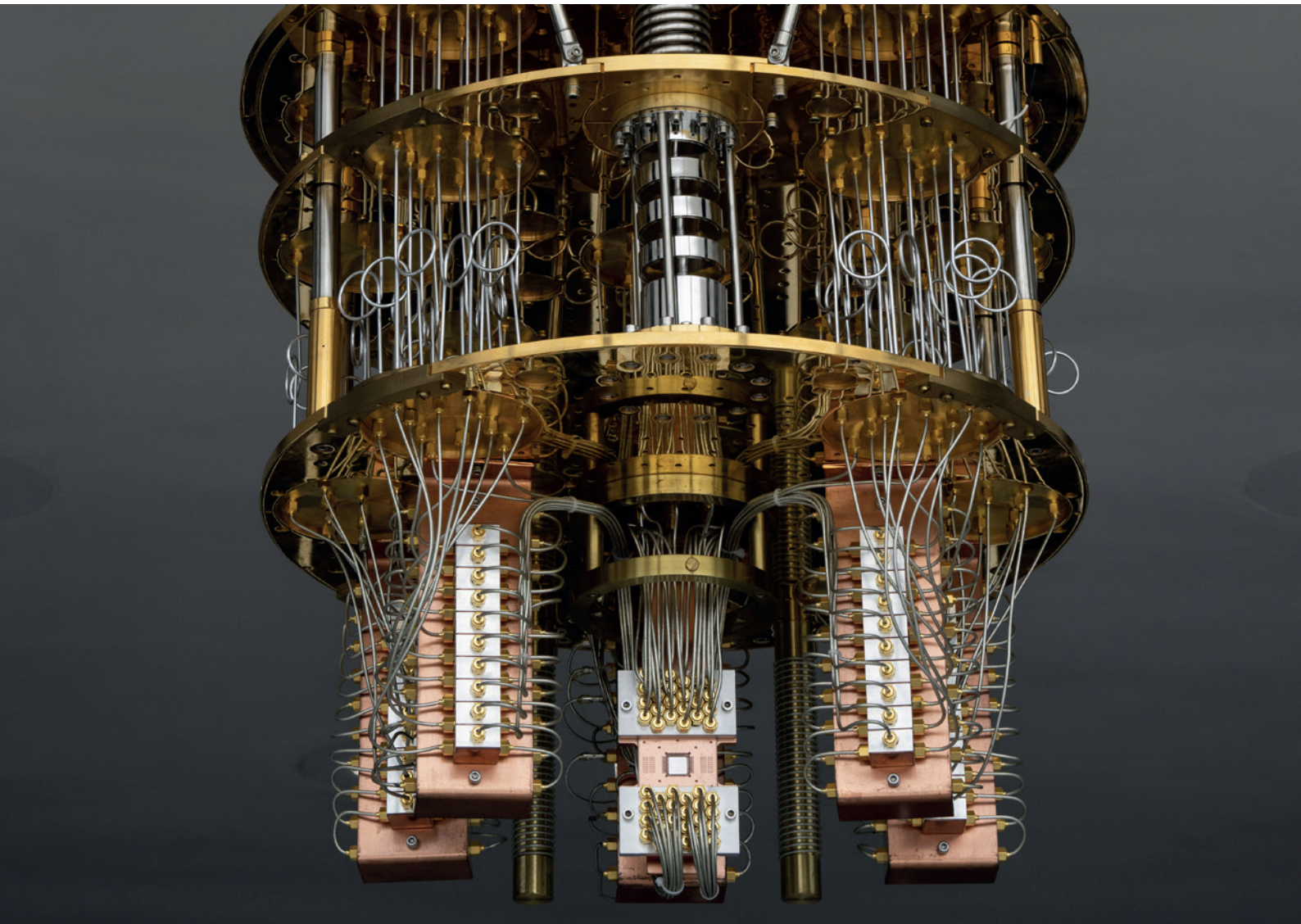
Maak je organisatie quantumveilig

Een handreiking voor het maken van een risicoanalyse en migratieplanning



AIVD

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) beschermt de democratie tegen nationale en internationale dreigingen, zodat we in vrijheid kunnen leven. We waken, vaak onzichtbaar, over Nederland en zijn bevolking. We doen daarvoor onderzoek in binnen- en buitenland. De AIVD doet wat nodig is om te voorkomen dat staten, organisaties of personen onze rechtsstaat tegenwerken, ondergraven of aanvallen. Ons werk doen we niet alleen. De AIVD heeft zijn eigen rol in het netwerk van overheidsorganisaties die de veiligheid van Nederland beschermen. De AIVD is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

NCSC

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving. Daarnaast heeft zij als doel de vitale infrastructuur en Rijksoverheid van Nederland te beschermen door de digitale weerbaarheid van Nederland te vergroten en de gevolgen van cyberincidenten te beperken.

