Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1007

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 april 2023

Middels deze brief informeer ik, mede namens de Minister van Economische Zaken en Klimaat en de Minister van Justitie en Veiligheid, uw Kamer over de uitvoering van twee moties Rajkowski, van Weerdenburg, c.s.

1.
Op 29 maart 2022 hebben Kamerleden Rajkowski (VVD) en Van Weerdenburg (PVV) een motie ingediend die ten eerste vraagt om 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 (Kamerstuk 26 643, nr. 830) Ten tweede wordt gevraagd 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.

2.
Daarnaast is in het hoofdlijnendebat digitalisering op 30 juni jl. (Handelingen II 2022/23, nr. 99, item 5 en 8) een tweede motie ingediend (en aangenomen) door Rajkowski, c.s. die de regering verzoekt om te komen met een richtlijn voor de rijksoverheid en haar leveranciers, dat producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda gericht tegen Nederland uit bepaalde aanbestedingen geweerd kunnen worden, en de Kamer hierover te informeren (Kamerstuk 26 643, nr. 874). Deze motie overlapt inhoudelijk met de motie Rajkowski (VVD) en Van Weerdenburg (PVV) uit maart 2022.

Met uw Kamer ziet het kabinet de risico's en dreigingen die uitgaan van landen met een offensief cyber(spionage)programma tegen Nederlandse

kst-26643-1007
ISSN 0921 - 7371
's-Gravenhage 2023

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. Dit mede ter voorkoming van spionage, sabotage en het ontstaan van risicovolle strategische afhankelijkheden van andere landen en/of partijen.
Het kabinet voert landenneutraal beleid. Dit betekent dat leveranciers uit specifieke landen door de aanbestedende dienst niet op voorhand categorisch worden uitgesloten, maar dat dit per casus op basis van een risicoafweging wordt bepaald.
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 ga ik verder versterken door middel van meer voorlichting en communicatie over de (juridische) mogelijkheden ten aanzien van veilig inkopen en aanbesteden. Ten tweede verplicht het kabinet de toepassing van passende instrumenten in het inkoop- en aanbestedingsproces door een nadere aanscherping van de kaderstelling, waarin procesafspraken zijn opgenomen, en door monitoring binnen de rijksoverheid. Ten slotte 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. De hierboven genoemde terreinen komen aanbod in de onderliggende brief. Tevens besteed ik in deze context aandacht aan de samenwerking met de departementen en doorontwikkeling van instrumentarium ten aanzien van informatieveiligheid ten behoeve van het inkoopproces (Inkoopeisen Cybersecurity Overheid).

Samenwerking en verantwoordelijkheden

Het heeft de prioriteit van het kabinet om in samenwerking met alle departementen het veilig inkopen en aanbesteden in onderlinge samenhang verder te verbeteren en te versterken. De (nieuwe) maatregelen worden samen met alle ministeries uitgevoerd. Gezien de beleidsverantwoordelijkheid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ten aanzien van veilige inkoop door de rijksoverheid en voor een veilige digitale overheid, neem ik de verantwoordelijkheid voor de uitvoering van de moties ten aanzien van het weren van producten en diensten uit landen met een offensief cyberprogramma tegen Nederland in aanbestedingen van de (rijks)overheid. Dit pak ik op in gezamenlijkheid met de Minister van Justitie en Veiligheid (JenV), waar de coördinerende verantwoordelijkheid voor nationale veiligheid ligt, waaronder ook de inzet tegen statelijke dreigingen. Vanwege de verantwoordelijkheid voor de Aanbestedingswetgeving wordt ook door de Minister van Economische Zaken en Klimaat (EZK) een bijdrage geleverd.

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. Momenteel werkt het kabinet, onder coördinatie van de Minister van JenV, aan een Versterkte Aanpak Vitaal voor een verbeterde bescherming van de Nederlandse vitale infrastructuur. De uitwerking van dit deel van de motie

[1] Kamerstuk 26 643, nr. 925.
[2] Kamerstuk 30 821, nr. 175.

vormt onderdeel van deze aanpak. In de Versterkte Aanpak Vitaal is nadrukkelijk aandacht voor afhankelijkheden, potentiële risico's en maatregelen ter versterking van de weerbaarheid van de vitale infrastructuur. Zoals vermeld in de Kamerbrief Aanpak Statelijke Dreigingen[3] zal daarnaast het (laten) meewegen van nationale veiligheid bij inkoop en aanbestedingen in de vitale infrastructuur ook in de versterkte aanpak vitaal worden meegenomen. De Kamer wordt in het tweede kwartaal van 2023 geïnformeerd over deze Versterkte Aanpak Vitaal en de uitvoering van de motie t.a.v. de gevraagde scan binnen de vitale sectoren.

