Rijksoverheid

Quickscan nationale veiligheid bij inkoop en aanbesteden

Zo houdt u rekening met nationale veiligheidsrisico's door dreigingen vanuit statelijke actoren

1

Toelichting

Nederland heeft een open en vrije markteconomie. Politiek en economie raken echter steeds meer met elkaar vervlochten, wat leidt tot een steeds verdere (geo)politisering van de (wereld) economie. Economische en de daarbij horende technologische ontwikkelingen vormen de basis voor politieke en militaire macht. Om grip te krijgen of te houden op die economische en technologische ontwikkelingen zetten staten onder andere economische instrumenten in, zoals de invloed die zij in of over bedrijven hebben. Dat betekent dat uw zakenpartners mogelijk niet alleen worden gedreven door economische motieven, maar dat motieven van een andere overheid leidend zijn. Overheden kunnen daarnaast vergaande toegang tot bedrijfsinformatie vastleggen in wet- en regelgeving in het kader van nationale veiligheid. Bedrijven en individuen zijn dan wettelijk verplicht medewerking te verlenen aan de overheid.

Inkoop en aanbesteding

Inkoop- en aanbestedingstrajecten in Nederland zijn aantrekkelijk voor statelijke actoren. Er wordt tijdens een inkoop- of aanbestedingstraject vaak veel informatie gedeeld, onder andere via openbare aanbestedingsdocumenten. Uit de documenten wordt veelal duidelijk over welk soort expertise bedrijven beschikken; hiermee worden potentiële doelwitten geïdentificeerd. Daarnaast kunnen statelijke actoren via inkoop- en aanbestedingstrajecten toegang krijgen tot gevoelige systemen of informatie, of kunnen zij een deel van de markt in handen krijgen. Dit marktaandeel kan op langere termijn risicovolle strategische afhankelijkheden opleveren. Verder bieden geleverde goederen en diensten statelijke actoren kansen voor sabotage en spionage. Zo is er de afgelopen jaren bij zowel aanbestedingen van Defensie, politie en andere Nederlandse overheidsinstanties een spionagerisico geconstateerd.[1] Niet alleen bij voor de hand liggende aanbestedingen zoals militair materiaal zijn risico's te vinden, maar ook bij relatief onschuldig ogende aanbestedingen voor bijvoorbeeld ICT-middelen.

De **Toolbox veilig inkopen** is ontwikkeld om bovenstaande risico's te signaleren en te bepalen of er maatregelen nodig zijn. De **Toolbox veilig inkopen** is bedoeld voor alle partijen die aanbestedingsplichtig zijn, zoals (een deel van) vitale aanbieders[2], de Rijksoverheid, lokale overheden (gemeenten, provincies en waterschappen) en kennisinstellingen. Ook partijen die niet aanbestedingsplichtig zijn, maar wel producten en diensten inkopen en zelf werken met gevoelige informatie, kennis of technologie, kunnen inspiratie opdoen uit deze toolbox. Daarnaast is de toepassing van de toolbox ook relevant voor partijen die moeten gaan voldoen aan de verplichtingen die voortvloeien uit de Europese richtlijnen Critical Entity Resilience Directive (CER) en Network and Information Security Directive 2 (NIS2) die zich richten op de continuïteit van de levering van essentiële diensten.[3] De **Toolbox veilig inkopen** bestaat uit 1) de **Quickscan** voor het signaleren van risico's, 2) de **Handleiding** voor het uitvoeren van risicoanalyses en 3) **de Quickguide,** een samenvatting van het document Handvatten[4] risicomitigatie, met aanbestedingsrechtelijke mogelijkheden om deze risico's te mitigeren.

Het instrument dat voor u ligt is de **Quickscan**, het eerste instrument van de **Toolbox veilig inkopen**. De Quickscan bestaat uit een beperkt aantal vragen om snel te kunnen bepalen of een inkoop en/of aanbestedingsopdracht (hierna: opdracht) mogelijk raakt aan een belang voor de nationale veiligheid.

Door wie wordt de Quickscan uitgevoerd?