Doelgroep

Deze handreiking is geschreven voor personen die een belangrijke rol spelen bij het voorbereiden op de migratie naar nieuwe standaarden en een verantwoordelijkheid hebben bij het opstellen en uitvoeren van een migratieplan. Dit zijn in de eerste plaats CIO's, CTO's en CISO's. Daarnaast kan deze handreiking mogelijk ook interessant zijn om te lezen voor (crypto)beheerders en ICT- en security-architecten.

Aan deze handreiking hebben bijgedragen

Anita Wehmann (MinBZK), Oscar Koeroo (departementaal CISO MinVWS), Thomas Attema (CWI/TNO), Vincent Dunning (TNO) en medewerkers van de Nederlandse vereniging van Banken en van KPN CISO Office.

Inleiding

De ontwikkeling van een krachtige quantumcomputer is de laatste jaren in een stroomversnelling geraakt. Het algemene beeld onder experts is dat quantumcomputers tussen 2030 en 2040 waarschijnlijk over voldoende rekenkracht zullen beschikken om veel van de meest gebruikte cryptografische algoritmen te kunnen breken. Cryptografie vormt een belangrijk fundament voor informatiebeveiliging. De komst van een krachtige quantumcomputer kan daarom aanzienlijke beveiligingsrisico's voor organisaties opleveren waardoor de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en processen risico loopt.

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Nationaal Cyber Security Centrum (NCSC) hebben sinds 2014 verschillende publicaties uitgebracht om organisaties te informeren over deze risico's.[1] Het is nu tijd dat organisaties in actie komen en zich gaan voorbereiden op de migratie naar quantumveilige cryptografie. De AIVD en het NCSC hebben daarom deze handreiking gemaakt voor CIO's, CTO's en CISO's van de overheid, het bedrijfsleven en kennisinstellingen.

1 Zie: "Informatieblad over quantumcomputers", AIVD, 2014, https://www.aivd.nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers; "Factsheet postkwantumcryptografie", NCSC, 2019, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-postkwantumcryptografie; en
"Bereid je voor op de dreiging van quantumcomputers", AIVD, 2021, https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.

Aan de slag met het voorbereiden op de migratie naar quantumveilige cryptografie

De migratie naar quantumveilige cryptografie/post-quantumcryptografie (PQC)[2] is een complexe opgave en zal organisaties veel tijd en middelen gaan kosten. Het is daarom belangrijk om nu al te beginnen met voorbereiden op migratie om je organisatie tijdig te beschermen tegen de dreiging van de quantumcomputer. Deze handreiking biedt een aantal concrete handvatten voor:

- Het inventariseren van de risico's die een organisatie loopt met de quantumdreiging;
- Het inventariseren van de cryptomiddelen die een organisatie gebruikt;
- Het beoordelen van de risico's;
- Het opstellen van een migratieplan.

Ook wordt kort ingegaan op de dreiging van de quantumcomputer en op een aantal concrete acties die je nu al kunt ondernemen. Dat zijn de zogeheten *no regret*-maatregelen (maatregelen die hoe dan ook van waarde zijn voor jouw organisatie). Tot slot wordt ingegaan op ontwikkelingen over de komst van de quantumcomputer voor de periode 2023-2024 zoals weergegeven in Tabel 1. Deze handreiking is een aanvulling op het recent gepubliceerde PQC-migratiehandboek[3] en geeft een nadere uitwerking van de in het handboek beschreven stappen waar organisaties nu mee aan de slag moeten (inventarisatie en planning).

De urgentie om te migreren is voor iedere organisatie anders. Sommige organisaties kunnen niet wachten op post-quantumcryptografiestandaarden, die naar verwachting vanaf 2024 beschikbaar komen, omdat hun data nu al quantumveilig moeten zijn. Andere organisaties hebben juist voordeel bij het wachten op het beschikbaar komen van nieuwe quantumveilige cryptografische standaarden. De urgentie en snelheid om te migreren is afhankelijk van het risicoprofiel van de organisatie. Voor alle organisaties geldt dat het belangrijk is om een specifieke risicoanalyse voor de quantumdreiging uit te voeren en te beginnen met het voorbereiden op de migratie naar quantumveilige cryptografie.

