annealing. Deze techniek is minder algemeen inzetbaar dan universele quantumcomputers, maar kan geschikt zijn voor bepaalde optimalisatievraagstukken. In de praktijk worden annealers en 'quantum-geïnspireerde' algoritmen soms gecombineerd met klassieke rekenkracht. Voor CIO's is dit vooral relevant als experimenteerroute: kleine pilots kunnen inzicht geven in waar optimalisatie winst oplevert, zonder direct te wachten op grootschalige foutgecorrigeerde quantumcomputers.

D-Wave (Canada [19]) levert bijvoorbeeld quantum computers die gebaseerd zijn op quantum annealing en heeft deze computers al aan verschillende firma's verkocht (Google, Lockheed Martin, Volkswagen). Volkswagen gebruikt de machine om verkeersbewegingen in Beijing te optimaliseren, Lockheed Martin voor het ontwerp van nieuwe vliegtuigen en Google om machine learning van quantum computing mee te onderzoeken. Voor CIO's is het verstandig om deze voorbeelden te zien als 'proof-of-technology': interessant voor pilots en kennisopbouw, maar niet automatisch een blauwdruk voor grootschalige productie-inzet.

STRATEGISCHE ROADMAP VOOR QUANTUM READINESS

De voorbereiding van organisaties om klaar te zijn voor het quantumtijdperk vraagt een meerjarige aanpak, omdat cryptografie diep verweven is met applicaties, infrastructuur, leverancierssketens en governance. Een strategische roadmap helpt om de overgang naar quantum-veilige cryptografie beheersbaar te maken: eerst zicht krijgen op risico's en afhankelijkheden, daarna gericht testen, prioriteren en gefaseerd migreren.

Omdat quantumtechnologie en standaarden zich nog ontwikkelen, is een gefaseerde aanpak verstandig. Onderstaande stappen helpen om de eerste basis op orde te brengen en tegelijk ruimte te houden voor nieuwe standaarden en leveranciersontwikkelingen.

1. Quantum risico-analyse (zie ook kader 1 verderop in dit artikel)

- Prioriteer kroonjuwelen en de keten: identificeer kritieke bedrijfsprocessen, externe systemen met koppelingen naar buiten en leveranciers met toegang die kwetsbaar zijn voor quantum aanvallen.
- Label data op 'houdbaarheid': welke informatie moet over 5, 10, 20 jaar nog vertrouwelijk zijn?
- Analyseer de impact van quantum computing op huidige beveiligingsmaatregelen van extra vertrouwelijke, bedrijfs- of nationaal kritische informatie met een niet tijdelijk karakter die je opslaat in systemen die toegankelijk zijn vanaf of uitwisselt via openbare infrastructuren.
- Breng het "harvest now, decrypt later"-risico in kaart: welke verbindingen en datasets zijn onderschepbaar en wat is de vereiste vertrouwelijkheidstermijn?
- Evalueer compliance-vereisten vanuit NIS2 en andere regelgeving.

2. Inventarisatie van cryptografische assets (zie ook kader 1 verderop in dit artikel)

- Maak een compleet overzicht van alle cryptografische toepassingen: waar gebruikt de organisatie encryptie, signing, certificaten en key management, ook bij authenticatie en autorisatie (IAM) en in koppelingen met derden[2]?
- Identificeer gebruikte algoritmes en sleutellengtes[3].
- Documenteer certificaten en hun levenscyclus.

---

[22] Let op: signing, PKI en identiteit zijn vaak de lastigste migraties. Bij PQC gaat het niet alleen om versleutelde verbindingen (zoals TLS/VPN). Juist digitale handtekeningen en certificaatketens raken diep verweven onderdelen: code signing, firmware updates, device identities, S/MIME, documentondertekening en identiteitstoegang (IAM/PKI), API toegang/gebruik. Neem deze 'trust keten' expliciet mee in de inventarisatie, omdat vervanging hier vaak meer ketenimpact en langere doorlooptijd heeft dan bij alleen transport encryptie

[3] Binnen cryptografie wordt vaak onderscheid gemaakt tussen asymmetrische en symmetrische encryptie. Vooral asymmetrische encryptie is kwetsbaar voor quantumcomputers. Dat ligt aan het feit dat asymmetrische encryptie, zoals algoritmen als RSA en ECC, gebaseerd is op priemfactorisatie wat volledig te breken is met quantum computers. Symmetrische encryptie, zoals AES, loopt een kleiner risico. Een quantumcomputer kan het zoeken naar de juiste sleutel wel versnellen, maar dit risico is meestal te beperken door grotere sleutels te gebruiken. Daarom ligt bij quantum readiness de eerste focus op het in kaart brengen en vervangen van asymmetrische algoritmen..