Sterker benutten van de huidige mogelijkheden binnen de Aanbestedingswetgeving

Uw Kamer vraagt of de rijksoverheid en haar leveranciers producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda gericht tegen Nederland uit bepaalde aanbestedingen kunnen weren. De aanbestedingsregelgeving biedt overheden een aantal mogelijkheden om bij de inkoop van apparatuur of programmatuur bepaalde leveranciers op basis van een risicoafweging te weren of op een andere wijze de risico's voor de nationale veiligheid te mitigeren. 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 Government Procurement Agreement (GPA-verdrag).[4] Bij aanbestedingen onder de Aanbestedingswet op Defensie- en Veiligheidsgebied is het mogelijk leveranciers uit te sluiten van elk land buiten de EU.

Toch kunnen deze voorbeelden van bestaande mogelijkheden, die gericht zijn op leveranciers, niet altijd voorkomen dat specifieke producten, programmatuur, apparatuur of diensten uit organisaties en bedrijven uit landen met een offensieve cyberagenda worden aangeboden bij (Europese) aanbestedingen van overheidsopdrachten, bijvoorbeeld als onderdeel of component of via toeleveranciers uit andere landen. Per dienst of product kunnen wel inhoudelijke eisen worden gesteld waardoor risico's beperkt kunnen worden. Voor overige aanbestedingsrechtelijke mogelijkheden verwijs ik uw Kamer naar de bijlage en de Handvatten Risicomitigatie.[5] Voor de zomer van 2023 zal de Minister van EZK een overzichtelijke samenvatting van deze Handvatten publiceren (de «Quick Guide»).

Vergroten van de bewustwording ten aanzien van nationale veiligheidsrisico's

Vanwege de serieuze dreigingen die uw Kamer en ook het kabinet signaleren acht ik het van belang dat aanbestedende diensten zich bewust zijn van de risico's en dat zij op de hoogte zijn van de mogelijkheden die de aanbestedingsregelgeving biedt om die risico's te beheersen. Het kabinet wil extra inzetten op voorlichting hierover. Het kabinet doet een beroep op de verantwoordelijkheid van aanbestedende diensten om deze risico's te beheersen.

---

[3] Kamerstuk 30 821, nr. 175.

[4] Deze overeenkomst inzake overheidsopdrachten is een multilateraal verdrag dat is gesloten in het kader van de Wereldhandelsorganisatie (WTO). Wanneer de GPA van toepassing is, mogen leveranciers uit derde landen geen minder gunstige behandeling krijgen dan ondernemers uit de EU.

[5] Handvatten risicomitigatie bij inkoop en aanbesteding voor aanbestedende diensten en vitale aanbieders (2019), https://www.pianoo.nl/nl/regelgeving/crisis-en-inkoop/nationale-veiligheid/quickscanrisicomitigatie-nationale-veiligheid-bij.

Het kabinet wil dat de Europese aanbestedingsregels voldoende toekomstbestendig zijn en ondersteunend zijn aan het doel van veilige inkoop. Hoewel er een aantal mogelijkheden binnen de aanbestedingsregelgeving zijn, kunnen niet altijd alle risico's bij een aanbesteding volledig uitgesloten worden. 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 u voor het zomerreces door de Minister van EZK geïnformeerd in de Kamerbrief over aanbesteden en derde landen.