2 Met post-quantumcryptografie (PQC) wordt de cryptografie bedoeld die bestand is tegen de dreiging van de quantumcomputer. De definitie van PQC is echter niet eenduidig. Volgens sommige definities omvat PQC bijvoorbeeld geen symmetrische cryptografie, zoals AES. In deze handreiking refereren we met quantumveilige cryptografie aan zowel asymmetrische als symmetrische cryptografie die weerbaar is tegen de dreiging van de quantumcomputer.

3 Zie: "Het PQC-migratie handboek", TNO, CWI en AIVD, 2023, https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek.

Tabel 1: Een overzicht van de belangrijkste dreigingen, het handelingsperspectief en de verwachte ontwikkelingen op het gebied van quantumveilige cryptografie.

	Nu van toepassing (2023-2024)	Toekomst (2025-2035)
Dreigingen	- Het '*store now, decrypt later*'-scenario.	- Aantasting van de integriteit van digitale handtekeningen. - Aantasting van de betrouwbaarheid en integriteit van data en systemen.
Handelingsperspectief	- Het uitvoeren van een risico-analyse, het inventariseren van cryptomiddelen en het voorbereiden op migratie door het opstellen van een migratieplan. - Het treffen van *no regret*-maatregelen.	- Het daadwerkelijk uitvoeren van migratietrajecten.
Externe ontwikkelingen	- Het beschikbaar komen van nieuwe PQC-standaarden (NIST). - De ontwikkeling van nieuwe software (bijvoorbeeld voor inventarisatie en asset *management*).	- Inbedding van nieuwe standaarden in producten. - De ontwikkeling van aanvullende handvatten en *best practices* t.a.v. migratie. - Grootschalige migratietrajecten (bijvoorbeeld internetstandaarden).

De dreiging toegelicht

Het is onwaarschijnlijk dat er op dit moment al quantumcomputers bestaan die over voldoende rekenkracht beschikken om een serieuze bedreiging te vormen voor de huidige cryptografie. Het is niet met zekerheid te voorspellen op welk moment quantumcomputers ingezet kunnen worden om enkele van de meest gebruikte vormen van cryptografie te breken. Zo kan een doorbraak ervoor zorgen dat er sneller dan verwacht een krachtige quantumcomputer ontwikkeld wordt. Ook kunnen er bijvoorbeeld nieuwe quantumalgoritmen ontwikkeld worden die met beperkte rekenkracht een bedreiging vormen voor cryptografische algoritmen.

Op basis van de huidige inzichten vormt het '*store now, decrypt later*'-scenario de meest urgente dreiging voor organisaties. Kwaadwillende actoren zouden nu al versleutelde data van hun doelwitten kunnen verzamelen om deze data op een later moment, als de quantumcomputer over voldoende rekenkracht beschikt, te ontsleutelen. Deze dreiging gaat nu vooral uit van statelijke actoren, omdat deze over de intentie en vereiste middelen beschikken om dergelijke aanvallen uit te kunnen voeren. Organisaties die over gevoelige data beschikken die ook na de komst van de quantumcomputer nog vertrouwelijk

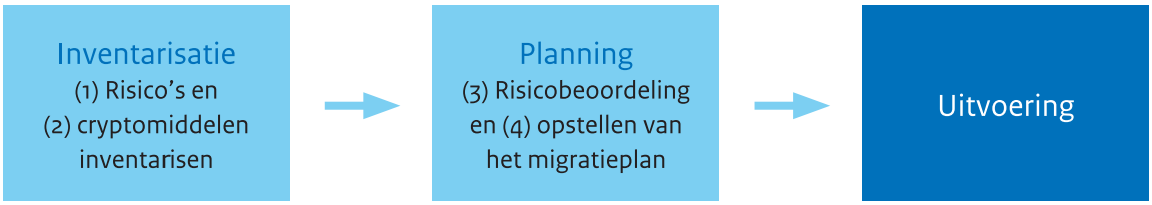
moet zijn, moeten daarom nu al aanvullende maatregelen treffen om zich te beschermen tegen de reële dreiging van de quantumcomputer.

