Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER ONDERTEKENING

Nota actief openbaar
Ja

Onze referentie
2023-0000200214

Datum
6 april 2023

Opgesteld door
DGDOO/IFHR

Samengewerkt met
DGDOO/CIO Rijk en departementen EZK, J&V en Defensie

Bijlage(n)
2

Aan Staatssecretaris Koninkrijksrelaties en Digitale Zaken
Cc Minister BZK

Van dgDOO

nota

Beslisnota Kamerbrief aanpassingen moties Rajkowski

Aanleiding

In het overleg met plv.dgDOO op 31 maart jl. zijn gewenste wijzigingen besproken ten aanzien van de Kamerbrief over de uitvoering van de moties Rajkowski c.s.
Bijgaand treft u een aangepaste versie aan.

In het hiervoor genoemde overleg is gevraagd:
- aan te geven welke intensivering sinds de moties heeft plaatsgevonden
- aan te geven wanneer welke resultaten worden opgeleverd
- scope van de gevraagde scan te duiden
- op welke wijze leveranciers/producten en diensten kunnen worden geweerd in aanbestedingen.

Geadviseerd besluit

Akkoord gevraagd met de voorgestelde brief met de gewenste wijzigingen. De brief zal mede namens de minister van J&V en de minister van EZK worden verzonden, gezien de verdeling van verantwoordelijkheden. Beide ministers zijn inmiddels akkoord. De brief is op verzoek van de minister van Defensie ook met haar gedeeld. Zij hecht veel belang aan dit onderwerp maar is geen medeondertekenaar. De Minister van Defensie is ook akkoord met de brief.

Kern

Kern van de beantwoording:

- Het kabinet ziet met de Kamer de risico's en dreigingen die uitgaan van landen met een offensief cyber(spionage)programma tegen Nederlandse belangen. In onder meer het recente Cyber Security Beeld Nederland[1] en het Dreigingsbeeld Statelijke Dreigingen[2] wordt hier uitgebreid op ingegaan. Vanwege deze dreiging voelt het kabinet de noodzaak om alert te zijn en passende maatregelen te nemen ten aanzien van producten en diensten die wij als overheid verwerven.
- Het kabinet voert landenneutraal beleid. Dit betekent dat leveranciers uit specifieke landen door de aanbestedende dienst niet op voorhand

[1] Kamerstuk II 2022/23, 26643, nr. 925
[2] Kamerstuk II 2022/23, 30821, nr.175

categorisch worden uitgesloten, maar dat dit per casus op basis van een risicoafweging wordt bepaald.
- De aanbestedingsregelgeving biedt overheden een aantal mogelijkheden om bij de inkoop van producten en diensten, bepaalde leveranciers op basis van deze risicoafweging te weren of op een andere wijze de risico's voor de nationale veiligheid te mitigeren. (zie bijlage)
- Bij aanbestedingen die onder de Aanbestedingswet 2012 vallen is het bijvoorbeeld mogelijk om leveranciers uit te sluiten afkomstig van landen die niet aangesloten zijn bij het GPA-verdrag (Government Procurement Agreement).
- De minister van EZK onderzoekt welke extra maatregelen voor uitsluiting en risicomitigatie binnen de aanbestedingsregelgeving nodig en effectief zijn. Over de Europese inzet op dit thema wordt de Kamer voor het zomerreces door de minister van EZK geïnformeerd in de Kamerbrief over aanbesteden en derde landen.
- Het deel van de motie dat oproept om inzicht te verschaffen in de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in *de vitale infrastructuur* wordt uitgevoerd door de Minister van JenV gezien de beleidsverantwoordelijkheid voor het vitaal stelsel.
- Er is afgelopen periode en mede naar aanleiding van genoemde moties op drie terreinen sprake van intensivering. Als eerste is stevig ingezet op het sterker benutten van de huidige mogelijkheden binnen de Aanbestedingswetgeving en op het vergroten van de bewustwording ten aanzien van nationale veiligheidsrisico's. Deze inzet wordt verder versterkt. Ten tweede verplicht het kabinet de toepassing van passende instrumenten in het inkoop- en aanbestedingsproces. Tenslotte wordt een regeling opgezet (genaamd Algemene Beveiligingseisen Rijksoverheid Opdrachten of afgekort ABRO) voor aanbestedingen van de rijksoverheid en de Nationale Politie die de nationale veiligheid raken.

Toelichting
Motie Rajkowski vraagt:

- te onderzoeken hoe apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda geweerd kunnen worden uit aanbestedingen van de rijksoverheid.
- om een richtlijn voor de rijksoverheid en haar leveranciers, zodat producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda gericht tegen Nederland uit bepaalde aanbestedingen kunnen worden geweerd
- een scan uit te voeren op de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in de vitale infrastructuur.

Politieke context
Sinds de moties zijn er verschillende momenten geweest dat mediaberichtgeving de aandacht ook uit de Kamer weer op veilige digitale middelen heeft gevestigd. Daarbij kan bijvoorbeeld worden gedacht aan de berichtgeving over Chinese camera's van Hikvision in enkele typen NS-treinen.

Financiële/juridische overwegingen
De inzet zoals geschetst op staand en nieuw beleid wordt gefinancierd uit de middelen voor het cybersecuritybudget zoals beschikbaar zijn via het Regeerakkoord.

Krachtenveld (intern)
De Kamerbrief is afgestemd met de ministers van EZK, J&V en Defensie. Daaraan voorafgaand is de Kamerbrief parallel afgestemd met de ICIA (Interdepartementale Commissie Inkopen en Aanbesteden), CISO's van de departementen en enkele grote uitvoeringsorganisaties (via de CISO-Raad) en de Taskforce Economische Veiligheid (informeel gremium op DG-niveau beleidsgremium voor economische en nationale veiligheid).

Op basis van de input uit de gremia blijkt dat er veel interesse is in het onderwerp. Deze gremia zijn betrokken bij het werken aan bewustzijn rondom de bestaande instrumenten en mogelijkheden, en het verbeteren ervan.

Strategie
De genoemde activiteiten zijn onderdeel van Veilig inkopen en aanbesteden binnen de rijksoverheid.

Uitvoering
De uitvoering is samen met alle departementen opgepakt. De verantwoordelijkheidsverdeling is ook in de brief opgenomen.

Communicatie
nvt