De behoeftestellende partij (de achterliggende opdrachtgever) is verantwoordelijk voor voor a) het beoordelen of bij een opdracht mogelijk sprake is van een nationaal veiligheidsbelang en b) welke wet van toepassing is (Aanbestedingswet 2012 of de Aanbestedingswet op Defensie- en Veiligheidsgebied). De inkoper en/of aanbestedingsjurist uit de eigen organisatie ondersteunt de opdrachtgever bij het selecteren en toepassen van adequate risicomitigerende maatregelen in de aanbestedingsprocedure.

Wanneer wordt de Quickscan uitgevoerd?

De Quickscan dient in een zo vroeg mogelijk stadium in het inkoopproces te worden uitgevoerd, in ieder geval vóór het verzoek om offerte (bij enkel- of meervoudige onderhandse procedures) of ruim voordat de aankondiging van een opdracht wordt gepubliceerd (bij aanbestedingsprocedures).

Vervolg

Als uit de Quickscan blijkt dat er mogelijk risico's zijn of dat er aanvullend onderzoek nodig is, wordt geadviseerd om een risicoanalyse uit te voeren. Daarin wordt vastgesteld welke risico's er zijn en hoe kan worden gehandeld om deze risico's te mitigeren. Hiervoor kunt u gebruik maken van de **Handleiding** voor het uitvoeren van risicoanalyses.

[1] Zie ook het Dreigingsbeeld Statelijke Actoren 2, opgesteld door de AIVD, MIVD en NCTV van 2022.

[2] Dit betreft vitale aanbieders die vallen onder de zogenoemde speciale-sectorbedrijven zoals openbaarvervoerbedrijven, drinkwaterbedrijven, energiebedrijven en havenbedrijven.

[3] Deze Europese richtlijnen zijn gepubliceerd in december 2022.

[4] Handvatten risicomitigatie bij inkoop en aanbesteding. Voor aanbestedende diensten en vitale aanbieders. Uitgave van De Nationaal Coördinator Terrorismebestrijding en Veiligheid in samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Juni 2019.

Quickscan

Indien op één van onderstaande vragen 'ja/mogelijk' is geantwoord, zijn er mogelijk risico's voor de nationale veiligheid en is een risicoanalyse de volgende stap. Het is van belang om alle vragen één voor één af te lopen, ook als het antwoord op vraag 1 'nee' is. Mochten er zaken veranderen in de opdrachtverlening, doe de Quickscan dan opnieuw.

Verstoring van het vitale proces

Het gunnen van een opdracht aan een bepaalde partij kan ertoe leiden dat deze partij een positie verwerft waarmee de continuïteit van levering, dienstverlening of productie van één van de vitale processen kan worden beïnvloed. Vitale processen zijn processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid, denk aan telecommunicatie of energievoorziening.
In de bijlage van deze Quickscan is de lijst met vitale processen opgenomen.

• Kan de opdrachtnemer (of dienst onderaannemers) het vitale proces beïnvloeden (saboteren of manipuleren)? Krijgt de opdrachtnemers (of diens onderaannemers) bijvoorbeeld toegang tot systemen die controle geven over, of inzicht geven in (een deel van) het vitale proces?	☐ Ja/Mogelijk ☐ Nee	Toelichting:

Weglekken van gevoelige kennis, technologie en informatie

Het is mogelijk dat voor de uitvoering van een opdracht een opdrachtnemer (of diens onderaannemers) toegang krijgt of kan verschaffen tot hoogwaardige kennis, technologie en/of vertrouwelijke informatie. Denk bijvoorbeeld aan toegang tot kennis over het functioneren van vitale processen, datasets met (bijzondere) persoonsgegevens van Nederlandse burgers, bepaalde vertrouwelijke beleidsstandpunten en strategieën of technologische kennis voor militaire toepassingen die Nederland een unieke kennispositie geeft. Het kan zijn dat de opdrachtnemer directe toegang krijgt tot deze informatie of dat de opdrachtnemer toegang krijgt tot een (fysieke) locatie waardoor hij bij die gevoelige informatie kan komen.

Informatie
Heeft de opdrachtnemer (of diens onderaannemers) toegang (of toegang nodig) tot gevoelige informatie voor het uitvoeren van de opdracht?