Zoals Tabel 1 laat zien, zijn er nog meer relevante dreigingen om rekening mee te houden. Zo zijn er ook risico's voor processen die gebruikmaken van authenticatie- of autorisatiesystemen, of waarvoor het tekenen en verifiëren van digitale handtekeningen vereist is. Deze dreigingen liggen misschien verder in de toekomst, maar dit neemt niet weg dat alle organisaties nu al aan de slag moeten met het voorbereiden op migreren naar quantumveilige cryptografie.

Voorbereiden op migratie

De migratie naar quantumveilige cryptografie kent complexe uitdagingen die veel tijd, planning en voorbereiding zullen vragen.[4] Organisaties die te laat starten met de voorbereidingen om te migreren naar quantumveilige cryptografie, lopen het risico niet op tijd beschermd te zijn tegen de dreiging van de quantumcomputer. Het is daarom belangrijk om op een gestructureerde en effectieve manier tijd en middelen hiervoor beschikbaar te maken en in te zetten in je organisatie.

Figuur 1: In deze handreiking worden handvatten geboden voor het inventariseren van risico's en cryptomiddelen, het beoordelen van risico's en het opstellen van het moooigratieplan.



Het structureren en prioriteren van te nemen stappen hangt nauw samen met het beoordelen en beheersen van de specifieke risico's die een organisatie loopt door de quantumdreiging. Zorg er daarom voor dat jouw organisatie een bestaand en doorlopend risicomanagementproces heeft.[5] Gebruik dit proces om de belangrijkste te beschermen belangen in kaart te brengen en een beeld te schetsen bij de bestaande organisatiebrede risico's. Dit helpt je om de risico's die gepaard gaan met de quantumdreiging beter te kunnen duiden en prioriteiten te stellen voor acties die nodig zijn in de (voorbereiding op) migratie.

4 Zelfs met een enkele vercijferingsstandaard kan migratie lang duren. Zo was er bijvoorbeeld meer dan vijf jaar nodig om van SHA-1 naar SHA-256 te migreren, terwijl de specificaties en implementaties al beschikbaar waren. De migratie naar quantumveilige cryptografie is vele malen complexer en omvangrijker en vergt daarom naar verwachting veel tijd en inzet.

5 Zie: "Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt", NCSC, 2023, https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing.

In de volgende hoofdstukken geven we handvatten die je kunt gebruiken om specifieke risico's voor de quantumdreiging op te nemen in je bestaande risicomanagementproces. Deze handvatten bestaan uit:

1. Het bepalen of, en zo ja welke, onderdelen van jouw organisatie een verhoogd risico lopen met de huidige quantumdreiging en de belangrijkste te beschermen belangen van je organisatie;
2. Het in kaart brengen van jouw beveiligingsmaatregelen voor de te beschermen belangen die gebruikmaken van cryptografie;
3. Het beoordelen en prioriteren van risico's;
4. Het beheersen van deze risico's door een migratieplan op te stellen en maatregelen te nemen die de weerbaarheid van jouw organisatie nu al verhogen.

1. Maak risico's inzichtelijk

De risico's die jouw organisatie loopt, hangen samen met de belangen die je beschermt en de intenties van een actor die over een krachtige quantumcomputer beschikt. De eerste stap in het opstellen van jouw migratieplan is zicht krijgen op potentiële risico's. Op basis van de huidige kennis over de quantumdreiging adviseren we om in je risicoanalyse rekening te houden met de volgende uitgangspunten:[6]

- In eerste instantie zullen waarschijnlijk alleen geavanceerde (statelijke) actoren over een quantumcomputer beschikken die krachtig genoeg is om de huidige cryptografische algoritmen te breken. Als jouw organisatie of een van je ketenpartners, afnemers of leveranciers een mogelijk doelwit vormt voor statelijke actoren, dan kan de komst van de quantumcomputer een dreiging voor jouw organisatie vormen.[7]

- Op dit moment vormt de inbreuk op vertrouwelijkheid van gegevens de meest reële en actuele dreiging. Andere dreigingen, zoals de inbreuk op authenticatie- en autorisatiesystemen, worden relevant op het moment dat een krachtige quantumcomputer beschikbaar komt. Breng daarom in je risicoanalyse processen, systemen en infrastructuren in kaart waarmee gevoelige of vertrouwelijke informatie wordt opgeslagen, bewerkt of getransporteerd. Houd hierbij met name rekening met informatie die ook na de komst van de quantumcomputer nog vertrouwelijk moet blijven.

