De race tegen kwantumcomputers

Actie en regie nodig om cyberaanvallen te voorkomen

Verslag van het minisymposium Parlement & Wetenschap 'Klaar voor kwantum? De gevolgen van kwantumtechnologie voor de veiligheid', gehouden op 10 mei 2023 in in de Max van der Stoelzaal van de Tweede Kamer, georganiseerd door de Tweede Kamer, in samenspraak met Parlement & Wetenschap.

De komst van kwantumcomputers brengt grote risico's met zich mee voor de beveiliging van gegevens. In een minisymposium kwamen experts en Tweede Kamerleden samen om de gevolgen hiervan te bespreken. In een volle Max van der Stoelzaal, met zo'n honderd bezoekers, werd duidelijk dat urgente actie nodig is. Nederland loopt achter bij de invoering van veilige techniek, die bestand is tegen cyberaanvallen van kwantumcomputers. Wat moet er *nu* gebeuren om de risico's te beperken en hoe kan de overheid zich hierop voorbereiden?

Als de bedreigingen worden weggenomen, blijven de positieve kanten van kwantumcomputers over: hun grote rekenkracht belooft vooruitgang te brengen bij veel maatschappelijke vraagstukken.

Grote rekenkracht

Lieven Vandersypen legde aan het begin van de bijeenkomst uit hoe kwantumcomputers werken en hoe ze in de toekomst beveiligde gegevens kunnen kraken. Hij is hoogleraar aan de TU Delft en wetenschappelijk directeur van QuTech, een instituut waarin TU Delft en TNO samenwerken. Kwantumcomputers werken volgens een ander principe dan klassieke computers en kunnen daardoor miljoenen berekeningen tegelijk uitvoeren. Klassieke computers doen berekeningen stapsgewijs na elkaar. Kwantumcomputers zijn door hun parallelle werkwijze onvergelijkbaar veel sneller en kunnen in de toekomst complexe opgaven oplossen die voor klassieke computers te moeilijk zijn.

Zodra kwantumcomputers krachtig en betrouwbaar genoeg zijn, is de huidige cryptografische beveiliging van internet en van gegevensbestanden op slag waardeloos. Zover is het nog niet, want de beste kwantumcomputers hebben nu nog slechts enkele tientallen geheugencellen ('qubits'). Wereldwijd wordt in laboratoria echter hard gewerkt om de prestaties te verbeteren. Experts spreken van 'Q-Day', de dag dat de huidige beveiliging van informatie bezwijkt onder de rekenkracht van kwantumcomputers.

‘Dat duurt nog zeker tien jaar’, denkt Lieven Vandersypen. ‘Misschien wel vijftien jaar’, zo was later op de middag de schatting van Marc Stevens van het Centrum Wiskunde & Informatica. Maar beiden benadrukten dat het omschakelen naar nieuwe technieken, die veilig zijn voor kwantumcomputers, ook lang duurt. ‘Voor sommige toepassingen zijn we al te laat’, aldus Marc Stevens.

De kwantumcomputer heeft ook veel nuttige toepassing, zo liet Lieven Vandersypen zien. De snelle berekeningen zullen preciezer inzicht geven in chemische reacties. Dat leidt tot betere medicijnen, accu's en zonnecellen. ‘Kwantumcomputers zijn daarom belangrijk voor de energietransitie en voor gezondheidszorg. Als we erin slagen om de problemen met de beveiliging op te lossen, blijven de nuttige toepassingen over’, aldus Lieven Vandersypen.

Actie en regie

De overheid moet nu al maatregelen nemen, stelt Nitesh Bharosa. Hij is hoogleraar aan de TU Delft en wetenschappelijk directeur van Digicampus, een centrum voor digitale publieke dienstverlening. De maatschappij raakt ontwricht als communicatie niet meer beveiligd kan worden. Vertrouwelijkheid is niet meer gewaarborgd en de echtheid van berichten kan niet meer gecontroleerd worden. Banken kunnen dan niet meer vertrouwen op digitale overboekingen en hebben geen andere mogelijkheid dan te stoppen met het geldverkeer. Digitale handtekeningen zijn niet meer te controleren waardoor DigiD en het netwerk van overheidsdiensten onbruikbaar worden.

Ook de huidige communicatie loopt gevaar. Kwaadwillenden kunnen nu al versleutelde gegevens bewaren zodat ze die later, na Q-Day, kunnen kraken. Dat kan leiden tot misbruik.

Beveiliging die bestand is tegen de rekenkracht van kwantumcomputers is nu al beschikbaar en zal in 2024 volledig zijn vastgelegd in standaarden, zodat die overal op dezelfde manier kan worden ingevoerd. De omschakeling kan daarom alvast worden voorbereid. ‘Maar er zijn veel partijen die betrokken zijn bij het beveiligen van informatie, er is geen coördinatie’, aldus Nitesh Bharosa. ‘De rijksoverheid moet bij die migratie een leidende rol nemen.’