3. Zet een PQC-strategie/migratiepad uit en herijk deze regelmatig

In deze strategie staan de stappen en beslissingen die een organisatie neemt om haar cryptografische infrastructuur toekomstbestendig te maken tegen quantumdreigingen. In zo'n strategie zijn naast de resultaten van de hiervoor genoemde risico-analyse en crypto-inventarisatie, de volgende onderdelen opgenomen:

- Een hybride migratieaanpak van crypto-maatregelen: implementeer een combinatie van klassieke en quantum-veilige algoritmes (hybride cryptografie) om een soepele overgang te waarborgen en compatibiliteit met bestaande systemen te behouden.

- Bepaal welke quantum-veilige algoritmes en standaarden uiteindelijk binnen de gehele organisatie zullen worden gehanteerd.

- Stel een haalbare planning op met heldere stappen en deadlines, bijvoorbeeld voor het testen, het stap voor stap uitfaseren van oude protocollen en de volledige implementatie van PQC-oplossingen.

- Pas beleid, architectuurprincipes en inkoopcriteria aan op PQC, met inachtneming van relevante wet- en regelgeving zoals NIS2.

- Start met proefprojecten en testmomenten om te waarborgen dat de nieuwe cryptografie daadwerkelijk veilig en werkbaar is voor de organisatie.

- Zorg voor duidelijke communicatie en training: licht de veranderingen toe aan medewerkers en leveranciers, zodat iedereen goed voorbereid is op de overgang.

- Organiseer een Q-day scenario in de vorm van een simulatiebijeenkomst. Q-day is het moment waarop een quantumcomputer bestaande publieke-sleutelcryptografie praktisch kan breken. Bespreek samen met IT, security, juridische experts, privacy-specialisten en bestuur stap voor stap hoe gereageerd zou worden op incidenten als gevolg van Q-day. Dit draagt bij aan het identificeren van mogelijke blinde vlekken, zonder onnodige paniek te veroorzaken.

- Maak PQC onderdeel van inkoop, contracten en leveranciersstering. Omdat cryptografie ketenbreed werkt, is post-quantum readiness zo sterk als de zwakste schakel. Neem daarom eisen op richting kernleveranciers (SaaS, netwerk, IAM/PKI, HSM/KMS, OT-leveranciers), bijvoorbeeld:
  - Welke NIST-PQC algoritmen worden ondersteund (nu en gepland), en vanaf wanneer?
  - Is hybride cryptografie beschikbaar (klassiek + PQC) en hoe is fallback/compatibiliteit geregeld?
  - Hoe borgen jullie crypto-agility (configureerbaarheid, rotatie, uitfasering) in product en implementatie?
  - Wat betekent PQC voor certificaten, signing en identity-flows (PKI/IAM), en welke migratiehulp bieden jullie?
  - Welke assurance leveren jullie (testresultaten, audits, roadmap, end-of-support voor klassieke algoritmen)?

Een effectief migratiepad naar quantum-veilige cryptografie is dus meer dan alleen techniek. Het vraagt om een integrale aanpak met aandacht voor processen, mensen en governance. Door vooraf helderheid te verschaffen over de gewenste eindsituatie en de tijdlijn, worden ad-hoc maatregelen voorkomen en ontstaat een duurzame beveiliging.

4. Identificeer kansen en potentiële toepassingsgebieden

Kijk niet alleen naar de risico's, maar ook naar de voordelen die quantum computing kan bieden voor de organisatie.

- Breng in kaart welke essentiële middelen in bedrijfsprocessen het verschil maken voor de organisatie en hoe deze samenhangen met andere processen. Quantum computing kan in bepaalde processen voor een betere, efficiëntere inzet van deze middelen zorgen dan gewone computers. Denk bijvoorbeeld aan scenario's waarin een 5% tot 10% hogere efficiëntie leidt tot minder doorlooptijd, lagere kosten of minder CO2-uitstoot.