- Vervang je, of schaf je binnenkort systemen aan die een langere levensduur kennen, zoals ICS/SCADA-systemen? Dan is het aannemelijk dat deze systemen nog binnen hun huidige levensduur te maken krijgen met de komst van een krachtige quantumcomputer. Hierdoor zullen deze systemen niet alleen te maken krijgen met '*store now, decrypt later*'-dreigingen, maar bijvoorbeeld ook met de inbreuk op authenticatie- en autorisatiesystemen. Neem daarom ook voor de aankoop- of vervangingstrajecten van dergelijke systemen de quantumdreiging in je risicoanalyse mee.

6 Zie voor aanvullende informatie hoofdstuk 2 van het PQC-migratiehandboek.

7 Zie voor aanvullende informatie: "Dreigingsbeeld Statelijke Actoren (DBSA 2)", AIVD, 2022, https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2.

2. Beheer een overzicht van de gebruikte cryptomiddelen (crypto-asset management)

Het belang van overzicht

Cryptomiddelen zijn alle (beveiligings)maatregelen die gebruikmaken van cryptografie. Een overzicht van jouw cryptografische middelen is onmisbaar bij het opzetten van een gestructureerd en effectief migratieplan. In bredere zin helpt een actueel en accuraat overzicht om mogelijke kwetsbaarheden in jouw huidige security-architectuur te monitoren en snel op te lossen als er bijvoorbeeld kwetsbaarheden gevonden worden in een algoritme of softwarebibliotheken. Het bijhouden van een inventaris is daarom niet alleen belangrijk met het oog op migreren naar quantumveilige cryptografie, maar vormt in brede zin een essentieel onderdeel van je asset management.

Het daadwerkelijke risico dat jouw organisatie loopt, hangt af van de beveiligingsmaatregelen die zijn getroffen en hoe die gebruikmaken van cryptografie. Met een actueel en accuraat overzicht van de gebruikte cryptografische middelen krijg je hier zicht op. Het maken van dit overzicht kan een uitdagende opgave zijn. We adviseren om deze inventarisatie in eerste instantie uit te voeren voor de te beschermen belangen die volgens de eerste stap van de risicoanalyse een verhoogd risico lopen door de quantumdreiging.

We raden aan om iemand namens het management of bestuur verantwoordelijk te maken voor het beheren (en up-to-date houden) van het overzicht van gebruikte cryptomiddelen. Dit kan bijvoorbeeld de cryptobeheerder van jouw organisatie zijn. In veel gevallen zal deze het overzicht handmatig moeten opstellen en beheren in samenwerking met jouw leveranciers en technische specialisten. Op dit moment wordt er software ontwikkeld waarmee in de nabije toekomst semiautomatisch een overzicht gemaakt kan worden. De CISO is doorgaans namens het management of bestuur de verantwoordelijke persoon om ervoor te zorgen dat dit overzicht gedeeld en geduid kan worden binnen de gehele organisatie.

Voor het vastleggen van de cryptomiddelen binnen jouw organisatie kan gebruik gemaakt worden van een *Cryptographic Bill of Materials* (CBOM). Dit is een afgeleide van de bekendere *Software Bill of Materials* (SBOM) die de cryptomiddelen en hun afhankelijkheden beschrijft. Leg hierbij onder andere het volgende vast:

- De gebruikte vormen van cryptografische algoritmen en protocollen (type, versie);
- De gebruikte cryptografische materialen (bijvoorbeeld certificaten met bijbehorende verloopdata en sleutellengtes);
- De betrokken fysieke systemen (bijvoorbeeld servers, informatiesystemen, smartcards);
- De afhankelijkheden van andere systemen of data (bijvoorbeeld open source-bibliotheken);
- Je afhankelijkheden van derde partijen - bijvoorbeeld de leverancier van het systeem en de bijbehorende afspraken - voor ingekochte (*closed source* en *open source*) hardware of software.

Maak hierbij ook inzichtelijk welk doel de gebruikte cryptografie heeft. Moet deze bijvoorbeeld de gegevens beschermen of vormt het een onderdeel van een autorisatiesysteem? Maak daarbij de koppeling tussen deze cryptomiddelen en je te beschermen belangen. Hiermee kan je bepalen in welke mate en welk (kritiek) deel van je organisatie risico loopt.