Queeny Rajkowski (Tweede Kamer, VVD) reageert met de constatering dat vertrouwen in systemen een belangrijk onderwerp is voor de Tweede Kamer. Het gevaar van kwantumcomputers is volgens haar een complex onderwerp, waarvoor de hulp van experts nodig is. ‘Kwantumcomputers moeten we niet alleen als een innovatie zien. Er is meer sturing vanuit de overheid nodig, meer landelijke regie. Het gaat om bestuurlijke verantwoordelijkheid en bescherming van de rechtstaat. Dat zijn bij uitstek onderwerpen waarover de Tweede Kamer gaat.’ We moeten voorkomen dat bedrijven de kwantumtechniek monopoliseren, vindt zij. De rijksoverheid moet

tegenwicht geven. Dat geldt ook Europees. We kunnen het in goede banen leiden als de Europese Commissie keuzes maakt over wat wel en niet kan en daarop goed toezicht houdt.'

Draaiboek voor maatregelen

Daarna ging Maran van Heesch in op de omschakeling naar beveiliging die ook bestand is tegen kwantumcomputers. Zij is bij TNO senior consultant kwantumveiligheid. TNO, het CWI en de AIVD hebben samen Het PQC-migratiehandboek samengesteld voor de overstap naar postkwantumcryptografie (PQC). Daarin wordt uitgelegd hoe je kunt identificeren welke systemen in een organisatie je moet migreren en in welke volgorde. De bediening van bijvoorbeeld een sluis gaat lang mee. De sluizen die nu vernieuwd worden, moeten over twintig jaar ook nog functioneren. Het is daarom belangrijk om snel te beginnen met kritieke systemen en om ze flexibel te maken, zodat de beveiliging later ook nog goed aangepast kan worden.

TNO voert samen met andere instellingen het vijfjarig onderzoeksproject HAPKIDO uit waarin nieuwe, kwantumveilige technieken worden uitgetest. Het gaat daarbij niet alleen om de bits en bytes, maar ook om organisatie en bestuur.

Knelpunt is het geringe aantal experts. Er is bovendien kennis nodig uit verschillende domeinen. Het kost tijd om dat op te bouwen.

Lisa van Ginneken (Tweede Kamer, D66) hoopte in haar reactie dat ze droge voeten zou houden. 'Mijn angst is dat de sluizen open blijven. Als het mis gaat met onze infrastructuur hebben we grote problemen. Kunnen we binnen tien jaar de kritieke systemen voldoende beveiligen? Of moet het onderzoek naar kwantumcomputers tijdelijk stoppen, zoals nu ook voor kunstmatige intelligentie wordt bepleit?'

'We kunnen alleen ons eigen onderzoek stoppen, op andere landen hebben we geen invloed', reageerde Maran van Heesch. 'En veilige techniek is al in 2024 beschikbaar. Het is belangrijk om nu al in te zetten op *crypto agility*, zorg dat je flexibel bent in het updaten van systemen.'

Nederland op achterstand

De Verenigde Staten lopen voorop in de migratie naar kwantumveilige systemen, vertelde Marc Stevens, onderzoeker bij het Centrum Wiskunde & Informatica. Al in 2015 onderkende de National Security Agency (NSA) dat actie nodig was. Vanaf dat moment werd in standaarden vastgelegd hoe veilige technieken gebruikt moeten worden. Dat werk is in 2024 voltooid. De standaarden die dan beschikbaar komen, worden verplicht voor de federale overheid. In 2022 werd de Quantum Computing Cybersecurity Preparedness Act aangenomen, die voorschrijft dat de migratie naar veilige technieken in 2035 voltooid moet zijn.

‘VS heeft sinds 2015 een voorsprong. Nederland is nog in het stadium dat we een minisymposium over dit onderwerp houden’, aldus Marc Stevens. In Nederland is geen centrale sturing. Overheidsinstellingen zijn zelf verantwoordelijk voor migratie. Dat kan tot problemen leiden als verschillende IT-systemen moeten samenwerken. Er liggen ook nog geen deadlines vast, zoals in de VS, en er is geen centraal expertisecentrum voor de migratie. Het is ook nog niet duidelijk wanneer het gebruik van oude technieken, die niet kwantumveilig zijn, in strijd is met de Algemene verordening gegevensbescherming (AVG).

Danai van Weerdenburg (Tweede Kamer, PVV) reageert dat haast geboden is, omdat er nog veel werk moet worden verzet. ‘Het lijkt ver weg, maar eigenlijk zijn we al hopeloos te laat. Nederland stelt eerst overlegorganen en commissies in. Het beleid wacht tot er een crisis is. We moeten duwen en trekken om de achterstand in te halen. Er moet een datum komen, anders gebeurt er niets.’

Rapport over kwantumtechnologie

Aan het slot van de bijeenkomst presenteerde Bart Karstens, senior onderzoeker bij het Rathenau Instituut, het rapport Quantumtechnologie in de samenleving. Dat rapport inventariseert toepassingen van kwantumcomputers in de logistiek, biochemie en medische wetenschap en beschrijft de maatschappelijke zorgen die de technologie oproept. Het rapport is een korte scan, die laat zien wat de nieuwe technologie oplevert en geeft een overzicht van de risico's.

De presentaties tijdens het minisymposium zijn hier beschikbaar.

Verslag: Bram Vermeer