- Quantum computing is al als dienst beschikbaar: organisaties kunnen capaciteit afnemen op basis van een abonnement. De meeste organisaties zullen zelf niet meteen de behoefte hebben om dit te doen, behalve organisaties die zelf inzetten op (onderzoek naar) de toepassingsgebieden die we hiervoor benoemen. Maar een gesprek met leveranciers van software diensten over wat hun visie en strategie op dit gebied is, kan wel van belang zijn. Ga in dat geval het gesprek met de leveranciers van de kernapplicaties binnen de relevante toepassingsgebieden aan over:
  - hoe zij kansen zien voor quantum computing;
  - hoe zij daarop inspelen (volger vs. visionair);
  - schat in wat hun uitvoeringskracht is (kunnen ze dit aantoonbaar leveren?);
  - inventariseer wat er op hun roadmap staat.

Hiermee zijn de eerste stappen gezet: zicht op risico's, inzicht in cryptografie en een richtinggevend migratiepad. Maak het vervolgens bestuurbaar met eenvoudige mijlpalen, zoals bijvoorbeeld % systemen in crypto-inventaris, % externe verbindingen 'hybride-ready', aantal kroonjuwelen gemigreerd en leveranciersdekking (welke kernleveranciers hebben een getoetste PQC-roadmap). Zo blijft het onderwerp concreet en kunt u tijdig bijsturen als standaarden, techniek of regelgeving veranderen.

CONCLUSIE EN AANBEVELINGEN

De transitie naar het quantumtijdperk vraagt een gebalanceerde aanpak: risico's tijdig mitigeren én kansen selectief verkennen. CIO's die nu starten met crypto-inventarisatie, prioritering op data-houdbaarheid en een realistisch PQC-migratiepad, vergroten de weerbaarheid van hun organisatie. Daarbij is leveranciersstering cruciaal: post-quantum readiness is zo sterk als de zwakste schakel in de keten.

Dat de eerste PQC-standaarden beschikbaar zijn en dat er handreikingen en tooling bestaan (zoals het PQC Migration Handbook [12] en de PQChoiceAssistant [13]) maakt het mogelijk om gestructureerd te beginnen. Wie nu een basis legt, governance, crypto-agility en ketenafspraken, voorkomt dat quantum security straks een haastklus wordt en creëert ruimte om technologische kansen verantwoord te benutten.

Kader 1: Quantum computing risico analyse - NIS2/BIO

Quantum computing vormt op dit moment geen bedreiging voor correct toegepaste symmetrische encryptie (AES 256). Quantum computers vormen géén existentiële bedreiging voor moderne symmetrische encryptie zoals AES 256, zolang voldoende sleutelgroottes worden gebruikt.
De grootste impact raakt asymmetrische cryptografie zoals die worden gebruikt voor certificaten en sleuteluitwisseling (bv RSA en ECC).
NIS2 (artikel 21 - **noot 1**) en BIO (controls 9.4.1, 9.4.3 en 6.1 - **noot 2**) vereisen geen directe overstap naar post quantum cryptografie, maar wel aantoonbaar risicobewustzijn, modern sleutelbeheer en een toekomstgerichte cryptografiestrategie. Risicobewustzijn inzake lange termijn data (harvest now, decrypt later) die is opgeslagen met asymmetrische versleuteling en maatregelen voor certificaten en sleuteluitwisseling omdat daar vaak asymmetrische algoritmen voor worden gebruikt. Concreet:

- quantum computing is geen showstopper voor AES, mits AES-256 wordt toegepast, geen AES-128 (128 bit keylengte is te kort). AES is een symmetrisch algoritme;
- de focus moet zijn op het vervangen van asymmetrische algoritmen. Deze worden gebruikt bij de volgende toepassingen waar het echte risico bij zit, t.w.
  - digitale handtekeningen (PKI, certificaten, identiteiten);
  - sleuteluitwisseling;
  - opgeslagen sessies en data die zijn versleuteld met asymmetrische algoritmen.

Een hybride migratieaanpak van crypto-maatregelen helpt om de risico's te managen. Daarbij implementeert de organisatie een combinatie van klassieke en quantum-veilige algoritmes (hybride cryptografie) om een soepele overgang te waarborgen en compatibiliteit met bestaande systemen te behouden. Bij hybride cryptografie wordt een beveiliging pas als geldig beschouwd als beide algoritmen veilig zijn.

Concreet voorbeeld: sleutelaanmaak (key exchange). Stel je bouwt een beveiligde verbinding (zoals TLS/VPN):

- klassiek algoritme (bijv. ECC);
- quantum-veilig algoritme (bijv. CRYSTALS-Kyber).