Zie *crypto-asset management* als onderdeel van een bredere *asset management*-strategie. Leg bijvoorbeeld de koppeling tussen jouw CBOM- en SBOM-inventarissen en maak cryptomiddelen onderdeel van jouw Configuration Management Database (CMDB). Zorg er tot slot voor dat je jouw inventarissen op een passende manier beveiligt.

Het belang van *crypto-agility*

Er is sprake van *crypto-agility* als cryptografische protocollen, producten en systemen zodanig worden geïmplementeerd dat de betrokken cryptografische algoritmen met minimale inspanning kunnen worden gewijzigd. Zo zal een modulair systeem dat gebruikmaakt van softwarematige cryptografische algoritmen meer *crypto-agile* zijn dan een gespecialiseerd hardware systeem. *Crypto-agility* is een inrichting- en ontwerpkeuze van systemen, waarbij ondersteuning vanuit personen of processen nodig is.

We adviseren ervoor te zorgen dat (nieuwe) systemen voldoende *crypto-agile* zijn, op basis van je risicoanalyse. Dit houdt in dat er een redelijke verwachting is dat deze systemen binnen hun levensduur aangepast kunnen worden bij ontwikkelingen van de quantumdreiging, zoals de ontdekking van kwetsbaarheden in cryptografische (quantumveilige) algoritmen. De vereiste mate van *crypto-agility* is daarbij afhankelijk van de toepassing. Op dit moment is er geen generiek voorschrift van eisen beschikbaar waaraan een *crypto-agile* systeem moet voldoen. We adviseren je om alvast met jouw leveranciers in gesprek te gaan om je behoefte voor *crypto-agility* kenbaar te maken.

3. Beoordeel risico's

Met behulp van een risicoanalyse kun je bepalen in welke mate je beveiligingsmaatregelen die gebruikmaken van cryptografie, risico lopen door de komst van de quantumcomputer. Cryptografie is doorgaans onderdeel van een breder pakket van beveiligingsmaatregelen. De risico's die jouw organisatie loopt, zijn daarom ook afhankelijk van de manier waarop deze beveiligingsmaatregelen ingezet worden. In bepaalde situaties - zoals het transport van informatie - is cryptografie soms de enige beveiligingsmaatregel tegen *man-in-the-middle*-aanvallen. Mocht de beveiliging van kritieke processen of infrastructuren binnen je organisatie sterk steunen op cryptografische algoritmen, dan verdienen deze extra aandacht bij het opstellen van een migratieplan.

Beoordeel de uitkomsten van de risicoanalyse op de volgende factoren:

- De dreiging;
- De te beschermen belangen;
- De beveiligingsmaatregelen die cruciaal zijn voor het beschermen van deze belangen;
- De cryptografische algoritmen waar deze beveiligingsmaatregelen op steunen.

4. Stel je migratieplan op

Met de uitkomsten van de risicoanalyse, kun je een migratieplan opstellen dat aansluit bij de behoefte van jouw organisatie. Hieruit wordt duidelijk binnen welke tijdslijnen de migratie moet gebeuren, welke acties prioriteit hebben en met welke urgentie (nu al) onderdelen van de organisatie quantumveilig gemaakt moeten worden.

Er bestaan verschillende mitigatiestrategieën om je organisatie quantumveilig te maken. Denk hierbij bijvoorbeeld aan het migreren van de gebruikte cryptografie, aanvullende (fysieke) segmentatie of het isoleren van systemen. In de meeste gevallen heeft wachten op het beschikbaar komen van quantumveilige standaarden voor migratie de voorkeur, omdat het implementeren van deze nieuwe standaarden het minste impact zal hebben op de bedrijfsvoering. In aanvulling hierop adviseren we ook om een aantal concrete *no regret*-maatregelen op te nemen in je migratieplan. Op basis van de eerder beschreven stappen kun je de tijdslijnen waarbinnen jouw organisatie deze migratieactiviteiten moet uitvoeren, concreet maken.

No regret-maatregelen en *early adoption*

Er zijn een aantal *no regret*-maatregelen die je nu al kunt opnemen in je migratieplan en die weinig risico voor de huidige bedrijfsvoering zullen opleveren. Zo kun je ervoor zorgen dat de door jou gebruikte cryptografische protocollen, zoals TLS, gebruikmaken van de meest recente versie (TLS1.3).[8] Het is waarschijnlijk dat nieuwe quantumveilige standaarden alleen ingebed zullen worden in de recentste versie. Door nu al voorbereidende stappen te ondernemen en gebruik te maken van de meest actuele cryptografische protocollen, zorg je ervoor dat de migratie soepeler verloopt.[9]

We adviseren ook om de sleutellengte te verdubbelen bij het gebruik van symmetrische cryptografie. De huidige consensus is dat dit voldoende is om de quantumdreiging te mitigeren. Voor asymmetrische algoritmen is het advies om het standaardisatietraject van NIST af te wachten (zie ook het kopje ‘Vooruitblik’).

