Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan:
MinBZK

I.a.a.:
StasBZK/KRD

Via:
SG BZK

Van:
DGAIVD

TER BESLUITVORMING

Nota actief openbaar
Ja

Datum
6 augustus 2024

Ons kenmerk
9ca567b3-or1-1.2

Opgesteld door
AIVD/CS

Samengewerkt met

Bijlagen
2

nota

Beslisnota bij Verslag Schriftelijk Overleg inzake Fiche: Aanbeveling Routekaart Post-Quantumcryptografie

Aanleiding

- Op 17 mei is het BNC-fiche Aanbeveling Routekaart Post-Quantumcryptografie aangeboden aan de Staten-Generaal. AIVD was penvoerder voor dit fiche.
- Naar aanleiding van het fiche heeft de vaste commissie voor Digitale Zaken van de Tweede Kamer enkele vragen en opmerkingen aan u voorgelegd.

Geadviseerd besluit

- U kunt instemmen met het aanbieden van de bijgevoegde beantwoording aan de Kamer.

Kern

- GL-PVDA, VVD en NSC hebben enkele verduidelijkende vragen gesteld over de kabinetsinzet. In de beantwoording licht u de kabinetsinzet toe.
- Het doel van de aanbeveling van de Europese Commissie is om de nationale transitieplannen naar Post-Quantumcryptografie (PQC) gecoördineerd uit te voeren met behulp van een Europese routekaart ten behoeve van internationale interoperabiliteit.
- In het BNC-fiche verwelkomt het kabinet het initiatief en het hierin beschreven plan van activiteiten. Wel plaatst het kabinet enkele kanttekeningen, onder meer over het meenemen van *Quantum Key Distribution* (QKD) in de routekaart.
- GL-PVDA, VVD en NSC hebben bijzondere aandacht voor QKD. Ten aanzien van dit onderwerp geeft u aan dat QKD op dit moment en in de nabije toekomst nog niet volwassen genoeg is om ingezet te worden voor informatiebeveiliging. In de specifieke context van de aanbeveling van de Commissie is het kabinet daarom geen voorstander van het meenemen van QKD in de routekaart.
- Het kabinet acht het namelijk van het grootste belang dat organisaties PQC nu zo snel mogelijk inzetten om de acute dreiging van quantumtechnologie op het gebied van informatiebeveiliging te mitigeren.

- Wel is QKD een technologie die volop in ontwikkeling is en mogelijk kansen biedt voor verschillende toepassingen. Daarom blijft het kabinet inzetten op de verdere ontwikkelingen van de technologie voor toepassing op de langere termijn. Mede daarom is de inzet van het kabinet dat de routekaart aanpasbaar wordt.
- De beantwoording is afgestemd met dezelfde brede groep interdepartementale meelezers als het BNC-fiche.

Toelichting

- De Commissie herkent de urgentie van de dreiging van de quantumcomputer op de vertrouwelijkheid van informatie en adviseert een spoedige transitie naar PQC.
- De Commissie moedigt de lidstaten aan om in onderlinge samenwerking een strategie en routekaart te ontwikkelen voor de adoptie van PQC voor een gecoördineerde en gesynchroniseerde transitie onder de lidstaten.
- Lidstaten worden aangemoedigd hun acties te coördineren via een lidstatenforum van vertegenwoordigers van nationale beveiligings- en cybersecurityautoriteiten en ENISA. Inmiddels is duidelijk dat Duitsland, Frankrijk en Nederland het co-voorzitterschap van dit forum op zich nemen.
- De routekaart moet als blauwdruk dienen voor de nationale plannen voor transitie naar PQC of, indien deze plannen al bestaan, voor afstemming op de routekaart.
- De meeste acties in de aanbeveling zijn in lijn met staand Nederlands beleid. Nederland hanteert echter een andere definitie van 'hybride oplossing'. Waar de Commissie een 'hybride oplossing' definieert als een combinatie van PQC en QKD, wordt deze term binnen de cryptografie meestal gebruikt voor combinaties van asymmetrische en symmetrische cryptografie of voor combinaties van asymmetrische cryptografie en Post-Quantumcryptografie. Daarom is de term verwarrend als men deze gebruikt om een combinatie van PQC en QKD aan te duiden.
- Het nationale beleidsadvies is de inzet van een hybride oplossing van PQC gecombineerd met de huidige cryptografie.
- PQC en QKD zijn volstrekt andere technologieën. PQC is gebaseerd op onderliggende wiskundige problemen die niet gekraakt kunnen worden met de bekende quantumalgoritmes, terwijl QKD is gebaseerd op het uitwisselen van (natuurkundige) quantumtoestanden.

Politieke context

- Op 15 maart 2024 heeft een groep Europarlementariërs, waaronder Bart Groothuis (VVD), een brandbrief verstuurd aan de Europese Commissie waarin opgeroepen wordt de transitie naar Post-Quantumcryptografie te starten.

Krachtenveld

- Samen met Duitsland, Zweden, Frankrijk en Italië maakt Nederland deel uit van de *AQUA Reference Group*. Dit is een selecte groep landen die cryptoproducten kunnen en mogen evalueren voor gebruik in EU-verband ('tweedelandsevaluatie'). Namens Nederland neemt de AIVD deel aan deze groep.
- De *AQUA Reference Group* is eensgezind over een gecoördineerde transitie naar Post-Quantumcryptografie.

- Enkele leden van de *AQUA Reference Group* hebben een gezamenlijke visie op de transitie naar Post-Quantumcryptografie in januari 2024 toegelicht in een *position paper*.
- In dit paper adviseren de leden meer onderzoek te doen naar de beveiligingsaspecten van QKD, opdat deze technologie op langere termijn ook inzetbaar wordt voor informatiebeveiligingsdoeleinden.
- Uw voorganger heeft dit *position paper* op 16 februari aangeboden aan de Kamer.