Artikel 44 vragen - Digitale Quantum veiligheid

1. Is GS op de hoogte van het artikel in het Financieel Dagblad van afgelopen donderdag 5 februari 2026, naar aanleiding van het rekenkamerrapport “Focus op quantum bij de Rijksoverheid”?

2. Ziet GS het gevaar van Q-day? Oftewel het moment rond 2030 dat de snelle rekenkracht van de quantum computer de Zeeuwse digitale sloten kan kraken?

3. Heeft GS in beeld wat dit kan betekenen voor de Zeeuwse samenleving? M.a.w. maakt dit onderdeel uit van de risico analyse van Zeeland?

4. Klopt het dat bijvoorbeeld in geval van nood onze stormvloedkering niet kan sluiten door ontwrichting via quantum computers?

5. Welke veiligheidsmaatregelen neemt de Provincie Zeeland NU om voorbereid te zijn op Q-day in 2030? Denk aan samenwerking RIJK, risico-inventarisatie Zeeland, prioritering bescherming, externe ICT-leveranciers.

6. Gaat digitale quantum veiligheid een plek krijgen in de digitale agenda? Zo ja, op welke manier past dat er dan het beste in?

Christine Govaert
BBB Zeeland

TECH EN MEDIA

Rekenkamer: kwantumcomputer kan over 4 jaar leven 'ontwrichten'

Rijksoverheid is te laks met de bescherming van data en digitale systemen

Jan Fred van Wijnen
Amsterdam

Vijandige mogendheden kunnen over vier jaar de sluizen en waterkeringen in Nederland hacken en overnemen, zo stelt de Algemene Rekenkamer. Ook data voor paspoorten en DigiD zijn vanaf 2030 te manipuleren door hackers en spionnen. Volgens de financiële toezichthouder op het Rijk breekt in dat jaar 'Q-day' aan: de dag dat kwantumcomputers elke huidige beveiliging van data en apparatuur kunnen kraken.

De Rijksoverheid is nauwelijks voorbereid op deze situatie, zo meldt de Rekenkamer in een rapport dat gisteren in een besloten sessie met de Tweede Kamer is besproken. Bijna driekwart van de overheid moet nog beginnen met beschermende maatregelen, terwijl de staatssecretaris Digitalisering al een jaar geleden een hulpprogramma hiervoor heeft aangeboden.

Rekenkamer-bestuurder Ewout Irrgang had 'gehoopt' dat de uitkomst beter zou zijn, zegt hij in een toelichting. 'We praten niet over theoretische scenario's. Het kan ineens gebeuren dat de stormvloedkering niet dichtgaat bij hoogwater.' Hij roept de overheid op om in ieder geval te beginnen met de inventarisatie van cruciale systemen waar de kwantumcomputer schade kan aanrichten.

Ook vindt Irrgang dat cruciale infrastructuur zo snel mogelijk in een Europese clouddienst moet worden beheerd: 'Ook de afhankelijkheid van Amerikaanse IT maakt Nederland kwetsbaar.' Zo'n Europese clouddienst moet dan wel 'kwantumproof' zijn, zegt hij.

> Ook data voor **paspoorten en DigiD zijn vanaf 2030 te manipuleren door hackers en spionnen**

Van de 63 onderzochte organisaties, waaronder de Belastingdienst, Nationale Politie en Inspectie Veiligheid Defensie, zijn er maar vier die de kwantumdreiging serieus nemen. De rest bespreekt het af en toe of helemaal niet. De Rekenkamer maakt niet bekend wie voor- of achterloopt.

'Wij noemen geen namen van organisaties,' zegt Irrgang, 'want dat zou de kwetsbaarheid van Nederland tegenover buitenlandse mogendheden vergroten.' Overheden in andere landen zijn overigens niet sneller in hun voorbereiding op kwantum, zegt hij.

De demissionaire staatssecretaris voor Digitalisering, Eddie van Marum (BBB), stelt in een reactie dat de departementen 'nu werk moeten maken' van hun bescherming tegen kwantumcomputers. Hij maakt hiervoor 'de benodigde middelen vrij'. Slechte beveiliging noemt hij 'een direct risico voor burgers en bedrijven'.

Kwantumcomputers werken met een nieuw soort technologie die in potentie ongeëvenaarde rekenkracht biedt. Op dit moment zijn ze nog niet in staat om de encryptie van beveiligde systemen te kraken. Maar de ontwikkeling gaat zo snel dat elke huidige vorm van versleuteling binnen een paar jaar onbeschermd zal zijn, zo denken experts. Grote techbedrijven zoals IBM en Google verwachten daarentegen dat hun kwantumcomputers pas na 2033 superieur zijn aan de beste klassieke computer van vandaag.

De Rekenkamer vindt dat de overheid rekening moet houden met een eerdere doorbraak in kwantumtechnologie. Vandaar de waarschuwing dat hackers vanaf 2030 ongekende schade kunnen aanrichten, zoals 'de sluizen openzetten' of het manipuleren van gevoelige data.

Vervolg op pagina 3

Vervolg van pagina 1

Paspoorten, fiscale informatie en het Kadaster zijn dan niet meer te vertrouwen. Dit kan de samenleving 'ontwrichten', aldus de Rekenkamer.

De veiligheidsdienst AIVD begon al in 2014 met waarschuwingen voor Q-day (de q verwijst naar de Engelse schrijfwijze 'quantum'). De AIVD zelf is niet onderzocht door de Rekenkamer, zegt bestuurder Irrgang, 'in verband met de gevoeligheid van de inlichtingen'. De onderzoekers zijn wel 'in gesprek' geweest met de inlichtingendienst over de noodzaak van kwantumbeveiliging.

De traagheid van de Rijksoverheid is opmerkelijk, omdat de nationale cyberwaakhond NCSC al enkele jaren waarschuwt voor het kwantumrisico. Ook is een handboek voor kwantumbeveiliging beschikbaar bij de inlichtingendienst AIVD en onderzoeksinstelling TNO.

> Een handboek voor **kwantumbeveiliging is beschikbaar bij de inlichtingendienst AIVD en bij TNO**

De bescherming tegen kwantuminbraken is nog in ontwikkeling. Data en wachtwoorden kunnen beveiligd worden met nieuwe algoritmes, die ook voor de kwantumcomputer te complex zijn om te kraken. Deze versleuteling heet 'post quantum cryptografie'. De Amerikaanse overheidsorganisatie Nist heeft sinds kort drie van zulke algoritmes beschikbaar gesteld. Ze zijn ontwikkeld in een prijsvraag die in 2016 werd uitgezet.

De Rekenkamer is wel lovend over de Nederlandse toppositie in kwantumtechnologie. Die is mede mogelijk gemaakt door staatssubsidies van €615 mln, die uit het Nationale Groeifonds komen. Maar dat geld is na volgend jaar helemaal uitgegeven en er is nog geen besluit genomen over nieuwe overheidsinvesteringen. Andere landen investeren juist wel miljarden in de nieuwe technologie. Daarom waarschuwt de Rekenkamer voor het verlies van de Nederlandse voorsprong.