Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1178

Vragen van het lid **Sneller** (D66) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *quantumproof encryptie* (ingezonden 16 januari 2024).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 7 maart 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, 1028

Vraag 1
Bent u bekend met het risico dat quantumcomputing encryptie zal doorbreken en daarmee toegang wordt verkregen tot een schat aan gevoelige informatie?

Antwoord 1
Ja, het is mij bekend dat krachtige quantumcomputers bepaalde versleuteling (of cryptografie) sterk kunnen verzwakken of doorbreken. Dit veroorzaakt risico's voor de Rijksoverheid en ook voor burgers, ondernemingen en andere overheden die tijdig beheerst moeten worden.
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 (vertrouwelijkheid). Daarnaast wordt het ingezet om gegevens te beschermen tegen wijzigingen (integriteit), zekerheid te verkrijgen van verzenden en ontvangen van informatie (onweerlegbaarheid) en bevestiging van identiteiten van zender en ontvanger te bewerkstelligen (authenticatie). Daarvoor zijn in ons dagelijks leven zeer veel toepassingen en cryptografie wordt om die reden 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 instrument om de vertrouwelijkheid, integriteit en beschikbaarheid van processen en data te beschermen.
Met de komst van een krachtige quantumcomputer is de meeste cryptografie echter niet meer (voldoende) veilig: bestaande encryptiemethodes zullen onze digitale gegevens niet meer voldoende kunnen beschermen.
De overgang van kwetsbare cryptografie naar quantumveilige cryptografie is een technologisch ingrijpende wijziging die nog niet eerder op deze schaal is

ah-tk-20232024-1178
ISSN 0921 - 7398
's-Gravenhage 2024

voorgekomen. Daarom moeten er nu voorbereidende acties worden ondernomen, zie ook de beantwoording bij vraag 5.

Vraag 2
Welke kansen en risicos ziet u op het gebied van quantum?

Antwoord 2
Er zijn met betrekking tot quantum in relatie tot quantumproof encryptie zowel kansen als risico's.
In mijn brief van 7 november 2023[1] heb ik u geïnformeerd over een aantal belangrijke knelpunten in de transitie naar quantumveilige cryptografie en een aantal kansen die dit biedt.
Daarnaast zijn er risico's zoals onvoldoende bewustzijn en kennis. Voor dat laatste ontwikkel ik samen met de private sector een cryptografie opleiding om alle typen IT- beheer bij te scholen. Deze komt naar verwachting in de loop van 2024 beschikbaar.

Vraag 3
Bent u bekend met het gegeven dat de Amerikaanse president Biden reeds een wet heeft getekend die overheidsorganisaties verplicht om te migreren naar IT-systemen die quantum-proof zijn?[2]

Antwoord 3
Het kabinet volgt de internationale ontwikkelingen en heeft kennis genomen van de genoemde Amerikaanse wetgeving[3]. Deze wetgeving geeft de verplichting aan federale overheidsinstanties om te migreren naar quantumveilige cryptografie: het adopteren van de standaarden die door het Amerikaanse National Institute of Standards and Technology dit jaar gepubliceerd worden om weerbaar te zijn tegen de dreiging van quantumtechnologie. Deze migratie en beschreven aanpak hiervoor worden ook binnen de Rijksoverheid gezien als de belangrijkste instrumenten om deze dreiging het hoofd te bieden.
De aanpak van de Rijksoverheid past bij de generieke, risicogerichte aanpak voor digitale weerbaarheid. Deze aanpak geeft ruimte om ook andere maatregelen te nemen om de hiervoor genoemde risico's te beheersen, indien bijvoorbeeld bepaalde systemen niet kunnen migreren naar quantumveilige cryptografie.

Vraag 4
Kunt u toelichten in hoeverre er vergelijkbare wetgeving nodig is in Nederland en in hoeverre dit wordt voorbereid?