Verplichten instrumenten nationale veiligheid bij inkoop en aanbesteden

Binnen het huidige kabinetsbeleid wordt, vanwege de dreiging van statelijke actoren, doorlopend ingezet op het identificeren en beheersen van risico's voor de nationale veiligheid bij de inkoop en het gebruik van producten en diensten bij de rijksoverheid, lokale overheden en vitale aanbieders. Het uitgangspunt is om per inkoopopdracht risico's voor de nationale veiligheid in kaart te brengen en hier waar nodig maatregelen op te treffen. Ter ondersteuning van dit beleid is in 2018 en 2019 instrumentarium ontwikkeld dat organisaties mogelijkheden biedt bij het maken van een risicoanalyse en het treffen van maatregelen. Dit instrumentarium bestaat uit:
(1) een quickscan om risico's te identificeren;
(2) een handleiding voor het uitvoeren van een uitgebreidere risicoanalyse;
(3) aanbestedingsrechtelijke handvatten voor het beheersen van risico's

Dit instrumentarium is openbaar en te vinden op de site van PIANOo, Expertisecentrum aanbesteden. Er wordt ondersteuning geboden vanuit de rijksoverheid (Ministerie van BZK, EZK en de NCTV) bij de toepassing van het instrumentarium.
Op dit moment wordt gewerkt aan een actualisatie en aanscherping van het instrumentarium. Dit is binnen de rijksoverheid een verplicht kader met procesafspraken. De verwachting is dat dit voor de zomer van 2023 wordt afgerond. Deze geactualiseerde instrumenten worden ook openbaar gemaakt en worden wederom verspreid binnen de rijksoverheid, lokale overheden en vitale aanbieders. Daarnaast worden ook verschillende activiteiten georganiseerd om de bewustwording over dit thema en de mogelijkheden om risicos te beheersen te vergroten, zowel bij de rijksoverheid, lokale overheden als vitale aanbieders.

Risico's t.a.v. spionage, beïnvloeding en sabotage

Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen is het van belang om een aantal overwegingen mee te nemen in de hierboven genoemde risicoanalyse. Het kabinet heeft deze overwegingen onder andere gehanteerd bij het verwerven van antivirussoftware, apparatuur en programmatuur van aanbieders van Nederlandse mobiele telecomnetwerken en het communicatiesysteem voor hulpdiensten C2000.[6]
1. *Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?*

[6] Kamerstuk 25 124, nr. 96

2. *Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?*

3A. *Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?*

3B. *Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?*

Deze overwegingen moeten in samenhang met elkaar worden bekeken en alleen wanneer alle overwegingen van toepassing zijn, en blijkt dat nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar juridisch mogelijk partijen uitgesloten. Voor zover de huidige juridische mogelijkheden voor specifieke producten of diensten ontoereikend zijn wordt ingezet op het creëren van nieuwe mogelijkheden. Denk daarbij aan de besluiten die het kabinet heeft genomen ten aanzien antivirussoftware, mobiele telecomnetwerken en communicatiesystemen voor hulpdiensten.

Richtlijn

Het bovengenoemde instrumentarium geeft opdrachtgevers, inkopers en informatiebeveiligers handvatten om risico's voor de nationale veiligheid te identificeren en te beheersen, bijvoorbeeld het (in)direct weren van leveranciers of dienstverleners wanneer zij een risico vormen voor de nationale veiligheid. Om terug te komen op uw vraag om te komen tot een richtlijn maakt het kabinet daarom (onder andere) de toepassing van de hierboven genoemde instrumenten verplicht voor relevante inkoopopdrachten binnen de rijksoverheid. Daarbij wordt doorlopend ingezet op bewustwording van opdrachtgevers, inkopers en informatiebeveiligers van de rijksoverheid in het gebruik van dit instrumentarium en het signaleren van risico's in het inkoopproces. Hierbij gaat het om bewustwording van de dreiging die uitgaat van statelijke actoren, het signaleren van risico's bij een inkoopopdracht en het treffen van de juiste mitigerende en aanbestedingsrechtelijke maatregelen.

Algemene Beveiligingseisen rijksoverheid opdrachten (ABRO)

