Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bereid je voor op de dreiging van

quantum computers

Hoe bereid je je voor op de dreiging van quantumcomputers?

Al jaren wordt de komst van de quantumcomputer voorspeld die bepaalde cryptografie kan breken. Dit brengt risico's met zich mee op het gebied van informatiebeveiliging. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) volgt de ontwikkelingen op de voet en doet onderzoek om tijdig producten en oplossingen te kunnen bieden voor deze beveiligingsrisico's.

Werk je met gevoelige informatie? In deze publicatie deelt het NBV zijn visie op de dreiging van quantumcomputers en lees je welke maatregelen je kunt nemen om je hiertegen te beschermen. In onze eerdere publicatie uit 2014[1] adviseerden we al waakzaam te zijn voor de ontwikkeling van de quantumcomputer.

Wat is het NBV?

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) heeft als doel om Nederland digitaal veilig te houden tegen statelijke dreigingen en andere Advanced Persistent Threats (APT's). Wij zijn uniek doordat wij onze specialistische beveiligingskennis combineren met de bijzondere inlichtingenpositie die we hebben als onderdeel van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). We werken nauw samen met onze veiligheidspartners MIVD, NCTV en NCSC. Gezamenlijk helpen we de Rijksoverheid en de vitale sector om bijzondere en gevoelige informatie zoals staatsgeheimen te beschermen.

Quantumcomputers: een reëel risico?

Al tientallen jaren is bekend dat inzichten vanuit de quantummechanica gebruikt kunnen worden om de meest gebruikte asymmetrische cryptografie aan te vallen met een quantumcomputer. Bijvoorbeeld RSA en elliptische krommen veel gebruikt in HTTPS. Deze vorm van cryptografie noemen we in deze publicatie ‘klassieke cryptografie’. De nu al werkende quantumcomputers hebben nog niet voldoende rekenkracht om een serieuze bedreiging te zijn voor de huidige cryptografie. Met de term quantumcomputer bedoelen we een geavanceerde quantumcomputer die klassieke cryptografie kan breken.

Experts achten de kans klein maar reëel dat quantumcomputers in 2030 al krachtig genoeg zullen zijn [2, 3] om de huidige cryptografische standaarden te breken. Voor gevoelige informatie vindt het NBV een kleine kans voldoende reden om passende maatregelen te nemen. Tot die tijd zijn er ook risico’s voor de huidige cryptografie. De data die je nu vercijferd verstuurt of opslaat, kan onderschept worden en op een later moment met een quantumcomputer ontcijferd worden. Gegevens die in 2030 nog steeds gevoelig zijn en geheim moeten blijven, moeten daarom nu al vercijferd worden met cryptografie die beschermt tegen aanvallen met een quantumcomputer.

Daarom adviseren we je om op tijd te werken aan een migratieplan voor een quantum-veilige oplossing. De migratie naar nieuwe cryptografische mechanismen is een complex proces dat tijd kost. Houd je hier geen rekening mee en neem je te laat maatregelen? Dan loop je het risico dat je gevoelige of vertrouwelijke informatie later alsnog ontcijferd wordt.

Store now, decrypt later
Omdat vertrouwelijke informatie vaak een lange geheimhoudingstermijn heeft, is de dreiging van een quantumcomputer reëel. Vercijferde data die nu onderschept en opgeslagen wordt, kan op een later moment ontcijferd worden met een quantumcomputer. Dat kan gebeuren voordat de geheimhoudingstermijn van je informatie verloopt.

Hoe beveilig je je tegen de dreiging van quantumcomputers?
- Bereid je nu voor op migratie naar quantumveilige cryptografie.
- Gebruik voor symmetrische cryptografie sleutellengtes van 256 bits.
- Migreer naar Post-Quantum Cryptografie zodra de standaarden beschikbaar zijn. Kijk in de tussentijd naar hybride constructies.
- Met alleen Quantum Key Distribution kun je gevoelige informatie niet beveiligen tegen quantumcomputers.

