



VVD schudt ministers wakker over cryptokrakers met kwantumcomputers

Amerikanen al bezig met wapens, actie in Nederland vereist.

2

© Shutterstock.com

28 JULI 2022



De VVD heeft de ministers van Justitie en Veiligheid en Economische Zaken en Klimaat gevraagd naar concrete stappen tegen het gevaar dat criminelen met kwantumcomputers aan de slag gaan. De vragen werden gesteld naar aanleiding van een verhaal in AG Connect.

AG Connect schreef onlangs over het Amerikaanse National Institute for Standards and Technology (NIST), dat inmiddels **een selectie samenstelde uit vele voorstellen** ter vervanging van huidige encryptiemethoden die straks eenvoudig zijn te kraken met een kwantumcomputer.

Kamerlid Queeny Rajkowski wil nu van de ministers weten of zij het ermee eens zijn dat kwantumcomputers een serieus gevaar kunnen vormen voor het Nederlandse briefgeheim en veilige communicatie tussen veiligheidsdiensten en Nederlandse burgers. Ze vraagt hoe de minister het gevaar beoordeelt en welke concrete stappen en voorbereidingen er gezet zijn en worden in de komende jaren.

Rajkowski wil onder meer ook weten of de ministers hierin samen optrekken met experts en bedrijven om oplossingen te vinden waarmee encryptie bestendig kan worden gemaakt tegen de komst van kwantumcomputers en net als het Amerikaanse NIST een selectie heeft gemaakt van alternatieve cryptografische methoden die niet vatbaar zijn voor het kwantumrekengeweld.

Podcast

De kwantumcomputer lijkt nog ver weg. Maar kopieën van alle data die nu versleuteld worden verstuurd, komen ergens in een database terecht. Ook al wil je dat niet. Die informatie ligt straks open en bloot. En er zijn meer redenen om nu al te zorgen dat gegevens straks nog steeds veilig zijn.

[AG Connect ging hierover in een podcast](#)

[in gesprek](#) met Maran van Heesch, Quantum Security specialist TNO, en Ronald Cramer, hoogleraar Cryptologie aan de Universiteit Leiden en groepsleider Cryptologie aan het Centrum Wiskunde & informatica (CWI)

Waarschuwingen

Hoogleraar ICT Recht aan de Universiteit Tilburg Lokke Moerel, die gespecialiseerd is op het gebied van digitaliseringsstrategie en cybersecurity, waarschuwde onlangs [in een debat in de Balie](#) dat de huidige encryptie die nu gebruikt wordt om informatie te beschermen, niet bestand is tegen de rekenkracht van kwantumcomputers.

Lees meer over: [encryptie](#), [kwantumcomputer](#)



SJOERD HARTHOLT

is redacteur bij AG Connect.

GERELATEERDE ARTIKELEN



NIST kiest wapens tegen kwantumcomputer als cryptokraker



Lokke Moerel: Huidige encryptie is niet bestand tegen kwantumcomputer



→ Kwantumcomputer bedreigt straks encryptie: kom nu in actie