Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER BESLUITVORMING

Nota actief openbaar
Ja

Onze referentie
2023-0000650214

Datum

Opgesteld door

Samengewerkt met
ministerie van EZK

Bijlage(n)
2

Aan Staatssecretaris Koninkrijksrelaties en Digitale Zaken
Van CIO Rijk

nota

oplegnota kennisvragen KamerCIE DIZA "Aanvullende kennisvragen inzake Quantumtechnologie en de gevolgen voor encryptie"

Aanleiding

De Kamercommissie Digitale Zaken heeft 5 juli jongstleden bovengenoemde brief gestuurd met daarin 5 kennisvragen. Deze brief is aan u gericht en aan de Minister van Economische Zaken en Klimaat.
Bijgaand vindt u de brief van de Kamercommissie en uw brief met de antwoorden op de gestelde vragen. De antwoorden zijn afgestemd met het ministerie van EZK. U tekent mede namens hen.
De Kamercommissie heeft om een reactie gevraagd vóór 1 november 2023.

Geadviseerd besluit

- Akkoord gevraagd met verzending van de brief met de antwoorden naar de Kamercommissie Digitale Zaken.

Kern

Met deze brief geeft u antwoorden op de gestelde kennisvragen. Deze vragen zijn:

1. Wat is er nodig om op het gebied van informatiebeveiliging rijksbreed klaar te zijn voor de gevolgen van de komst van quantumcomputers?
2. Op welke manieren wordt op dit moment regie genomen om dit te bereiken?
3. Welke knelpunten en kansen ziet het kabinet hierbij?
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)?
5. Wat vindt het kabinet van dergelijke wetgeving en acht zij iets soortgelijks nuttig voor Nederland?

In de beantwoording van **vraag 1 en 2** gaat u vooral in op:

- De Rijksbrede aanpak waarmee u regie neemt: het programma Quantumveilige Cryptografie Rijk. Dit is het ondersteunings- en stimuleringsprogramma van de rijksoverheid om de departementen en uitvoeringsorganisaties van de rijksoverheid te helpen in hun verantwoordelijkheid om op tijd de risico's van de quantumcomputer voor cryptografie te beheersen.

- Het PQC migratie handboek van de AIVD maakt eveneens deel uit van de regie. Het is ontwikkeld in samenwerking met TNO en CWI. U heeft dit handboek 4 april jongstleden in ontvangst genomen.
- De Nationale Cryptostrategie. U gaat kort in op het belang van beschikbaarheid van specialistische cryptografie van Nederlandse bodem om nationale en economische veiligheid en soevereiniteit naar de toekomst toe te borgen.
- De rol van en samenwerking met EZK en de routekaart cryptocommunicatie van Dcypher.

In de beantwoording van **vraag 3**

- Komen de knelpunten naar voren uit de beantwoording van vraag 1:
  - Gebrek aan inzicht in gebruikte cryptografie en instrumenten om automatisch dit inzicht te kunnen genereren
  - Problemen bij het voorbereiden van de migratie naar quantumveilige cryptografie vanwege technologische aspecten.
  - Verwachte wachtrijen bij certificeringsinstanties als veel producten in de toekomst in korte tijd opnieuw gecertificeerd moeten worden.
  - Het verkrijgen van voldoende kennis en innovatievermogen om de transitie naar quantumveilige cryptografie te kunnen uitvoeren. Er is schaarste
- En beschrijft u de kansen die dit biedt voor:
  - Gespecialiseerde MKB-bedrijven. Er zal veel dienstverlening vanuit de commerciële markt nodig zijn om de overheid voor te bereiden op quantumveilige cryptografie, en blijvend veilig te houden.
  - Nederlandse bedrijven. U gaat in op het veiligheidsbelang van een zorgvuldige migratie naar quantumveilige cryptografie en dat deze markt vooral wordt gevoed door Nederlandse bedrijven, en met kennis en innovaties die in Nederland ontwikkeld zijn. Hiervoor is cryptografie ook opgenomen in de Agenda Digitale Open Strategische Autonomie[1] die de Kamercommissie DIZA 17 oktober jl. heeft ontvangen van de minister van EZK.

Bij **vraag 4 en 5** geeft u aan dat:

- De Amerikaanse wetgeving zich richt op de verplichting van het implementeren van één oplossing om weerbaar te zijn tegen de dreiging van quantumtechnologie. En geeft u onderbouwing waarom de aanpak van de Rijksoverheid past bij de generieke aanpak voor digitale weerbaarheid: een risicogerichte aanpak.
- De huidige Europese, nationale en overheidsbrede en wet- en regelgeving op het gebied van informatiebeveiliging cq. cybersecurity (NIS2 en Baseline informatiebeveiliging Overheid - BIO) een bredere werking hebben en voldoende aanknopingspunten bieden om in actie te moeten komen.

Politieke context

- In september 2022 heeft u Kamervragen beantwoord naar aanleiding van de schriftelijke vragen van het lid Rajkowski (VVD) inzake het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'[2].

[1] Kamerstuknr. 2023Z17637

[2] Het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'. | Tweede Kamer der Staten-Generaal

- Tijdens het IVD debat van 21 juni jl. heeft Kamerlid Rajkowski de volgende vraag gesteld: Digitale aanvallen, China grootste dreiging EV, dreiging safe now decrypt later, kabinet zet in op beter beveiliging overheid. Wilt u de regie pakken op dit thema om actiever samen te werken met het bedrijfsleven?
- Twee partijen hebben de quantumdreiging opgenomen in hun verkiezingsprogramma:
  - VVD – Nationaal actieplan Quantum: Ook werken we aan een Nationaal Actieplan Quantum om onze economie en maatschappij voor te bereiden op de veiligheidsrisico's van quantumtechnologie zodat veilige digitale communicatie ook in de toekomst mogelijk blijft.
  - VOLT – Quantum: We implementeren een centrale aanpak die ervoor zorgt dat de overheid (en met name de kritieke infrastructuur) uiterlijk in 2028 kwantumbestendig is. Codes die met de huidige technologie waterdicht zijn versleuteld kunnen namelijk eenvoudig gekraakt worden door kwantumcomputers. Daarbij moeten de overheid en het bedrijfsleven samenwerken.
  - NSC – Quantum: Experts achten de kans aanzienlijk dat een krachtige quantumcomputer over een aantal jaar de huidige vormen van encryptie kan breken, wat zou betekenen dat alle systemen in Nederland gecompromitteerd kunnen worden en alle overheidsgegevens zouden kunnen uitlekken. De overheid moet werk maken van de migratie van overheidssystemen naar quantumveilige cryptografie, met bijzondere aandacht voor verouderde systemen die een lange levensduur hebben en onze vitale processen waarborgen.

Bijlagen

Volgnummer	**Naam**	**Informatie**
1	2. ciebrief – Verzoek beantwoording kennisvragen Kwantumtechnologie	Brief met 5 kennisvragen van de Kamercommissie DIZA van 5 juli 2023
2	3.antwoorden CIE-brief DIZA kwantum van 05-07-2023	Brief met uw antwoorden op de 5 kennisvragen van de Kamercommissie DIZA van 5 juli 2023