Hoe kun je je organisatie beveiligen tegen de dreiging van quantumcomputers?

Het NBV adviseert het gebruik van PQC

Om je gevoelige of vertrouwelijke data quantumveilig te beschermen, adviseert het Nationaal Bureau voor Verbindingsbeveiliging het gebruik van Post-Quantum Cryptografie (PQC) in combinatie met een bestaand asymmetrisch algoritme (hybride constructie, zie kader). We zien dit als dé manier om je te beveiligen tegen aanvallen van quantumcomputers.

Het NBV heeft veel vertrouwen in de veiligheid en het toepassen van deze vorm van cryptografie, ook al zijn er nog geen internationale standaarden. Waar uitrollen van PQC nog niet mogelijk is, adviseren we als tussenoplossing het toevoegen van symmetrische cryptografie aan bestaande toepassingen.

Post-Quantum Cryptografie (PQC)
Post-Quantum Cryptografie (PQC) is een vorm van cryptografie die gebaseerd is op wiskundige problemen die niet effectief te kraken zijn met een quantumcomputer. Op dit moment wordt gewerkt aan nieuwe PQC-standaarden, die de huidige asymmetrische standaarden kunnen vervangen.

Om zeker te zijn van de veiligheid van deze nieuwe standaarden hebben deze vormen van cryptografie tijd nodig om volwassen te worden. Met wetenschappelijk onderzoek wordt het vertrouwen in de veiligheid van deze standaarden vergroot. Dit is een proces dat veel tijd kost. Het National Institute of Standards and Technology (NIST) van de VS is al in 2016 begonnen met een open proces om internationale standaarden te krijgen. Deze standaarden worden rond 2024 verwacht. Ook onderzoeksprogramma PQCRYPTO-EU doet onderzoek naar vormen van Post-Quantum Cryptografie.

Het is ook mogelijk om PQC in combinatie met klassieke cryptografie in te zetten. Dit noemen we een hybride constructie (zie kader).

Te vroeg overgaan naar een quantumveilige oplossing kan veel tijd en geld kosten. Te laat is ook geen optie door het risico dat je gevoelige informatie kwetsbaar is. Daarom adviseert het NBV om nu alvast een migratiestrategie uit te werken. Hieronder lees je hoe je dat kunt doen.

Hybride constructies

Er is voldoende zekerheid in de veiligheid van de PQC algoritmen, maar de implementaties zijn nog erg onvolwassen. Dat betekent dat het nog niet zeker is dat er in de implementaties geen fouten zijn gemaakt waardoor het algoritme gebroken kan worden.

Een oplossing om je nu al beter te beschermen tegen dreigingen van een quantumcomputer, zonder verlies van veiligheid, is een hybride constructie. Dit is een combinatie van klassieke cryptografie (elliptische krommen of RSA) met PQC. Het PQC-gedeelte zorgt voor weerbaarheid tegen quantumaanvallen, terwijl het klassieke deel ervoor zorgt dat de beveiliging nooit zwakker wordt.

Hoe bereid je een migratie naar PQC voor?

Voordat je naar PQC migreert, is het belangrijk om een inventarisatie te maken van je te beschermen data, de geheimhoudingstermijn daarvan en de cryptografie die je gebruikt. Hierdoor krijg je goed inzicht in je assets en systemen.

Welke informatie moet je geheim of vertrouwelijk houden? Hoe lang moet deze geheim blijven? En wordt het beschermd door asymmetrische of symmetrische cryptografie, of een combinatie daarvan? Dit helpt je om te bepalen welke cryptografische oplossing het beste past bij je organisatie.

