Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1085

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 november 2023

In antwoord op uw brief van 5 juli 2023 stuur ik u, mede namens de Minister van Economische Zaken en Klimaat, de beantwoording van de brief van uw commissie: «Aanvullende kennisvragen inzake Kwantumtechnologie en de gevolgen voor encryptie». U vindt de beantwoording in de bijlage bij deze brief.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

kst-26643-1085
ISSN 0921 - 7371
's-Gravenhage 2023

BIJLAGE

Aanvullende vragen van de vaste commissie Digitale Zaken aan de Minister van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties: «Aanvullende kennisvragen inzake Quantumtechnologie en de gevolgen voor encryptie».

1. Wat is er nodig om op het gebied van informatiebeveiliging rijksbreed klaar te zijn voor de gevolgen van de komst van quantumcomputers?

Het belangrijkste gevolg voor informatiebeveiliging rijksbreed is dat quantumcomputers bepaalde versleuteling (of cryptografie) sterk verzwakken. Dit veroorzaakt risico's voor de rijksoverheid en ook voor burgers, ondernemingen en andere overheden die tijdig beheerst moeten worden. De rijksoverheid bereidt zich hierop voor met het programma Quantumveilige Cryptografie Rijk.

Cryptografie zorgt voor veilige en vertrouwelijke digitale communicatie. Cryptografie houdt zich o.a. bezig met technieken om informatie op te slaan en over te dragen zodanig dat deze alleen leesbaar zijn door partijen die de juiste sleutel bezitten. Daarvoor zijn in ons dagelijks leven zeer veel toepassingen en cryptografie wordt daarom overal gebruikt. Door cryptografie zijn bijvoorbeeld onze identiteitsgegevens (paspoorten) beschermd, kunnen we veilig verkeerslichten en bruggen aansturen, mailen en appen we met elkaar, betalen we met onze telefoon en we gebruiken het om vertrouwelijke informatie te versleutelen, zoals bedrijfsgeheimen of staatsgeheimen. Cryptografie vormt dan ook een onmisbaar fundament om de vertrouwelijkheid, integriteit en beschikbaarheid van processen en data te beschermen. Met de komst van een krachtige quantumcomputer is meeste cryptografie echter niet meer (voldoende) veilig: bestaande encryptiemethodes zullen worden verzwakt of gebroken. Dat betekent dat onze data en communicatie dan niet meer beschermd zullen zijn. Daarom moeten er nu voorbereidende acties worden ondernomen.

De benodigde veranderingen om data en communicatie te beschermen tegen de capaciteiten van quantumcomputers zijn complex, omvangrijk en zullen vele jaren in beslag nemen. Nu beginnen met voorbereiden is dan ook noodzakelijk om risico's, inspanning en kosten te kunnen spreiden. Daarom heeft de rijksoverheid een Rijksbreed samenwerkingsprogramma Quantumveilige Cryptografie (QvC-Rijk) in uitvoering. Het plan van aanpak voor de rijksoverheid is april 2023 in het CIO-beraad vastgesteld. Departementen en uitvoeringsorganisaties zijn zelf verantwoordelijk voor het op tijd klaar zijn voor de bovengenoemde gevolgen. Met dit programma worden zij gestimuleerd en ondersteund om de risico's van deze dreiging tijdig te beheersen. Vanuit het programma wordt o.a. samengewerkt met onderzoek en wetenschap.

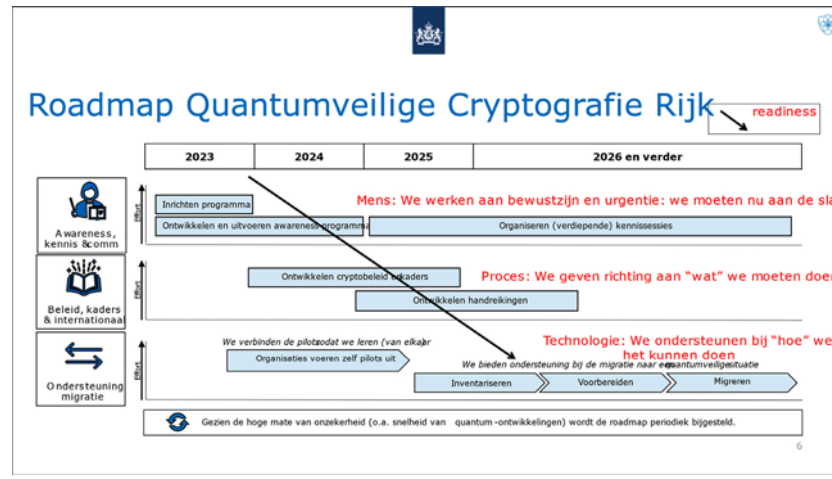
Op hoofdlijnen zijn de volgende zaken nodig:
- Mens: het programma werkt aan het vergroten van het bewustzijn van de dreiging en de urgentie om te beginnen met de voorbereidingen bij alle doelgroepen van de rijksoverheid. Dit geldt voor zowel rijksoverheid zelf als voor de leveranciers van de rijksoverheid die cryptografische componenten hebben verwerkt in hun diensten en producten. De awareness campagne en communicatieactiviteiten zijn in volle gang sinds voorjaar 2023 en lopen door in 2024.
- Proces: met Rijksbreed beleid en (in de toekomst) quantumveilige cryptografiestandaarden, het vaststellen van kaders en handreikingen geven we richting aan wat de rijksoverheid moet doen. Twee voorbeelden:

    - Met een interdepartementale werkgroep bereidt de rijksoverheid momenteel een Rijksbreed beleidskader cryptografie voor. Komend jaar wordt dit beleidskader vastgesteld.
    - Een gereedschap voor leveranciersmanagers om met leveranciers in gesprek te gaan is in concept gereed. Met dit gereedschap kunnen leveranciersmanagers het gesprek aangaan over de voorbereidingen die leveranciers moeten treffen. Met een aantal leveranciers van het Rijk wordt samengewerkt, zodat dit optimaal het goede gesprek zal faciliteren.
- Technologie: het programma beoogt ondersteuning te bieden bij de technische voorbereidingen voor de migratie van kwetsbare cryptografie naar quantumveilige cryptografie. Dit kunnen wij als rijksoverheid niet alleen. Daarom zoeken we vanuit ons programma de samenwerking tussen bedrijfsleven, wetenschap en overheid. Met partners bereiden we het volgende voor:
    - Voortdurend actueel inzicht in cryptografie die in gebruik is en borging daarvan in processen voor beheer van ICT-bedrijfsmiddelen is voor de rijksoverheid en elk bedrijf en leverancier noodzakelijk. (Zie verder onder vraag 3)
    - De overgang van kwetsbare cryptografie naar quantumveilige cryptografie is een technologisch ingrijpende wijziging die nog niet eerder op deze schaal is voorgekomen. Dat plaatst o.a. de rijksoverheid voor uitdagingen: het programma beoogt een expertisecentrum op te zetten om de obstakels en problemen die worden ontdekt samen met bedrijfsleven, wetenschap en overheid te onderzoeken en op te lossen.

Daar waar het programma QvC-Rijk zich focust op het gebruik van cryptografie die ook bestand moet zijn tegen de dreiging van de quantumcomputer, focust de Nationale Cryptostrategie (NCS) zich onder meer op het *aanbod* van quantumveilige cryptografie. De hoogste Te Beschermen Belangen (TBB) vragen specialistische cryptografie van Nederlandse bodem om nationale en economische veiligheid en soevereiniteit naar de toekomst toe te borgen. De NCS heeft als doel om de noodzakelijk benodigde bouwstenen daarvoor te realiseren.

Wat is er nodig om klaar te zijn voor de gevolgen van quantumcomputers? Samenvattend kunnen we voor de rijksoverheid het volgende stellen:
- Iedereen, ook in de politiek, is zich bewust van de potentiële gevaren van kwantumcomputers voor cryptografie;
- Partijen binnen de rijksoverheid, en haar IT-leveranciers en moeten zich nu al voorbereiden.
- De rijksoverheid wordt ondersteund door QvC-Rijk middels kennisdeling, ondersteuning, stimulans en kaders.

Dit vormt de aanpak van het Programma QvC Rijk, zoals hieronder schematisch is weergegeven.



2. Op welke manieren wordt op dit moment regie genomen om dit te bereiken?

Onder regie van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties wordt de migratie naar quantumveilige cryptografie binnen de rijksoverheid voorbereid.

De AIVD (Algemene Inlichtingen- en Veiligheidsdienst), het NCSC (Nationaal Cyber Security Centrum), CIO-Rijk (directie Chief Information Office- Rijk) en EZK (Ministerie van Economische Zaken en Klimaat) ontwikkelen hiervoor kennisproducten vanuit de taken die zij invullen. Dit gebeurt in onderlinge samenwerking en afstemming.