Heeft jouw organisatie een zeer hoge urgentie om te migreren, en kan deze daarom niet wachten op de standaarden voor quantumveilige cryptografie? Overweeg dan nu al het gebruik van hybride oplossingen, waarbij er gebruikgemaakt wordt van een combinatie van bestaande cryptografische standaarden en (kandidaat) PQC-algoritmen.[10]

8 Zie voor aanvullende informatie: “ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)”, NCSC, 2021, https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1.

9 Zie: “Guidelines for quantum-safe transport-layer encryption”, NCSC, 2022, https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption.

10 Zie hoofdstuk 4.1 van het PQC-migratiehandboek voor meer informatie over de migratie van symmetrische en asymmetrische algoritmen (inclusief hybride oplossingen).

We adviseren de CISO om binnen de organisatie, de afdeling of het departement iemand aan te stellen die helpt bij het opstellen en (laten) uitvoeren van het migratieplan. De CISO blijft namens het management of bestuur eindverantwoordelijk voor het uiteindelijke migratieplan. Deze persoon hoeft zelf geen cryptografisch expert te zijn, maar moet wel begrijpen waar en waarom cryptografische principes gebruikt worden, wat er mis kan gaan als deze protocollen gebroken worden en wat afhankelijkheden tussen systemen betekenen voor de (kritieke) bedrijfsvoering. De aangewezen persoon onderhoudt ook het contact met de diverse stakeholders, betrekt ze op het juiste moment en koppelt belangrijke bevindingen terug aan de CISO. Daarnaast heeft de aangewezen persoon zicht op de (technische) ontwikkelingen en mogelijkheden op het gebied van cryptografie. De aangewezen persoon zal in de praktijk doorgaans een rol hebben als enterprise- of security-architect of securityadviseur. Voor het coördineren van de daadwerkelijke uitvoering kan het daarnaast lonen om een projectleider aan te stellen.

Migreer in samenspel met je stakeholders

Voor de migratie naar quantumveilige cryptografie zal je afhankelijk zijn van verschillende stakeholders. De communicatie met deze stakeholders is belangrijk voor de beveiliging en interoperabiliteit tussen diensten. Hieronder worden de belangrijkste stakeholders genoemd en wordt uitgelegd wat je met hen kunt afstemmen tijdens het opstellen (en uitvoeren) van jouw migratieplannen.

Leveranciers en eigen ICT-afdeling

Jouw (interne of externe) leveranciers van soft- en hardware zijn misschien al bezig met het (voorbereiden van het) inbedden van quantumveilige cryptografie in hun geleverde producten. Ga het gesprek aan om te begrijpen hoe hun migratieplannen eruit zullen zien en toets in hoeverre deze plannen jouw risico's afdekken. Bespreek je behoefte met je leveranciers en maak duidelijke afspraken. Documenteer deze afspraken ook, zodat je binnen de organisatie kunt communiceren waarom bepaalde keuzes zijn gemaakt. Houd er rekening mee dat sommige marktpartijen zullen aangeven dat hun producten nu al quantumveilig of '*PQC ready*' zijn. We adviseren om dergelijke uitspraken altijd eerst nauwkeurig te onderzoeken en te toetsen.

Inkopers

Ga met de inkoopafdeling in gesprek over (het opstellen van) de eisen voor de aanschaf van systemen, maar ook voor soft- en hardware met cryptografische componenten. Voor toekomstige trajecten kunnen afspraken gemaakt worden over *crypto-agility* en wat dit betekent voor migratie van deze nieuwe systemen. Deze afspraken kunnen opgenomen worden in inkoopvoorwaarden.

Toezichthouders

Betrek toezichthouders om ervoor te zorgen dat je plannen voldoen aan geldende (wettelijke) kaders en richtlijnen.

