RACE NAAR REKENKRACHT

Q-DAY WERELD ZET ZICH SCHRAP VOOR DE DAG DAT QUANTUMCOMPUTERS ALLES OP Z'N KOP KUNNEN ZETTEN

FOTO 123RF

Q-day komt eraan als een dief in de nacht. De dag dat quantumcomputers met hun immense rekenkracht alles op z'n kop zetten. Allerlei computersystemen zijn plots niet meer veilig, staatsgeheimen liggen op straat, onderdelen van de maatschappij storten in. Inlichtingen- en veiligheidsdienst AIVD bracht samen met andere partijen een nieuwe handleiding uit om het tij te keren, want het is twee voor twaalf.

door **Silvan Schoonhoven**

Het nieuwe handboek straalt uit: dit is dringend. Eigenlijk hadden we gisteren al moeten beginnen met de aanleg van een verdedigingslijn tegen quantumcomputers. „Na een eerste versie vonden we dat die urgentie duidelijker naar voren moest komen", zegt onderzoeker Thomas Attema van TNO en het Centrum Wiskunde & Informatica, die met de geheime dienst meeschreven aan de nieuwe handleiding. „En dat we ook handvatten wilden bieden om aan de slag te gaan."

Want aan de slag moeten we. „We staan midden in twee van de grootste it-revoluties van de laatste dertig jaar: quantumcomputers en kunstmatige intelligentie", zei Alessandro Curioni, de directeur van IBM Research Europa eerder tegen De Telegraaf. „Samen gaan ze alles veranderen."

Google presenteerde vorige maand hun miljarden kostende Willow-quantumchip, volgens de techreus een belangrijke stap in de goede richting. Aan de andere kant liet de directeur van chipfabrikant Nvidia afgelopen week een bommetje vallen door te zeggen dat het nog meer dan vijftien jaar gaat duren voordat quantumcomputers hun nut gaan bewijzen. Waarop de aandelen van quantumontwikkelaars onderuit gingen op de beurs.

Technologie

Kortom: niemand weet wanneer Q-day precies komt. Dat hangt ermee samen dat de technologie zo anders is dan we gewend zijn. Computers werken met bits, die of een 1 of een 0 zijn. Een quantumcomputer daarentegen werkt met 'qubits'. Die kunnen een 1 en een 0 tegelijk zijn, of iets er tussenin. In de zichtbare wereld om ons heen kan dat niet. Een kat kan niet tegelijk dood zijn én leven. Maar in de kwantummechanica, die de wereld van de allerkleinste deeltjes beschrijft, is dat de gewoonste zaak van de wereld.

Een computer met qubits belooft een immense rekenkracht. Ter vergelijking: een gewone computer zoekt gangetje voor gangetje de uitgang van een doolhof, een quantumcomputer kan alle mogelijkheden tegelijk uitlopen.

„Het is echt een fundamenteel andere manier van rekenen en bewerkingen uitvoeren", zegt onderzoeker Attema.

„Als je die op de juiste manier inzet, dan kun je daar veel kracht uit halen. Bepaalde berekeningen die honderden jaren zouden duren met de huidige supercomputers, zou je met een quantumcomputer in een paar minuten kunnen doen."

Razendsnel rekenen belooft goed nieuws op allerlei terreinen. Voor wetenschappelijk onderzoek, de ontwikkeling van medicijnen, precieze weersverwachtingen, zelfs het terugdringen van broeikasgassen in de atmosfeer. Maar ook hackers en cyberspionnen kijken uit naar de quantumcomputer.

Amerika wil de eerste zijn met quantumcomputers maar weet dat de Chinezen er in het geheim minstens zo hard aan werken. En vlak ook Noord-Korea, Rusland en Iran niet uit.

Het doembeeld is een vijand die door een massale cyberaanval met quantumcomputers onze hele samenleving lamlegt. Bankverkeer hapert, energiecentrales vallen stil, defensiesystemen werken niet meer en de vijand kan ongehinderd door al onze staatsgeheimen bladeren.

'WhatsApp heeft de overgang al gemaakt'

„Neem chipfabrikant ASML", zegt Attema. „Dat bedrijf is constant bezig om te zorgen dat hun ideeën geheim blijven om hun technologische voorsprong te behouden. Als zij hun cryptografie niet op orde hebben, kan een aanvaller hun bedrijfsgeheimen stelen en de voorsprong ongedaan maken. Dat zou natuurlijk een gigantische klap betekenen. Dat soort zaken kan geopolitiek grote invloed hebben."

Encryptie

Wanhoop is nog niet nodig. Bedrijven en overheden kunnen hun systemen quantumproof maken. Kijk bijvoorbeeld naar WhatsApp. Voor veel mensen het bekendste voorbeeld van encryptie door de vertrouwde mededeling 'berichten en oproepen worden end-to-end versleuteld'. „WhatsApp is een van de weinige voorbeelden van bedrijven die de overgang al hebben gemaakt", zegt Attema. „Dus in principe zijn je appberichten eigenlijk nu al veilig voor quantumcomputers."

Veel lastiger wordt het voor bedrijven waar verouderde encryptie diep in de systemen zit ingebakken. „De overgang naar nieuwe standaarden is een enorme operatie", zei Michael Osborne, quantumexpert bij IBM eerder tegen De Telegraaf. „Vergelijk het maar met het in een paar jaar vervangen van al het staal in onze gebouwen, zonder de mensen eruit te halen."

De afgelopen veertig jaar hebben systeembouwers overal cryptografie gebruikt. Nu moeten we in al onze digitale infrastructuur de verouderde systemen identificeren en vervangen, van banksoftware tot internetprotocollen.

Veel onderdelen hangen met elkaar samen en één zwakke schakel in de keten kan het hele systeem ondermijnen. En niet iedereen voelt de urgentie al. „Veel organisaties begrijpen niet eens dat deze verandering hen raakt", zei hoofd quantumtechnologie Jaime Gómez García van de Spaanse grootbank Santander tegen De Telegraaf. „Maar cryptografie zit overal. We moeten een einde maken aan wat ik 'crypto-uitstelgedrag' noem."

Het Amerikaanse National Institute of Standards and Technology (NIST) heeft vorig jaar nieuwe encryptiestandaarden ingevoerd die zelfs voor quantumcomputers niet te kraken zijn. Ook Nederland is al bezig, zegt Attema.

Sommigen denken dat Q-day al binnen vijf jaar aanbreekt. „Het blijft speculeren", zegt Attema. „Vijf jaar lijkt me kort, maar je weet niet welke technologische doorbraken er komen waardoor het opeens snel gaat."

DOEMBEELD IS CYBERAANVAL DIE HELE SAMENLEVING LAMLEGT