In brede zin maakt het voorbereiden op quantumveilige cryptografie deel uit van de Nederlandse Cybersecuritystrategie 2022–2028[1]. Deze stelt onder andere dat, om de digitale veiligheid van Nederland nu en in de toekomst afdoende te kunnen beschermen, de ontwikkeling en toepassing van kennis en kunde op het gebied van cybersecurity continu worden versterkt. Intensieve en duurzame samenwerking tussen overheid, bedrijfsleven en kennisinstellingen is hiervoor essentieel. Het publiek-private samenwerkingsplatform Dcypher, onder verantwoordelijkheid van EZK, speelt hier voor de overheid een centrale rol in, en legt de basis voor agendering en programmering van meerjarige onderzoeks- en innovatietrajecten met overheidspartijen, bedrijven en kennisinstellingen.

- Bij CIO-Rijk is vanuit de I-strategie Rijk 2021 – 2025 Thema 2: Digitale Weerbaarheid, het programma Quantumveilige Cryptografie Rijk (QvC-Rijk) gestart. Onder dit thema valt ook de Nationale Cryptostrategie (NCS). De ambities en activiteiten van het programma Quantumveilige Cryptografie Rijk en de NCS zijn uitgewerkt onder vraag 1.
- Onder coördinatie van Dcypher wordt een routekaart cryptocommunicatie uitgevoerd. Onder deze routekaart is onder andere onderstaand handboek tot stand gekomen. Ook wordt o.a. onderzoek uitgevoerd voor publicatie van een beslisboom als toevoeging aan het handboek. Deze beslisboom gaat organisaties via een vraag-en antwoord pad helpen om, gegeven hun situatie, op relevante mogelijkheden voor quantumveilige cryptografie terecht te komen.
- De AIVD heeft in april van dit jaar een handboek gepubliceerd over de migratie naar quantumveilige cryptografie[2]. Dit handboek is biedt

[1] Nederlandse Cybersecuritystrategie 2022–2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
[2] https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek

organisaties handvatten om over te stappen naar een manier van beveiliging van gegevens die bestand is tegen de dreiging van quantumtechnologie. Het is mede tot stand gekomen als onderdeel van de routekaart Cryptocommunicatie van Dcypher en is ontwikkeld in samenwerking met TNO en CWI en mede gefinancierd door EZK. Het wordt gebruikt binnen het programma Quantumveilige Cryptografie Rijk.
- De AIVD en het NCSC hebben naar aanleiding van dit handboek een handreiking gemaakt voor CIO's (Chief Information Officers), CTO's (Chief Technology Officers) en CISO's (Chief Information Security Officers) van de overheid, het bedrijfsleven en kennisinstellingen. Dit ondersteunt de te nemen stappen voor de risicoanalyse en migratieplanning[3].
- Dcypher werkt samen met bedrijfs- en overheidspartijen om verdere ontwikkeling en adoptie van het handboek vorm te geven.

3. Welke knelpunten en kansen ziet het kabinet hierbij?

Zoals onder de beantwoording van vraag 1 is opgenomen, is de migratie van kwetsbare cryptografie naar quantumveilige cryptografie een verandering die nog niet eerder op deze schaal is voorgekomen. Dat plaatst niet alleen de rijksoverheid voor uitdagingen, maar ook alle bedrijven en organisaties. Een aantal belangrijke knelpunten hierbij:
- Voortdurend actueel inzicht in cryptografie (zie ook vraag 1) die in gebruik is en borging daarvan in het beheer van ICT-bedrijfsmiddelen is voor de rijksoverheid en elk bedrijf en leverancier noodzakelijk. In onze voortdurend veranderende en complexe digitale omgevingen is handmatig inventariseren van het gebruik van cryptografie niet effectief. Op deze grote schaal is beschikbaarheid van geschikte ICT-gereedschappen hiervoor een knelpunt, evenals de verwachte grootschalige behoefte aan ondersteuning voor de implementatie van deze gereedschappen.
- Doordat sprake is van een technologisch ingrijpende wijziging (zie ook vraag 1) zullen we obstakels en problemen gaan tegenkomen. Deze zullen moeten worden onderzocht zodat geschikte oplossingen kunnen worden gevonden.
- Op termijn zullen veel gecertificeerde producten opnieuw gecertificeerd moeten worden, op basis van nieuwe criteria op het gebied van cryptografie. Bij het beschikbaar komen van nieuwe (eisen voor) cryptografie zullen in korte tijd veel aanvragen voor certificering worden gedaan. Een reële kans is dat de certificerende organisaties enorme toeloop aan aanvragen niet aan zullen kunnen.
- Een ander knelpunt betreft het verkrijgen van voldoende kennis en innovatievermogen om de transitie naar quantumveilige cryptografie te kunnen uitvoeren. Kennis van cryptografie, migraties van cryptografie en daarbij samenhangende onderwerpen is zeer schaars. Om voldoende slagkracht te kunnen krijgen in de transitie naar quantumveilige cryptografie zal de rijksoverheid moeite hebben om de kennis en innovatiemarkt aan zich te kunnen binden, in de wetenschap dat de Nederlandse kennis- en innovatiemarkt beperkte capaciteit heeft.