Klanten en andere afhankelijken

Bespreek jouw migratieplannen met klanten, samenwerkingspartners en overige interne stakeholders en maak afspraken waar nodig. Deze communicatie is belangrijk, omdat de migratie bijvoorbeeld voor uitdagingen kan zorgen in de interoperabiliteit waardoor bepaalde diensten misschien onverwacht toch niet geleverd kunnen worden.

Risico's voor je migratietraject en een plan B

Er is nog veel onduidelijk over de tijdspaden van de quantumdreiging. Zo kan er altijd een technologische ontwikkeling zijn waardoor dreigingen urgenter worden. Ook kan de beoogde quantumveilige cryptografie onbedoeld kwetsbaarheden bevatten. Daarnaast kan de voortgang van jouw migratie - net als elke migratie - om verschillende redenen vertraging oplopen. Het is belangrijk de bovengenoemde ontwikkelingen en tijdspaden in de gaten te houden. Hiermee houd je zicht op de risico's voor jouw organisatie en of je migratie op tijd uitgevoerd kan worden. Neem in je migratieplan ook plannen op voor alternatieve mitigerende maatregelen, zoals aanvullende (fysieke) netwerksegmentatie, als de verwachting is dat jouw migratietraject niet tijdig genoeg het risico kan mitigeren. Beschrijf daarbij ook de verwachte impact op jouw organisatiedoelen en bedrijfsvoering.

Vooruitblik

Er wordt op dit moment op verschillende manieren gewerkt aan handvatten en standaarden voor het migreren naar quantumveilige oplossingen. Een voorbeeld hiervan is software die automatisch cryptomiddelen kan inventariseren binnen bestaande netwerken. Vanuit het Amerikaanse NIST wordt er in een open internationaal verband gewerkt aan standaarden voor quantumveilige cryptografie binnen de publieke sleutelcryptografie.[11] Deze standaarden worden naar verwachting in 2024 definitief vastgesteld en zullen op grote schaal gehanteerd worden. We adviseren om de ontwikkelingen van NIST op het gebied van PQC-algoritmen in de gaten te houden.

De AIVD en het NCSC volgen deze ontwikkelingen nauwlettend en nemen relevante nieuwe ontwikkelingen op in toekomstige versies van deze handreiking of in aanvullende kennisproducten. Houd daarom onze websites en sociale media in de gaten voor nieuwe publicaties.

11 Zie: "Post-Quantum Cryptography", Computer Security Resource Center (NIST), 2023, https://csrc.nist.gov/Projects/post-quantum-cryptography.

Het handelingsperspectief in het kort

- Voer eerst een risicoanalyse uit om te bepalen welke van je te beschermen belangen mogelijk een verhoogd risico lopen door de quantumdreiging.
- Maak met de uitkomsten van de risicoanalyse inzichtelijk welke cryptografie jouw organisatie gebruikt en in beheer heeft, wie deze levert, en welke beveiligingsmaatregelen nu steunen op deze cryptografie. Neem dit op in je bredere *asset management*-proces.
- Beoordeel je risico's op basis van de huidige inzichten in de quantumdreiging, je te beschermen belangen en de mate waarin jouw huidige beveiligingsmaatregelen afhankelijk zijn van cryptografie.
- Bepaal hoe je jouw risico's wil beheersen. Maak *crypto-agility* onderdeel van jouw inkoopvoorwaarden en stel een migratieplan op samen met je leveranciers, ketenpartners en overige stakeholders. Ontwikkel een alternatieve mitigatiestrategie als onderdeel van jouw migratieplan voor als je je migratie niet tijdig kunt uitvoeren.
- Blijf op de hoogte van belangrijke ontwikkelingen rondom quantumcomputers en toets deze ontwikkelingen periodiek aan je risicobeoordeling en migratieplan. Stel het migratieplan bij als ontwikkelingen hiervoor aanleiding geven.

Omdat het uitdagend kan zijn om kennis op te doen en belangrijke ontwikkelingen bij te houden, is het ook mogelijk om gebruik te maken van externe bronnen en samenwerkingsverbanden. Weet bij wie je binnen jouw organisatie terechtkunt met vragen of ga na aan wie je deze vragen extern kunt stellen. Beheer je staatsgeheime informatie? Neem in dat geval contact op met het NBV van de AIVD.

Deze brochure is een uitgave van:

Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl
Postbus 20010 | 2500 EA Den Haag

Nationaal Cyber Security Centrum
ncsc.nl
Postbus 117 | 2501 CC Den Haag

September 2023 | Publicatie-nr. 23405792