oktober 2023

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Quantumveiligheid

Maak uw organisatie quantumveilig

Wat is quantumveilig?

Cryptografie vormt een belangrijk fundament voor informatiebeveiliging. Cryptografie wordt bijvoorbeeld gebruikt om gegevens te beschermen door ze onleesbaar te maken voor onbevoegden. Een ander voorbeeld van een op cryptografie gebaseerde technologie is de digitale handtekening. Quantumveiligheid gaat over het treffen van voorbereidingen en het nemen van maatregelen om ervoor te zorgen dat uw organisatie weerbaar is tegen de dreiging van een krachtige quantumcomputer.

Waarom uw organisatie quantumveilig maken?

Het valt niet exact te voorspellen op welk moment de quantumcomputer ingezet kan gaan worden. Dat betekent echter niet dat er nu geen reële dreiging is waar u rekening mee moet houden. Kwaadwillenden zouden nu al versleutelde data van hun doelwitten kunnen verzamelen om deze op een later moment te ontsleutelen. Het zogenaamde '*store now, decrypt later*'-scenario. Op het moment dat er een krachtige quantumcomputer beschikbaar komt, lopen bedrijfsprocessen die gebruik maken van authenticatie- of autorisatiesystemen, of waarvoor het tekenen en verifiëren van digitale handtekeningen vereist is, ook risico. Zowel de huidige als toekomstige dreigingen maken dat organisaties nu al moeten denken over quantumveiligheid en wat dit betekent voor uw organisatie.

Welke stappen kunt u nu al nemen om uw organisatie tijdig quantumveilig te maken?

Inventarisatie
1. Maak risico's inzichtelijk
2. Inventariseer uw cryptomiddelen

Planning
3. Beoordeel de risico's
4. Stel een migratieplan op

Uitvoering

Tref nu al voorbereidingen om te migreren naar quantumveilige cryptografie.

Aangezien het migreren naar quantumveilige cryptografie uw organisatie veel tijd en middelen zal gaan kosten, adviseren we u om nu al te starten met de voorbereidingen hierop. De AIVD en het NCSC hebben gezamenlijk een handreiking gemaakt die u helpt om dit te doen.

Quantumveiligheid *(ncsc.nl)*