Ook kun je alvast een inschatting maken hoeveel tijd het kost om over te gaan naar PQC en controleren of de apparatuur die je organisatie gebruikt overgezet kan worden naar PQC. Daarnaast kun je in kaart brengen wat daar voor nodig is en welke knelpunten je tegenkomt. Voorbeelden hiervan zijn lastig te updaten apparatuur, benodigde interoperabiliteit met verschillende partijen, lage bandbreedte of beperkte rekenkracht. De laatste twee voorbeelden kunnen knelpunten veroorzaken doordat PQC-algoritmen vaak minder efficiënt zijn dan klassieke algoritmen. Voor de meeste toepassingen levert dit geen onoplosbare problemen op.

Tot slot kun je bij het aanschaffen van nieuwe apparatuur rekening houden met de overgang naar PQC als onderdeel van je *lifecycle management*. Bespreek alvast met je leverancier of er oplossingen zijn die PQC ondersteunen of een extra laag symmetrische cryptografie hebben. Houd bij de aanschaf van nieuwe apparatuur ook rekening met de *crypto-wendbaarheid* van deze apparatuur. Dat is heel belangrijk het geeft aan hoe flexibel de apparatuur kan omgaan met verschillende cryptografische algoritmen en sleutellengtes.

Het Amerikaanse NIST heeft een uitgebreide whitepaper geschreven over PQC migratie[4]. Ook TNO en het NCSC hebben een handige handreiking voor migratie naar PQC[5,6].

Wat als mijn data nu al quantumveilig moet zijn?

Heb je vastgesteld dat je vertrouwelijke informatie nu al quantumveilig opgeslagen moet worden? Dan adviseren we je dit:

1. Vul alle systemen waarvan de veiligheid afhankelijk is van asymmetrische cryptografie aan met een laag symmetrische cryptografie.
2. Kan dit niet of is je informatie zo gevoelig dat een extra laagje symmetrische cryptografie niet voldoende veiligheid biedt? Schakel dan nu alvast over op PQC in een hybride constructie (zie blz.7). Je kunt veel verschillende algoritmen gebruiken die variëren in prestatie, efficiëntie en veiligheid. Voor PQC raden we de meest veilige algoritmen aan, zoals Frodo[7] of McEliece[8]. Dit is in lijn met wat onder andere BSI, de Duitse evenknie van het NBV, adviseert[9]. Deze algoritmen geven de meeste zekerheid tegen nieuwe aanvallen in de toekomst, maar zijn niet het meest efficiënt.
3. Bieden de bovenstaande opties geen of onvoldoende oplossing? Dan kun je overwegen of het risico van het offline halen van je systemen opweegt tegen het veiligheidsrisico dat je loopt met een quantumcomputer.

Welke andere beveiligings-mogelijkheden zijn er?

Symmetrische cryptografie
Met symmetrische cryptografie (zoals AES) is je informatie minder kwetsbaar voor aanvallen met een quantumcomputer. Met een sterk algoritme zoals AES, geeft symmetrische cryptografie met een sleutellengte van 256 bits voldoende cryptografische weerstand tegen een quantumcomputer. Binnen je organisatie kan je de bestaande symmetrische sleutellengtes verhogen naar 256 bits.

Symmetrische cryptografie kan je ook gebruiken als aanvulling op je bestaande beveiliging. Met sommige VPN-producten is het mogelijk om een extra laagje beveiliging toe te voegen met een symmetrisch gedeeld geheim. Ook kun je door asymmetrische cryptografie beveiligde verbindingen tunnelen door een symmetrisch beveiligde verbinding. Op die manier is eventueel onderschepte informatie alsnog beveiligd tegen een aanvaller met een quantumcomputer. Belangrijk hierbij is dat het gedeelde symmetrische geheim op een quantumveilige manier wordt uitgewisseld, bijvoorbeeld door het offline uit te wisselen. Het NBV kan overheidsorganisaties helpen met een advies over goedgekeurde en andere producten.

Quantum Key Distribution (QKD)
Quantum Key Distribution (QKD) wisselt digitale sleutels uit met technieken uit de quantummechanica. Bij deze manier van sleuteluitwisseling wordt het meeluisteren door een derde partij altijd gesignaleerd.