Antwoord 4
De Amerikaanse wetgeving oplossing verplicht federale overheidsinstanties om te migreren naar quantumveilige cryptografie: namelijk het adopteren van de nieuwe standaarden van National Institute of Standards and Technology (zie vraag 3). De huidige Europese, nationale en overheidsbrede wet- en regelgeving op het gebied van informatiebeveiliging c.q. cybersecurity heeft een andere werking maar biedt voldoende aanknopingspunten om in actie te moeten komen.
Zo geeft NIS2[4] (Network and Information Security Directive) aan dat «state of the art» beveiligingsmaatregelen waaronder «state of the art» encryptie moeten worden toegepast. Deze richtlijn schrijft verder voor dat organisaties die onder de richtlijn vallen moeten hebben: «beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie».[5] De gekozen maatregelen om de systemen te beveiligen volgt uit de risicoanalyse van de

---

[1] Antwoorden op Kamervragen over gevolgen quantumtechnologie voor encryptie | Kamerstuk | Rijksoverheid.nl
[2] Forbes, Januari 25, 2023. What The quantum Computing Cybersecurity Preparedness Act Means For National Security (forbes.com)
[3] Text – H.R.7535 – 117th Congress (2021–2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress
[4] Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (NIS2-richtlijn) | Shaping Europe's digital future (europa.eu)
[5] NIS directive 2; onder andere art 21 (2).

te beveiligen informatie. De Minister van Justitie en Veiligheid heeft de Kamer per brief op 31 januari geïnformeerd over de voortgang van de implementatie van de richtlijn.
Daarnaast vereisen de Baseline Informatiebeveiliging Overheid (BIO) en de voor de overheid verplichte ISO-standaarden[6] dat nieuwe dreigingen en risico's worden opgenomen in het risicomanagementproces. Deze standaarden bevatten normen ten aanzien van beleid en beheer van cryptografie. Ook andere eisen zorgen ervoor dat organisaties moeten starten met het beheersbaar maken van de dreiging van de quantumcomputer voor cryptografie – die daar kwetsbaar voor is. Een voorbeeld is de eis rondom het beheersen van kwetsbaarheden.

Vraag 5
Welke ondersteuning wordt er nu vanuit de Rijksoverheid geboden aan organisaties om zich voor te bereiden op de komst van quantumcomputers en de effecten op encryptie?

Antwoord 5
De benodigde veranderingen om gegevens 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 is een Rijksbreed samenwerkingsprogramma opgezet: quantumveilige Cryptografie (QvC-Rijk). Hierover heb ik u in mijn brief van afgelopen november geïnformeerd[7]

Vraag 6
Welke stappen kunnen organisaties nu al nemen om gegevens te beschermen tegen de komst van quantumcomputers?

Antwoord 6
Veel (overheids)organisaties en IT-leveranciers moeten zich nu al voorbereiden op risico's die de komst van de quantumcomputer met zich meebrengen. Bijvoorbeeld organisaties die data verwerken, die over langere tijd nog vertrouwelijk moeten blijven zoals medische data of bedrijfsgeheime data. Of organisaties die systemen met een lange levensduur aanbieden, zoals bijvoorbeeld industriële automatisering[8].
De volgende acties kunnen nu al door bedrijven en (overheids)instanties ondernomen worden:
- Inzicht hebben in wat belangrijk is om te beschermen: de «kroonjuwelen»
- De quantumdreiging en het gebruik van cryptografie meenemen in het risicomanagementproces
- De sleutels van symmetrische cryptografie verlengen, waardoor de beveiligingswaarde verhoogt. Zo wordt encryptie standaard «AES-256» momenteel als quantumveilig beschouwd.
- Eisen toevoegen voor (toekomstige) cryptografie in aanbestedingen.

De volgende maatregelen kunnen worden getroffen om wijzigingen voor te bereiden, die op een later moment noodzakelijk zullen zijn:
- Weten waar welke cryptografie gebruikt wordt en dit borgen in het beheer van IT-bedrijfsmiddelen.
- Doorvoeren van voorbereidende wijzigingen zoals het vervangen van het cryptografisch protocol «Transport Layer Security» versie 1.2, door de gelijknamige versie 1.3.
- Met leveranciers in gesprek gaan over cryptografie in hun producten.

Vraag 7
In hoeverre wordt er internationaal of in Europees verband samengewerkt aan de voorbereiding van versterkte encryptie(-vereisten) voor de komst van quantumcomputers?

