ARTIKEL DIGITALE ZEGGENSCHAP 23 JULI 2020

Digitaal weerbaar in tijden van quantumcomputers

Het duurt nog even, maar zo rond het jaar 2040, misschien 2050, zijn er quantumcomputers die hun hand niet omdraaien voor het kraken van huidige sterke wachtwoorden en dataversleuteling. Wat kunnen we doen om ons weerbaar te maken? Kunnen we rustig gaan slapen? De nachtmerrie, de droom en de realiteit

De nachtmerrie

Het is 2040. Het Amerikaanse leger heeft in het diepste geheim een quantumcomputer gebouwd. Het heeft even geduurd, maar de computer doet het en hij loopt als een zonnetje. Nu is het tijd om de petabytes aan versleutelde gegevens die Amerika jarenlang verzamelde over China, Rusland en Europa te ontcijferen. Met een paar muisklikken verandert de tot nu toe onkraakbaar geachte geheimtaal in leesbare rapporten, heldere brieven en duidelijke verslagen. Van al onze versleutelde Whatsapp-berichten tot de medische gegevens van de Duitse Bondskanselier, van de creditcardafschriften van het Kremlin tot de blauwdrukken van de chipmachines van ASML. Niks is meer veilig.

De droom

Het is 2040. Delftse onderzoekers hebben samen met Microsoft een quantumcomputer gebouwd. Het heeft even geduurd, maar de computer doet het en hij loopt als een zonnetje. En omdat Europa en de Verenigde Staten al in 2025 begonnen met het grondig versleutelen van gegevens en het aanpassen van computerchips, websites en software, kunnen de oude standaarden met een gerust hart worden uitgeschakeld. De wereld haalt opgelucht adem. Je moet er toch niet aan denken dat het anders had gelopen.

De realiteit

Het is 2020. De quantumcomputer is er nog niet, maar onderzoekers over de hele wereld maken stapje bij stapje vorderingen. Medewerkers van Google hebben bekendgemaakt dat ze met een rudimentaire quantumcomputer in drie minuten een berekening kunnen uitvoeren waar een supercomputer tienduizend jaar over zou doen. Het gaat om een berekening zonder praktisch nut en een echte quantumcomputer is nog tientallen jaren weg, maar het begin is er.

In Nederland heeft het Rathenau Instituut net een rapport naar buiten gebracht met de titel 'Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie'. Het is een kwestie van tijd, aldus het instituut, voordat kwaadwillende partijen quantumcomputers gaan gebruiken voor digitale aanvallen. Gelukkig is er een lichtpuntje. We kunnen sterkere versleutelingsmethodes ontwikkelen en nieuwe technologieën zoals kunstmatige intelligentie gebruiken om ons weerbaar te maken. Maar dan moet er nu wel wat gebeuren.

Wat is een quantumcomputer?

Actie 1: een standaard bedenken
Een van de acties die Nederland en de wereld nu al kunnen uitvoeren, is het bedenken van een of meer standaarden voor het versleutelen van gegevens zodat quantumcomputers ze niet kunnen kraken. NIST, het Amerikaanse instituut voor standaarden, heeft al een prijsvraag uitgeschreven. Dat is een goed begin, zo zeggen de onderzoekers van het Rathenau Instituut, maar het zou beter zijn als het Europese ETSI of de wereldwijde ISO ook standaarden bepalen.

Actie 2: systemen aanpassen
Als er een standaard is om gegevens te versleutelen, dan moet die standaard natuurlijk ook worden ingevoerd. Dat klinkt gemakkelijker gezegd dan gedaan. Volgens experts duurt zo'n migratie naar een nieuw systeem met gemak tien à twintig jaar. De standaard moet namelijk worden geïmplementeerd in programmeertalen, in protocollen en op chips. Vervolgens moeten leveranciers die talen, protocollen en chips gaan gebruiken in hun producten. Daarna moeten de oude systemen worden uitgezet.

Een voorbeeld uit het verleden laat zien dat het aanpassen van systemen traag gaat. Microsoft schakelde bijvoorbeeld pas in 2014 het encryptieprotocol MD5 uit terwijl wetenschappers al in 2007 aantoonden dat het kwetsbaar was en hackers al sinds 2008 stilletjes spioneerden met behulp van vervalste certificaten.

Actie 3: oude gegevens vernietigen of versleutelen
Een derde actie die in aanloop naar de komst van de quantumcomputer moet plaatsvinden, is het vernietigen of versleutelen van oude gegevens. Ook dat is bewerkelijk. Kijk voor de grap eens rond in de kamer waar je nu zit. Je computer, je mobieltje, een draagbare harde schijf, een reservelaptop: al die apparaten bevatten gegevens die je liever niet met de buitenwereld wilt delen. En dat is alleen nog maar bij jou thuis. Voor bedrijven en instellingen is het opnieuw versleutelen of vernietigen een hels karwei. Denk aan de patiëntendossiers van een ziekenhuis of aan de concurrentiegevoelige informatie van een bedrijf.

Overigens gebeurt dat quantumproof maken van gegevens nu al op bescheiden schaal. Onze eigen inlichtingendienst AIVD versleutelt staatsgeheimen die de komende dertig jaar geheim moeten blijven. Experts zeggen dat dat versleutelen veel breder zou moeten gebeuren. Anders ligt met de komst van de quantumcomputer alles op straat.

Meer bedrijvigheid
Goed, het is duidelijk. Nederland moet zo'n beetje nu actie gaan ondernemen als we er over twintig jaar nog beschermd bij willen zitten. En het mooie is dat we veel kennis in huis hebben. Denk aan onderzoeksgroepen bij de TU Delft, de Radboud Universiteit, CWI, TU Eindhoven en Philips.

Maar onderzoek is niet genoeg. Melanie Peters, directeur van het Rathenau Instituut, onderstreept het belang van eigen IT-bedrijven in Nederland en Europa: "Door zelf meer digitale producten en diensten te ontwikkelen, kunnen we ervoor zorgen dat die producten en diensten recht doen aan belangrijke Europese waarden als veiligheid, privacy en autonomie." En dan? Dan kunnen we met een gerust hart gaan slapen. Tot de volgende dreiging.