Met QKD wordt de identiteit van de zender en ontvanger niet vastgesteld. Je hebt dus wel een beveiligde verbinding, maar je weet niet met wie. Het toevoegen van authenticatie is een must, omdat je anders het risico loopt op een zogenaamde *man-in-the-middle*-aanval. Authenticatie toevoegen is mogelijk met PQC of symmetrische cryptografie en maakt QKD in feite overbodig.

QKD wordt genoemd als een bewijsbaar veilige methode voor sleuteluitwisselingen. Op dit moment zijn er nog geen QKD-implementaties met een passend veiligheidsbewijs. Het gaat hier bijvoorbeeld om een onvolledig bewijs door slechts een deel van de toepassing te bewijzen. Soms worden er aannames gedaan over de hardware die niet realistisch zijn of waar de hardware niet aan kan voldoen.

Daarnaast is voor QKD de afstand beperkt doordat er een optische point-to-pointverbinding nodig is. Dit is in de praktijk op te lossen door netwerken te gebruiken met vertrouwde punten of in de toekomst met quantum repeaters. Dit zijn qua kosten en schaalbaarheid geen aantrekkelijke alternatieven voor PQC.

Tot slot is QKD geen volwaardig alternatief voor PQC, omdat het zich alleen op sleuteluitwisseling richt en niet op andere toepassingen zoals digitale handtekeningen.

Door de beperkingen in functionaliteit en de huidige onvolwassenheid van de technologie, is QKD zonder PQC volgens het NBV ongeschikt voor het beveiligen van gevoelige informatie tegen de dreiging van quantumcomputers. Het standpunt van het NBV tegen QKD wordt breder gedragen door internationale tegenhangers van het NBV, zoals bijvoorbeeld blijkt uit het paper over QKD van het Franse ANSSI[10] maar ook uit [11, 12, 13].

Heb je vragen?

Heb je vragen over het beveiligen van gevoelige informatie tegen de dreiging van quantumcomputers? Bel ons op: 079-3205050 en vraag naar het NBV. We helpen je graag om jouw organisatie weerbaarder te maken.

Referenties

1 AIVD. 'Informatieblad Quantumcomputers'. (2014).

2 M. Mosca, M. Piani. 'Quantum threat Timeline report 2020' (2021).

3 TNO. 'Migration to quantum-safe cryptography. About making decisions on when, what and how to migrate to a quantum-safe situation.' (2020).

4 NIST. 'Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.' (2021).

5 NCSC. 'Factsheet Postkwantumcryptografie. Bescherm uw data van vandaag tegen de dreiging van morgen.' (2017)

6 TNO. 'Migration to quantum-safe cryptography. About making decisions on when, what and how to migrate to a quantum-safe situation.' (2020).

7 E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila. 'FrodoKEM. Learning With Errors Key Encapsulation', https://frodokem.org (versie 4 juni 2021).

8 M.R. Albrecht, D.J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurisch, R. Misoczki, R. Niederhagen, K.G. Paterson, E.Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C.J. Tjhai, M. Tomlinson, W. Wang. 'Classic McEliece: conservative code-based cryptography', https://classic.mceliece.org (versie 10 oktober 2020).

9 Bundesamt für Sicherheit in der Informationstechnik. 'BSI – Technical Guideline. Cryptographic Mechanisms: Recommendations and Key Lengths'. (2021).

10 ANSSI. 'Technical position paper: QKD. Should Quantum Key Distribution be Used for Secure Communications?'. (2020).

11 BSI, 'Quantenkryptografie', https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie.html (versie 14 juli 2021). *(Duitstalig)*

12 NCSC, 'Whitepaper Quantum security technologies', https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, version 1.0, 24-03-2020.

13 NSA, 'Quantum Key Distribution (QKD) and Quantum Cryptography (QC)', https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/ (versie 14 juli 2021).

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
T (079) 320 50 50

september 2021