---

[6] Zie met name ISO 27001 en ISO 27002; ISO staat voor Internationale Organisatie voor standaardisatie
[7] Antwoorden op Kamervragen over gevolgen quantumtechnologie voor encryptie | Kamerstuk | Rijksoverheid.nl
[8] https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek

Antwoord 7
Een heel bekende samenwerking op dit vlak is de Amerikaanse National Institute of Standards and Technology competitie voor Post quantum cryptografie[9]. Nederland heeft ook een inzending gedaan, welke is geselecteerd (CRYSTALS-KYBER)[10] om in de nieuwe wereldwijde standaarden op te nemen.
Daarnaast wordt door de wetenschap ook op dit onderwerp internationaal samengewerkt (zie vraag 8).
Met de Franse en Duitse nationale informatiebeveiligingsinstituten bestaan onder andere vanuit de Rijksoverheid al langer samenwerkingen generiek op cybersecurity en ook cryptografie. Momenteel wordt besproken op welke onderwerpen de samenwerking en kennisdeling op het gebied van de quantumdreiging geïntensiveerd kunnen worden.

Vraag 8
Welk onderzoek wordt er nu verricht naar quantumcomputing, en meer specifiek naar de gevolgen voor encryptie?

Antwoord 8
Departementen hebben gezamenlijk geld beschikbaar gesteld voor het oplossen van een aantal vraagstukken over cybersecurity. Dit heeft geleid tot een programma: Cybersecurity – naar een veilig en betrouwbaar digitaal domein[11].
Binnen dit programma lopen 2 onderzoeken op het vlak van cryptografie:

- «HAPKIDO (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations)»
  Doel van dit onderzoek is om quantumveilige PKI-systemen te ontwikkelen en sector-gebaseerde groeipaden te leveren die organisaties zullen helpen hun systemen naar een quantumveilige toekomst te migreren. Dit gebeurt in samenwerking met koplopers in de telecommunicatie, financiële dienstverlening, zorg en publieke sector.
- «PROACT – Physical Attack Resistance of Cryptographic Algorithms and Circuits with Reduced Time to Market»
  Doel van dit onderzoek is het ontwerpen van nieuwe algoritmen en siliciumchips met inherente bescherming tegen fysieke aanvallen, en het ontwikkelen van nieuwe simulatie- en evaluatietechnieken voor fysieke beveiliging. PROACT zal daarom bijdragen aan een verhoogde beveiliging van onze persoonlijke en bedrijfsgevoelige gegevens.

Op veel meer plekken wordt op dit vlak onderzoek gedaan, zowel door onderzoek en wetenschap, maar ook door private partijen. Tijdens congressen wordt hierover kennis gedeeld. Een recent voorbeeld hiervan in Nederland is het congres van het PKI-consortium van afgelopen november. Het PKI-consortium heeft dit congres georganiseerd samen met de Rijksoverheid (Logius) en onderzoeksorganisaties (Centrum voor Wiskunde en Informatica-CWI- en TNO)[12].

Vraag 9
Welke maatregelen neemt de Staatssecretaris op korte termijn ter voorbereiding op de komst van quantumcomputers?

Antwoord 9
Onder regie van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties wordt de migratie naar quantumveilige cryptografie binnen de Rijksoverheid voorbereid. Voor wat betreft het programma quantumveilige Cryptografie Rijk (QvC-Rijk): zie antwoord bij vraag 5.
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.

---

[9] Post-Quantum Cryptography | CSRC (nist.gov)
[10] CWI involved in two primary Post-Quantum Cryptography standards
[11] 10 miljoen euro toegekend voor het oplossen van vraagstukken over cybersecurity | NWO
[12] Post-Quantum Cryptography Conference – November 7 and 8, 2023 – Amsterdam (NL) | PKI Consortium

In brede zin maakt het voorbereiden op quantumveilige cryptografie deel uit van de Nederlandse Cybersecuritystrategie 2022–2028[13]. 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.

- 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.
- 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 vorige jaar een handboek gepubliceerd over de migratie naar quantumveilige cryptografie[14]. Dit handboek biedt 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[15].
- dcypher werkt samen met bedrijfs- en overheidspartijen om verdere ontwikkeling en adoptie van het handboek vorm te geven.

[13] Nederlandse Cybersecuritystrategie 2022–2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

[14] https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek

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