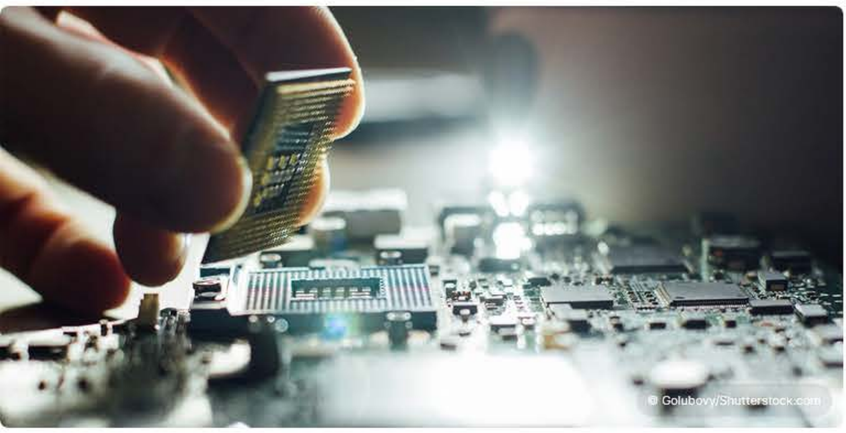
Europees Parlement bezorgd over computerbeveiliging

Anton Mous
Privacy en securityredacteur

Gepubliceerd: 18 maart 2024



Bedrijven en organisaties moeten zo snel mogelijk een begin maken met het verbeteren van de beveiliging van hun gegevens. Quantumcomputers worden steeds krachtiger en zijn op de langere termijn in staat om veelgebruikte computerbeveiliging te kraken. Ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) roept bedrijven op om hier zo snel mogelijk werk van te maken.

Twintig Europarlementariërs uiten hun zorgen over de afnemende effectiviteit van traditionele computerbeveiliging in een open brief aan de Europese Commissie, zo meldt de *NOS*.

'Q-day' is in aantocht

Cryptografie wordt volop gebruikt om gevoelige informatie te beschermen tegen hackers. Beveiligingsexperts vrezen dat dit op termijn niet langer voldoende is. Quantumcomputers zijn dan in staat om de huidige cryptografische standaarden te kraken. Dergelijke computers beschikken over dermate veel rekenkracht dat het hacken van reguliere computers een peulenschilletje is.

Europarlementariër Bart Groothuis (Renew), initiatiefnemer van de brandbrief, benadrukt dat het bedrijfsleven daarom direct moet beginnen om zich te wapenen tegen quantumcomputers. De overstap naar betere computerbeveiliging is een goede oplossing om gevoelige data in de toekomst te beschermen, maar kost tijd en geld om te implementeren.

Het moment dat quantumcomputers in staat zijn om de huidige generatie beveiliging te kraken, ook wel 'Q-day' genoemd, duurt misschien nog wel tien tot twintig jaar. Dat betekent echter niet dat we achterover kunnen leunen en pas over jaren in actie hoeven te komen. Met name bedrijven die actief zijn in de vitale sector en overheidsorganisaties die veel gevoelige data verwerken, moeten zich nu al zorgen maken en maatregelen treffen. "We kunnen dat risico niet nemen. De belangrijkste organisaties moeten hier nu mee beginnen", zo zegt Groothuis tegen de NOS.

'Denk nu al na over de mogelijkheden van quantumsystemen'

Julia Cramer, universitair docent Quantum and Society aan de Universiteit Leiden, vertelt dat er enorm veel vooruitgang wordt geboekt. Volgens haar hebben quantumcomputers 2.000 qubits nodig om wiskundige sleutels te ontcijferen. "Maar die 2.000 qubits zijn er nog lang niet", vertelt ze.

Daarnaast zijn qubits, die de rekenkracht exponentieel vergoten ten opzichte van reguliere bits, momenteel nog erg foutgevoelig. Maar dat kun je volgens Cramer ondervangen door meerdere qubits aan elkaar te koppelen. Quantumcomputers vormen daarom pas waarschijnlijk over tien jaar een gevaar voor de huidige cryptografische sleutels. "Maar vanwege de vele mogelijkheden van

Overstappen op andere algoritmes die beter bestand zijn tegen quantumcomputers, kan niet zomaar. Zowel de verzender als de ontvanger moeten dezelfde technologie gebruiken en ondersteunen. Een succesvolle aanpassing is daarom afhankelijk van softwaremakers. Zij moeten de nieuwe technologie invoeren.

Ook AIVD adviseert om nu al stappen te ondernemen

Ook de AIVD is bezorgd dat quantumcomputers over enkele jaren in staat zijn om de huidige beveiligingsstandaarden te omzeilen. "De AIVD benadrukt het belang van voldoende middelen en urgentie bij de leveranciers om zo snel mogelijk quantumveilige producten op te leveren en huidige producten te updaten", zo laat de veiligheidsdienst in een schriftelijke reactie weten.

Om de overstap naar quantumveilige communicatie te onderstrepen, introduceerde de AIVD in april vorig jaar het PQC-handboek. Met het handboek wil de veiligheidsdienst organisaties handvatten aanreiken om risico's te identificeren en concrete stappen te zetten om te werken aan een migratiestrategie. "De migratie naar nieuwe cryptografische mechanismen is een complex proces dat tijd kost. Houd je hier geen rekening mee en neem je te laat maatregelen? Dan loop je het risico dat je gevoelige of vertrouwelijke informatie later alsnog ontcijferd wordt", zo waarschuwde de veiligheidsdienst afgelopen jaar.

Demissionair staatssecretaris voor Digitalisering Alexandra van Huffelen sloot zich hierbij aan. "Het is van groot belang dat Nederland zich voorbereidt op de dreiging van de quantumcomputer voor onze beveiligde informatie en communicatie. Dit handboek biedt overheid en bedrijfsleven belangrijke ondersteuning hierbij. Mooi om te zien dat de samenwerking tussen de kennisinstellingen [AIVD, TNO en het Centrum voor Wiskunde en Informatica, red.] leidt tot de publicatie van dit handboek", aldus de bewindsvrouw.