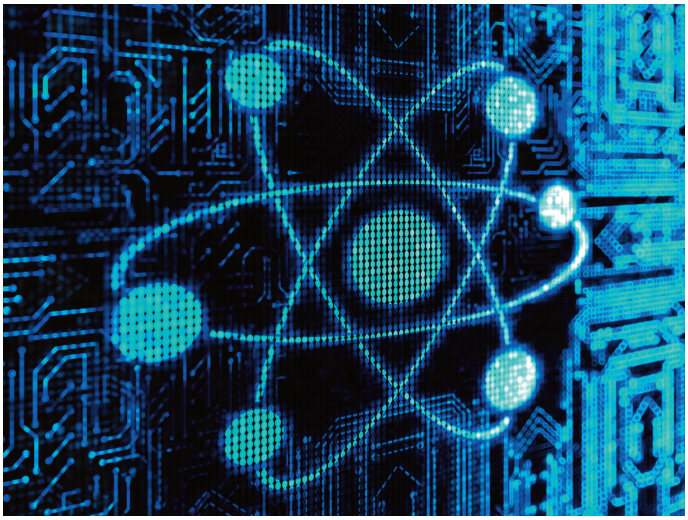
Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Quantumcomputers

Inleiding

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD geeft overheidspartijen advies over informatiebeveiliging voor gerubriceerde informatie. Ook begeleidt het NBV productontwikkelingen door de crypto-industrie en evalueert informatiebeveiligingsproducten. Een ontwikkeling die de informatiebeveiliging in gevaar brengt is de quantumcomputer. Deze ontwikkeling vormt een probleem voor beleidsmakers en uitvoeringsorganisaties die hun informatie langdurig willen beschermen.

Al jaren wordt de komst van de quantumcomputer voorspeld. Deze computer zou razendsnel kunnen rekenen en onze huidige computers overbodig maken. Met een quantumcomputer zou het mogelijk worden nieuwe medicijnen te ontwikkelen, nieuwe materialen te ontdekken en om cryptografie te kraken.
Met de huidige stand van de techniek komt daardoor de beveiliging van digitale gegevens ernstig in gevaar. Daarom moeten we nu investeren in nieuwe cryptografische oplossingen.



Wat is een quantumcomputer?

Een quantumcomputer is een computer die op een andere manier rekent dan de computer die we kennen. Een gewone computer werkt met bits die 0 of 1 zijn. Een quantumcomputer werkt met qubits, dat zijn bits die tegelijkertijd 0 en 1 kunnen zijn.

Voor de meeste doeleinden is een quantumcomputer helemaal niet beter dan een gewone computer. Het klopt dus niet dat gewone computers helemaal vervangen zullen worden door quantumcomputers. Maar voor sommige doeleinden is een quantumcomputer veel beter dan een gewone computer.

Een quantumcomputer is erg goed in het oplossen van bepaalde wiskundige problemen waarvan altijd gedacht is dat ze onoplosbaar zijn. Dat zijn precies de wiskundige problemen waarop een groot deel van onze informatiebeveiliging gebaseerd is. Met een quantumcomputer is het bijvoorbeeld mogelijk om beveiligd internetverkeer (https) te ontcijferen. Het is ook mogelijk om internetverkeer op te slaan, om het jaren later met een quantumcomputer te ontcijferen. Dat betekent dat we nu al rekening moeten houden met deze risico's, met name bij informatie die lange tijd geheim moet blijven.

Zijn er al quantumcomputers?

Er zijn al quantumcomputers, maar die zijn nog zo beperkt dat ze geen enkele bedreiging vormen voor onze informatiebeveiliging. Ze zijn gebouwd in laboratoria van universiteiten. Die universiteiten doen veel onderzoek naar hoe quantumcomputers verbeterd kunnen worden. De Universiteit van Innsbruck heeft dit jaar hun quantumcomputer verbeterd van 14 naar 16 qubits. Om onze informatiebeveiliging in gevaar te brengen zijn echter honderden tot duizenden qubits nodig. Voor wetenschappers is het een grote uitdaging om dat te gaan bereiken.

Wanneer is een dergelijke quantumcomputer te verwachten?

De TU Delft verwacht tussen 2030 en 2040 een quantumcomputer te bouwen met duizenden qubits. Van alle universiteiten zijn zij een van de voorlopers, maar ze zijn misschien niet de eerste partij die erin slaagt een quantumcomputer met duizenden qubits te bouwen. Ook grote inlichtingendiensten lijken geïnteresseerd in het bouwen van een quantumcomputer. Uit de Snowden-leaks blijkt bijvoorbeeld dat de NSA in 2011 al bezig was met onderzoek naar het bouwen van quantumcomputers. In de gelekte notities staan ambitieuze doelstellingen en grote budgetten voor deze ontwikkeling.

Welke oplossingen biedt quantum-cryptografie?

Met quantumtechnologie kun je niet alleen informatie kraken maar ook beveiligen. Quantumcryptografie wordt gebruikt voor informatiebeveiliging, om precies te zijn: voor het uitwisselen van sleutels. Het wordt daarom ook wel quantum key distribution (QKD) genoemd. QKD kan niet gekraakt worden met een quantumcomputer. Het is daarom geschikt als vervanger voor de huidige cryptografie. QKD-systemen zijn te koop, maar ze zijn momenteel nog erg kostbaar. QKD-systemen maken gebruik van een directe glasvezelverbinding of van lichtsignalen die door de lucht worden verstuurd. Het bereik is daardoor niet groter dan enkele honderden kilometers.

Een alternatief voor QKD-systemen is post-quantum-cryptografie. Dat zijn cryptografische algoritmes die niet gekraakt kunnen worden door een quantum-computer. Ook deze oplossing is geschikt als vervanger voor de huidige cryptografie. Er zijn hiervan al imple-mentaties op internet te vinden. Een nadeel is dat deze oplossing vrij veel rekenkracht en bandbreedte kost. Ook is meer wiskundig onderzoek nodig om te onder-bouwen dat deze oplossing echt veilig is. Bovendien zijn er nog geen internationale standaarden afgesproken voor post-quantum-cryptografie.

Wat kan ik doen?

Het is verstandig na te gaan welke partijen interesse kunnen hebben in uw informatie. Daarnaast is het belangrijk na te gaan hoe lang die informatie beschermd moet worden. Informatie die langdurig beschermd moet worden, kan nu al onderschept worden om later te ontcijferen. Als u inschat dat uw informatie gevaar loopt, is het verstandig een expert te vragen om advies. Het NBV beschikt over dergelijke expertise.

Wat doet het NBV tegen quantum-computers?

De weerbaarheid tegen quantumcomputers wordt steeds urgenter, met name voor strategische informatie met een lange beschermingstermijn. Daarom volgt het NBV deze ontwikkelingen op de voet en stelt waar nodig aanvullende eisen aan beveiligingsproducten.

Het NBV doet ook eigen onderzoek naar ontwikkelingen als post-quantum-cryptografie en werkt samen met andere organisaties zoals de TU Delft. Inzet is het tijdig beschikbaar krijgen van producten en oplossingen binnen de overheid, die beveiliging kunnen bieden tegen quantumcomputers.

Colofon
Algemene Inlichtingen-en Veiligheidsdienst (AIVD)
Nationaal Bureau voor Verbindingsbeveiliging (NBV)
Postbus 20010
2500 EA Den Haag

Telefoon: 079-3205050
E-mail: nbv@minbzk.nl
www.aivd.nl/onderwerpen/infobeveiliging/