Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER INFORMATIE

Nota actief openbaar
Ja

Onze referentie
2024-0000077926

Datum
1 februari 2024

Opgesteld door
[redacted]

Samengewerkt met
Ministerie van JenV

Bijlage(n)
2

Aan Staatssecretaris Koninkrijksrelaties en Digitale Zaken
Van CIO Rijk

nota

oplegnota kamervragen Kamerlid Sneller over Quantumproof encryptie

Aanleiding

Kamerlid Sneller heeft 16 januari jongstleden bovengenoemde kamervragen gesteld. De set van 9 vragen is aan u gericht en aan de Minister van Justitie en Veiligheid.
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 JenV. U tekent mede namens haar.

Geadviseerd besluit

- Akkoord gevraagd met verzending van de brief met de antwoorden naar de Tweede Kamer.

Kern

Deze vragen komen voor een groot deel overeen met de kamervragen van de Kamercommissie Digitale Zaken, die u afgelopen november heeft beantwoord[1].
Over deze vragen bent u toen ook mondeling bijgepraat.
Voor een groot deel zijn de antwoorden van die brief dan ook verwerkt in de bijgevoegde beantwoording, daar waar dat zinvol is. Of er wordt verwezen naar de vorige brief, daar waar dat logisch is.
Belangrijke verschillen ten opzichte van de vorige vragenset:

- De vragen zijn mede gesteld aan de minister van JenV; de vorige kamervragen waren mede gesteld aan minister van EZK.
- Er is in deze vragenset meer aandacht voor internationale samenwerking en onderzoek op dit onderwerp.

Toelichting op de beantwoording.

Alle antwoorden zijn passend binnen de context van de dreiging van de Quantumcomputer voor Cryptografie.

Vraag 1,2, gaan over de bekendheid van u over de dreiging en de geziene kansen en risico's. In Uw antwoord:

- Geeft u aan dat u met de dreiging bekend bent en licht deze verder toe.

[1] Antwoorden op Kamervragen over gevolgen kwantumtechnologie voor encryptie | Kamerstuk | Rijksoverheid.nl

- Verwijst u naar uw brief van november jl. als het gaat over de knelpunten en kansen die de transitie naar quantumveilige cryptografie met zich meebrengen.
- U voegt ten opzichte van de brief van 7 november het risico van onvoldoende bewustzijn en kennis toe. Om de kennis van alle typen IT-beheerders op dit vlak te vergroten ontwikkelt u in samenwerking met de private sector een cryptografie bijscholing voor deze doelgroep. De opleiding komt naar verwachting in de loop van dit jaar beschikbaar.

Vraag 3 en 4 gaan over de Amerikaanse wetgeving op dit punt en in hoeverre dergelijke wetgeving voor Nederland nodig is of wordt voorbereid. In uw antwoorden:

- Geeft u aan dat de Amerikaanse wetgeving zich richt op de verplichting van het implementeren Post Quantum Cryptografie 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 wet- en regelgeving op het gebied van informatiebeveiliging c.q. cybersecurity (NIS2 en Baseline informatiebeveiliging Overheid - BIO) een bredere werking hebben en voldoende aanknopingspunten bieden om in actie te moeten komen.

Vraag 5, 6 en 9 gaan over de ondersteuning aan de Rijksoverheid, de voorbereidende stappen die organisaties nu al kunnen zetten en de maatregelen die u op korte termijn treft. In uw antwoorden:

- Verwijst u naar de brief van november jl. daar waar het gaat over 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.
- Noemt u het PQC migratie handboek van de AIVD; dat maakt eveneens deel uit van de regie. Het is ontwikkeld in samenwerking met TNO en CWI. U heeft dit handboek 4 april 2023 in ontvangst genomen.
- Gaat u voor wat betreft de Nationale Cryptostrategie 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.
- Beschrijft u de rol van en samenwerking met EZK en de routekaart cryptocommunicatie van dcypher.

Vraag 7 gaat over nationale en Europese samenwerking aangaande de komst van de qauntumcomputer en de gevolgen voor encryptie.

- U benoemt de Amerikaanse NIST competitie als de meest belangrijke samenwerking op dit vlak: doel is om post quantum cryptografie standaarden vast te stellen.
- U geeft aan dat er samenwerkingsverbanden bestaan met Duitse en Franse nationale informatiebeveiligingsinstituten. Momenteel wordt besproken op welke onderwerpen de samenwerking en kennisdeling op het gebied van de quantumdreiging geïntensiveerd kunnen worden.

Vraag 8 gaat over onderzoek dat wordt uitgevoerd op dit onderwerp

- U gaat in op 2 onderzoeken die zijn gefinancierd door departementen in gezamenlijkheid.
- Daarnaast geeft u aan dat er op veel onderzoek wordt gedaan ook door private partijen en dat hier kennis over wordt gedeeld. U geeft een voorbeeld van een congres waarin dit gebeurde.

Politieke context

- U heeft afgelopen 7 november een brief gestuurd naar aanleiding van vergelijkbare vragen van de Kamercommissie Digitale zaken[2]
- 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	2024Z00327; kamervragen Quantumproof encryptie	Dit document bevat de set kamervragen
2	De Kamerbrief beantwoording kamervragen Quantumproof encryptie	De brief met uw antwoorden

[2] Antwoorden op Kamervragen over gevolgen kwantumtechnologie voor encryptie | Kamerstuk | Rijksoverheid.nl