1,8 miljoen euro subsidie om communiceren veilig te houden

MEI 10, 2021 REDACTIE

Het kan jaren duren om een versleuteld bericht te ontcijferen. Die tijd wordt echter snel korter. Nieuwe quantumtechnologie kan de huidige beveiligingsmethoden binnen enkele jaren waardeloos maken. Een groep Nederlandse organisaties start daarom met het toekomstbestendig maken van de digitale infrastructuur.

Een consortium van onder andere TNO, CWI (Centrum Wiskunde & Informatica) en de TU Delft ontvangt 1.8 miljoen subsidie van NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek) om onderzoek te doen naar het quantum veilig maken van de publieke sleutelinfrastructuur (PKI).

Veilige digitale verbindingen

Een PKI is een systeem waarmee uitgave en beheer van digitale certificaten kan worden gerealiseerd. Die certificaten vormen de basis van veilige digitale verbindingen en het beveiligen van digitale informatie. Het onderzoeksvoorstel genaamd HAPKIDO (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations) is ingediend naar aanleiding van een oproep van de Nationale Wetenschapsagenda (NWA). In het consortium zitten naast eerdergenoemde partijen ook KPN, Microsoft, de dienst digitale overheid Logius en softwarebedrijf Zynyo. Verder worden de deelnemende partijen ondersteund door verschillende particuliere- en publieke organisaties.

Kwetsbaar

Veel populaire cryptografische algoritmen en encryptieschema's worden onveilig door de vooruitgang in quantumcomputing. Zonder voorbereiding zullen gevoelige gegevens die door encryptieschema's worden beschermd, toegankelijk worden en zal de communicatie-infrastructuur worden verstoord. Dit heeft als gevolg dat onze transacties en informatie kwetsbaar zullen worden voor vijandige entiteiten waardoor ontelbare organisaties en miljoenen mensen worden getroffen.

Kansen en dreigingen

"We zijn enorm blij dat NWO ons voorstel heeft goedgekeurd. De ontwikkeling van quantumcomputing gaat razendsnel en dat biedt kansen maar ook dreigingen waar we op voorbereid moeten zijn. Quantum veilige vertrouwensdiensten, inclusief de onderliggende Public Key Infrastructure (PKI), zijn nodig om digitale samenlevingen tegen deze aanzienlijke risico's te beschermen", aldus Maran van Heesch, Programma manager Cyber Security & Robustness bij TNO.

Realisatie overgang quantumveilige infrastructuur

Het HAPKIDO-onderzoek richt zich met name op hoe een overgang naar een quantum veilige publieke sleutelinfrastructuur kan worden gerealiseerd. Als onderdeel hiervan kijkt het consortium naar onderliggende technische aspecten zoals het ontwerpen van een hybride PKI die rekening houdt met interoperabiliteit tussen verschillende systemen, backward-compatibiliteit en migratie-architecturen.

Toekomstige situatie
Tegelijkertijd onderzoekt het consortium welke groeimodellen mogelijk zijn om van de huidige naar toekomstige situatie te kunnen overgaan, en hoe het beheer (IT-governance) van digitale infrastructuren moet veranderen om quantum veiligheid te borgen. Hierbij worden ook de maatschappelijke risico's van een quantum onveilig PKI in het quantum-tijdperk meegenomen.

Nationale wetenschapsagenda cyber security
Het voorstel van TNO, CWI en de TU Delft is een van 5 gehonoreerde voorstellen van in totaal 19 die zijn ingediend. Voor de gehonoreerde voorstellen is een budget van €9.610.000 beschikbaar gemaakt. Deze voorstellen zijn ingediend naar aanleiding van de oproep van de Nationale Wetenschapsagenda (NWA) aan consortia om manieren te vinden voor veilige en vertrouwde data-deling, nu en in de toekomst. Het HAPKIDO voorstel wordt gesteund door 11 organisaties, waaronder verschillende ministeries, de NLNCSA, Politie, ING en ABN AMRO.