

Quantumcomputer vormt ook bedreiging voor onze gegevensbescherming

Quantum technologie

23 september 2022

Met quantumtechnologie staan we aan de vooravond van een technologische revolutie die een bijdrage kan leveren aan het oplossen van allerlei maatschappelijke uitdagingen. Tegelijkertijd is het van belang dat we ons als land tijdig wapenen tegen de cyberdreiging die deze technologie ook oplevert. De quantumcomputer verdient dan ook een hoge plaats op de nationale digitale veiligheidsagenda.

Onze cyberveiligheid wordt momenteel geborgd door cryptografische versleuteling die onder andere wordt ingezet om informatie af te schermen van onbevoegden en om de herkomst van een bericht te verifiëren.

Deze versleuteling is veelal gebaseerd op rekensommen die met computers van vandaag nauwelijks op te lossen zijn. Zelfs de snelste computers doen er tientallen tot honderden jaren over om versleutelde informatie te ontcijferen. Met de komst van de quantumcomputer komt hier verandering in.

Quantumcomputers kans vs dreiging

Quantumcomputers gaan een grote maatschappelijke bijdrage leveren door problemen op te lossen waarvoor er nu nog te weinig rekenkracht beschikbaar is. Denk aan de ontwikkeling van (gepersonaliseerde) medicijnen. Dit is echter een vooruitgang met een keerzijde.

Met ongekende rekenkracht is een quantumcomputer ook in staat om veel versleutelde informatie binnen een mum van de tijd te ontcijferen en worden staats- of bedrijfsgeheimen toegankelijk voor partijen met kwade bedoelingen. Dit vormt een risico voor onze nationale veiligheid en economie.

Wachten is geen optie meer

De ontwikkeling van quatumtechnologie en het benutten van de vele kansen is in volle gang. Zo werkt TNO met onder meer de TU Delft samen in QuTech aan de eerste schaalbare quantumcomputer en veilig quantuminternet.

Tegelijkertijd moeten we ook werken aan onze cyberveiligheid. Het 'quantum safe' maken van de huidige IT-systemen is zeer complex en vraagt veel tijd. Ondertussen kunnen kwaadwillenden vertrouwelijke informatie nu al onderscheppen en opslaan om later te ontcijferen, zodra de quantum computer er is. Ook wel 'store now, decrypt later' genoemd.

Omdat veel vertrouwelijke informatie een lange geheimhoudingstermijn heeft, vormt dit een reële, maar ook zeer acute dreiging. Al lijkt de quantumcomputer meer dan tien jaar van ons verwijderd, het is voor onze veiligheid nu al hard nodig om te werken aan quantum-safe cryptografie.

Tijd voor actie

Het is noodzakelijk dat, net als in andere landen, de overheid nu al voor onze nationale veiligheid, de Nederlandse economie en vitale sectoren de risico's in kaart brengt. Zodat inzichtelijk wordt wat de omvang en reikwijdte van deze uitdaging is.

Binnen bedrijven en overheidsorganisaties is het essentieel dat op technisch niveau in kaart wordt gebracht waar cryptografie wordt gebruikt die niet toekomstbestendig is en wat de implicaties daarvan zijn. Daarnaast is het van belang om als land tijdig te investeren in ontwikkeling van kennis en middelen om impact-analyses en migraties makkelijker en minder arbeidsintensief te laten verlopen.

Het is hoogst urgent dat de overheid, het bedrijfswezen en kennisinstellingen deze handschoen oppakken om onze staatsgeheimen, bedrijfsinformatie en toegang tot kritieke infrastructuur voldoende te beschermen.

Binnen de Nederlandse overheid wordt er momenteel interdepartementaal samengewerkt aan een plan voor de migratie naar quantum-safe cryptografie. Daarnaast zal TNO, samen met de AIVD en de cryptologie groep van het CWI, begin 2023 een migratiehandboek publiceren. Dit handboek biedt concrete handvatten om de migratie op gang te brengen.

Neem contact met ons op





Meer over Thomas →

Den Haag – New Babylon

+31 88 866 73 53

E-mail Thomas

Thomas op LinkedIn

Thomas Attema



Daniël Worm

Senior consultant



Maran van Heesch

Senior consultant



Patrick de

Laat je verder inspireren

Alles

Nieuws

Artikel

Evenement

Insight

Podcast

Webinar

Artikel

Quantum computing: wat kan jouw organisatie ermee?

Problemen real-time oplossen met quantum computing toepassingen? De enorme rekenkracht biedt mogelijkheden voor AI, optimalisatie en materiaalkunde.

Lees meer

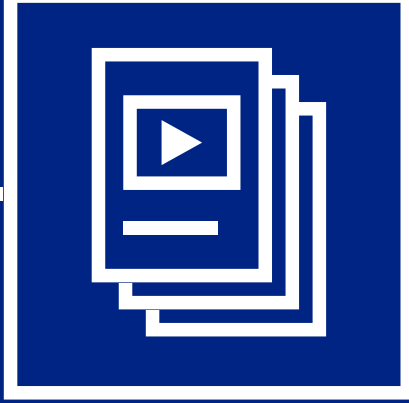


Artikel

Cyber security technologieën

Wat vandaag veilig is, is dat morgen misschien niet meer. Daarom werken we bij TNO Cyber security technologies aan de cybersecurity-innovaties van morgen.

Lees meer

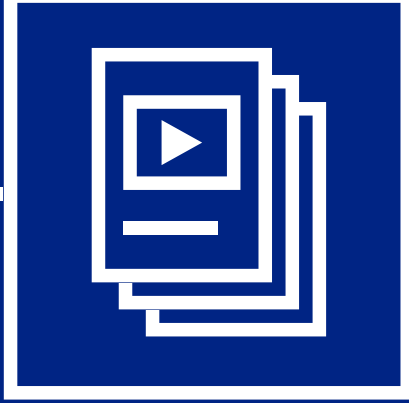


Artikel

Automated Security voor een veilige digitale economie

Automated Security is nodig om cyberaanvallen tijdig af te wenden. Samen met partners ontwikkelen we een tweetal cybersecurity-oplossingen voor de markt.

Lees meer



Artikel

Cybersecurity door quantum-safe crypto

De quantum computer biedt kansen en risico's. Bij TNO helpen we bedrijven met quantum-safe crypto netwerken te beveiligen en legacy-problemen op te lossen.

Lees meer



Artikel

Zorgeloos ondernemen dankzij security monitoring en detectie

Met Security Monitoring en Detectie kunnen bedrijven pro-actief hun netwerkverkeer en data analyseren om vroegtijdig verdachte patronen te signaleren.

Lees meer



Meer ↓

Hier werken we aan

Duurzaam

Gezond

Veilig

Digitaal

Sectoren

Werken bij

Newsroom

Agenda

Webinars

Insights

Podcasts

Abonneren TNO Update

Over TNO

Missie en strategie

Organisatie

Onze mensen

Contact

TNO en de maatschappij

Communities

Technologie en wetenschap

Laboratoria

Technologieën

Tech Transfer

Octrooien en licenties

Werken bij

Vacatures

TNO als werkgever

Professionals

Studenten en starters

Maak kennis met TNO

English

Privacy on this site

We collect and process your data on this site to better understand how it is used. You can give your consent to all or selected purposes, or you can decline them all. For more information, see our privacy policy.

Analytics

Conversion tracking

Remarketing

3rd party video

Consent details

Privacy policy

Accept all

Decline all

Powered by PIWIK