Uiteraard bieden technologische veranderingen en de knelpunten die daarbij ontstaan ook kansen:
- De transitie naar quantumveilige cryptografie van de hele samenleving en de rijksoverheid in het bijzonder is een opgave van zeer grote schaal, en met een zeer lange doorlooptijd. Er zal veel dienstverlening vanuit de commerciële markt nodig zijn om de overheid voor te

[3] https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig

bereiden op quantumveilige cryptografie, en de overheid daarna blijvend quantumveilig te houden. Dit biedt kansen voor de ontwikkeling van een nieuwe inkoopmarkt voor migratie naar kwantumveilige cryptografieen evaluatiediensten, waar met name gespecialiseerde MKB bedrijven baat bij zullen hebben.
- Gezien het veiligheidsbelang van een zorgvuldige migratie naar quantumveilige cryptografie is het belangrijk dat deze markt vooral wordt gevoed door Nederlandse bedrijven, en met kennis en innovaties die in Nederland ontwikkeld zijn. Deze ontwikkeling is belangrijk in het kader van het beschermen van de Nederlandse digitale open strategische autonomie. Hiervoor is cryptografie ook opgenomen in de Agenda Digitale Open Strategische Autonomie die u 17 oktober jl. heeft ontvangen van de Minister van EZK.[4]

4. In hoeverre heeft het kabinet ook gekeken naar het voorbeeld van de Amerikaanse regering die wetgeving heeft aangenomen waarmee federale overheidsinstanties worden verplicht over te gaan op «Post Quantum Cryptography», waarmee overheidssystemen bestand moeten zijn tegen aanvallen van zowel kwantumcomputers als standaardcomputers (H.R.7535 – Quantum Computing Cybersecurity Preparedness Act)?

Het kabinet volgt de internationale ontwikkelingen en heeft ook kennis genomen van de Amerikaanse wetgeving. De bovengenoemde wetgeving richt zich op de verplichting van het implementeren van één oplossing om weerbaar te zijn tegen de dreiging van quantumtechnologie.

De aanpak van de rijksoverheid past bij de generieke aanpak voor digitale weerbaarheid: een risicogerichte aanpak. De aanpak geeft daarbij ruimte om ook andere maatregelen te nemen om de risico's te beheersen. Dit doet de rijksoverheid o.a. omdat:
- Post quantum cryptografie als vervanging van de huidige asymmetrische cryptografie mogelijk niet overal kan worden toegepast.
- Voor symmetrische cryptografie, vergroting van de sleutellengte vooralsnog als voldoende wordt beschouwd en daarmee behouden kan blijven.
- Er ook andere technologie in ontwikkeling is die in de toekomst bij zou kunnen dragen aan het mitigeren van de risico's in bepaalde omgevingen, zoals hybride cryptografische technologie en Quantum Key Distribution (QKD).

5. Wat vindt het kabinet van dergelijke wetgeving en acht zij iets soortgelijks nuttig voor Nederland?

De Amerikaanse wetgeving is gericht op één specifieke technologische dreiging en verplicht federale overheidsinstanties om één specifieke maatregel te implementeren. De huidige Europese, nationale en overheidsbrede en wet- en regelgeving op het gebied van informatiebeveiliging c.q. cybersecurity heeft een bredere werking en biedt voldoende aanknopingspunten om in actie te moeten komen.

Zo geeft NIS2[5] (Network and Information Security Directive) aan dat «state of the art» beveiligingsmaatregelen moeten worden toegepast. Dit betreft ook encryptie.

---

[4] Kamerstuk 36 259, nr. 21

[5] Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (NIS2-richtlijn) | Shaping Europe's digital future (europa.eu)

Voor de overheid verplichte standaarden als ISO27001/2 en voor de overheid vertaald in de BIO[6] (Baseline Informatiebeveiliging Overheid) eisen dat nieuwe dreigingen en risico's moeten worden opgenomen in het risicomanagementproces. Daarnaast bevatten deze standaarden een specifieke eis ten aanzien van cryptografie. Ook andere eisen zorgen ervoor dat organisaties met de dreiging van de quantumcomputer voor cryptografie aan de gang moeten, bijvoorbeeld de eis rondom het beheersen van kwetsbaarheden.

[6] Home NL – bio-overheid