Aanvullend hierop werkt het kabinet tevens aan het ontwikkelen van beveiligingseisen ten aanzien van haar leveranciers. Hiertoe wordt een regeling opgezet voor aanbestedingen van de rijksoverheid en de Nationale Politie die de nationale veiligheid raken: de ABRO (Algemene beveiligingseisen rijksoverheid Opdrachten), doorontwikkeld vanuit de huidige ABDO (Algemene Beveiligingseisen voor Defensie Opdrachten) van het Ministerie van Defensie. De ABDO bevat bepalingen voor de opdrachtnemer met betrekking tot de fysieke beveiliging, (digitale) informatiebeveiliging en cybersecurity, (wijzigingen in) eigendomsstructuren, economische veiligheid, screening van personeel en procedures bij incidenten. Deze bepalingen/maatregelen dragen significant bij aan het voorkomen van (digitale)spionage, het weglekken van kennis en ongewenste overnames. Opdrachtnemers worden contractueel verplicht deze beveiligingseisen in te voeren. De rijksoverheid start hiervoor een meerjarig programma.
Naast de samenwerking met de verantwoordelijke departementen en het Ministerie van Defensie worden ook relevante uitvoeringsorganisaties zoals de Nationale Politie bij het vervolg betrokken. Mede gezien het feit dat de Nationale Politie bezig is met de uitvoering van de motie Van

Nispen (SP) van 19 mei 2022[7], die raakt aan dit onderwerp. In deze motie is al eerder aandacht gevraagd om bij aanbestedingen die de nationale veiligheid raken aan veiligheidsvereisten een zwaarder belang toe te kennen.
In 2023 en 2024 zal het kader met beveiligingseisen worden opgezet en vindt besluitvorming plaats. Eind 2024 start de uitvoeringsfase waarbij gezamenlijk de uitvoering opgepakt wordt ten behoeve van aanbestedingen van de rijksoverheid en relevante uitvoeringsorganisaties, die de nationale veiligheid raken.

Inkoopeisen Cybersecurity Overheid

De overheid hanteert de Baseline Informatiebeveiliging Overheid (BIO) als standaard om zich te weren tegen dreigingen gericht tegen de informatievoorziening van de overheid. Voor de vertaling naar meer specifieke eisen per in te kopen dienst of product zijn eisen ten aanzien van cybersecurity ontwikkeld. Deze eisen komen samen in een online-instrument welke beschikbaar is voor iedereen, met de naam «Inkoopeisen Cybersecurity Overheid (ICO)». De hedendaagse dreigingen vergen echter een meer specifiek eisenpakket per dienst of product, daarom worden aanvullende instrumenten ontwikkeld om dit eisenpakket aan te scherpen.
Deze cybersecurity-eisen kunnen als basis dienen om het programma van eisen op te stellen voor aanbestedingen en deze vervolgens op te nemen in af te sluiten contracten. Dit draagt tevens bij aan de eisen die overheid stelt aan haar leveranciers. Onlangs is dit aan uw Kamer gemeld in de Nederlandse Cybersecurity strategie[8] en in de Werkagenda Waardengedreven Digitaliseren die 4 november jl. aan uw Kamer is aangeboden[9]. In de Werkagenda is aangegeven dat uiterlijk eind 2025 via wetgeving is geborgd dat de normensets voor veilig inkopen van ICT-producten en -diensten verplicht worden toegepast door overheden.
Het ICO-instrument is sinds 2021 beschikbaar via de site BIO-overheid.nl[10] voor alle overheidsorganisaties en ook voor leveranciers van ICT-producten en -diensten. Er loopt een meerjarig programma om overheidsorganisaties te helpen bij het gebruik van het ICO-instrument. Verder geldt voor rijksoverheidsorganisaties ook een jaarlijkse audit- en verantwoordingssystematiek en een monitorende rol van CIO/CISO Rijk voor de implementatie en naleving van rijksbreed informatiebeveiligingsbeleid en -kaders.
Het kabinet geeft met het geheel aan bovengenoemde maatregelen om het veilig inkopen binnen de overheid te bevorderen, het verplicht stellen van het gebruik van het genoemde instrumentarium, ontwikkeling van de ABRO en de doorontwikkeling van het ICO-instrument, invulling aan de gevraagde richtlijn van uw Kamer.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

---

[7] Motie van het lid van Nispen (SP) van 19 mei 2022, Kamerstuk 29 628, nr. 1081, verzoekt de regering om een zwaarder belang toe te kennen aan veiligheidsvereisten bij aanbestedingen van apparatuur door de politie, zoals ANPR-camera's, afluisterapparatuur en drones en te streven naar apparatuur uit Nederland of op z'n minst uit landen binnen de Europese Unie.
[8] Kamerstuk 26 643, nr. 925.
[9] Kamerstuk 26 643, nr. 940.
[10] Zie onder meer www.bio-overheid.nl/ico-wizard/.