De uiteindelijke geheime sleutel = combinatie van beide resultaten. Als de klassieke cryptografie wordt gebroken dan blijft de verbinding veilig dankzij het veilige quantum deel. Als het quantum veilige algoritme een zwakte heeft dan beschermt het klassieke deel nog (als het quantum deel is gebroken dan moet ook nog het klassieke deel worden gebroken).

Noot 1:

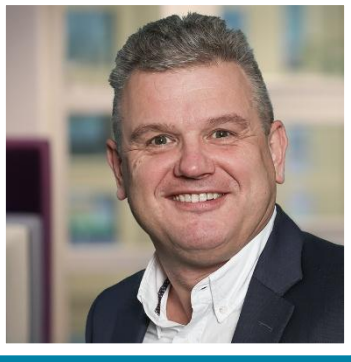
- artikel 21 – organisaties dienen passende technische maatregelen te nemen om risico's voor netwerk- en informatiesystemen te beheersen.

Noot 2:

- 9.4.1 – gebruik van cryptografie. Cryptografie moet passend zijn aan dreigementen. à AES-256 geldt als toekomstvast;
- 9.4.3 – hier ligt het grootste risico. BIO verwacht sleutelrotatie (regelmatig vervangen van sleutels), veilige sleutelopslag en sleutelopslag gescheiden van data. Vervang dus regelmatig sleutels (beleidsmaatregel en controle op uitvoering) en maak gebruik van voldoende grote sleutels.

MEER INFORMATIE?

Heeft u vragen, wilt u meer weten over dit onderwerp? Neem dan contact op met Richard Sitters of Karin Zwiggelaar.



richard.sitters@mxi.nl
06 30 71 84 19

karin.zwiggelaar@mxi.nl
06 51 54 01 54

BRONNEN

1 Digitale Overheid. “Bereid je voor op quantumveilige cryptografie.” https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/bereid-je-voor/
2 NIST (National Institute of Standards and Technology). “Quantum computing explained.”
3 https://www.nist.gov/quantum-information-science/quantum-computing-explained
4 Harvard Business Review. “Quantum Computing for Business Leaders” (2022). https://hbr.org/2022/01/quantum-computing-for-business-leaders
5 Quantum Zeitgeist. “Quantum computing for business: real-world use cases.” https://quantumzeitgeist.com/quantum-computing-for-business-real-world-use-cases/
6 Veritis. “Top applications of quantum computing.” https://www.veritis.com/blog/top-applications-of-quantum-computing/
7 World Economic Forum. “Quantum technology and business” (2025). https://www.weforum.org/stories/2025/01/quantum-technology-business/
8 TechTarget (SearchCIO). “Quantum computing in business applications is coming.” https://www.techtarget.com/searchcio/feature/Quantum-computing-in-business-applications-is-coming
9 The Quantum Insider. “Quantum industry explained: applications, innovations, challenges” (2024). https://thequantuminsider.com/2024/02/05/quantum-industry-explained-applications-innovations-challenges/
10 TNO. “Quantum computing.” https://www.tno.nl/en/digital/digital-innovations/trusted-ict/quantum-computing/
11 MIT Sloan Management Review. “The business case for quantum computing.” https://sloanreview.mit.edu/article/the-business-case-for-quantum-computing/
12 The Quantum Insider. “Quantum computing applications” (2023). https://thequantuminsider.com/2023/05/24/quantum-computing-applications/

13 AIVD, CWI en TNO. “Het PQC-migratie handboek. Richtlijnen voor het migreren naar post-quantumcryptografie” (2024). https://www.aivd.nl/documenten/2024/12/3/het-pqc-migratie-handboek
14 TNO. “PQChoiceAssistant” (tool; GitHub). https://github.com/TNO/PQChoiceAssistant
15 NIST (National Institute of Standards and Technology). “Post-Quantum Cryptography” (CSRC project). https://csrc.nist.gov/projects/post-quantum-cryptography
16 Europese Unie. “Richtlijn (EU) 2022/2555 (NIS2)” (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
17 Quantum Delta NL. Officiële website. https://quantumdelta.nl/
18 SURF. “Hoe Quantum Key Distribution de beveiliging verbetert: call voor co-creatie” (2024). https://www.surf.nl/artikel/hoe-quantum-key-distribution-de-beveiliging-verbetert-call-voor-co-creatie
19 Q*Bird. Officiële website. https://q-bird.com/
20 D-Wave Quantum. Officiële website. https://www.dwavequantum.com/