• Is er sprake van toegang tot een grote set aan persoonsgegevens van burgers of specifieke persoonsgegevens van hooggeplaatsten (bijvoorbeeld thuisadressen, gegevens bewindspersonen, bestuurders of directe staf hiervan)?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot informatie die is gerubriceerd, bijvoorbeeld TLP amber, departementaal vertrouwelijk , staatsgeheim, EU-classified of NATO-classified?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot bedrijfsvertrouwelijke informatie, zoals strategiedocumenten, intellectueel eigendom, blauwdrukken, formules, datasets etc.?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot informatie die inzicht geeft in de ICT-infrastructuur?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot informatie die inzicht geeft in de digitale of fysieke beveiliging van een (gevoelige) locatie?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot informatie die inzicht geeft in de Nederlandse positie of positie van bondgenoten op een thema dat interessant kan zijn voor statelijke actoren?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Is er sprake van toegang tot de persoonsgegevens van personen die over een VGB beschikken en daarmee toegang hebben tot gevoelige informatie?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
• Wordt er gevoelige kennis, data of informatie opgeslagen op (buitenlandse) servers/locaties?	☐ Ja/Mogelijk ☐ Nee	Toelichting:

Quickscan

Locatie
Krijgt het personeel van de opdrachtnemer (en/of diens onderaannemers) toegang tot fysieke gevoelige locaties van de opdrachtgever?

1. Wordt er op die locatie gewerkt met staats-geheime, EU-classified, NATO-classified of bedrijfsvertrouwelijke* informatie?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
2. Wordt er toegang gegeven tot ruimtes waar computers staan en is er een mogelijkheid dat die computers (zonder toezicht) ingelogd zijn?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
3. Wordt er toegang gegeven tot gebouwen van de inlichtingen- en veiligheidsdiensten?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
4. Wordt er toegang gegeven tot werkplekken van bewindspersonen of bestuurders?	☐ Ja/Mogelijk ☐ Nee	Toelichting:
5. Wordt er toegang gegeven tot een locatie waarbij inzage wordt gegeven in gevoelige delen van het vitale proces (zie ook vraag 1)?	☐ Ja/Mogelijk ☐ Nee	Toelichting:

Vervolg

Indien op één van de bovenstaande vragen 'ja/mogelijk' is geantwoord, zijn er mogelijk risico's voor de nationale veiligheid en is een risicoanalyse de volgende stap. Hiervoor kunt u het document **Handleiding risicoanalyse** raadplegen. Bij vragen kunt u contact opnemen met de NCTV via ev@nctv.minjenv.nl.

In een risicoanalyse wordt uitgebreider stilgestaan bij het identificeren van de risico's voor de nationale veiligheid en wordt gekeken of en hoe risico's kunnen worden gemitigeerd. U bent zelf verantwoordelijk voor het nemen van maatregelen om risico's te mitigeren. Denk hierbij bijvoorbeeld aan het inbouwen van maatregelen in de selectiefase (selectiecriteria, uitsluitingsgronden, geschiktheidseisen), het kiezen van de juiste procedure of het formuleren van contractvoorwaarden.

* Denk bijvoorbeeld aan blauwdrukken, tekeningen, schema's, modellen, formules, tabellen, technische ontwerpen en specificaties, handboeken en instructies.

Bijlage Quickscan

1.1 Overzicht vitale processen

De volgende processen zijn benoemd als vitaal proces (situatie december 2023). Categorie A vitale processen hebben grotere gevolgen bij uitval dan categorie B vitale processen.
Voor meer informatie over de vitale infrastructuur en de actuele lijst van vitale processen zie: Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

Sector	Vitale processen	Verantwoordelijk departement
Energie	Transport, distributie, productie, hervergassing en opslag van gas op land en op zee	Economische Zaken en Klimaat
	Opslag, transport, raffinage en behandeling van ruwe olie en aardolieproducten'	
	Transport, distributie en productie van elektriciteit op land en op zee	
Telecommunicatie	Internet en datadiensten	Economische Zaken en klimaat
	Internettoegang en dataverkeer	
	Spraakdienst en SMS	
	Plaats- en tijdsbepaling	Infrastructuur en Waterstaat
Transport	Vlucht- en vliegtuigafwikkeling	Infrastructuur en Waterstaat
	Scheepvaartafwikkeling	
	Vervoer van personen en goederen over (hoofd) spoorweginfrastructuur	
	Vervoer over (hoofd)wegennet	
Drinkwater	Drinkwatervoorziening	
Water	Keren en beheren waterkwantiteit	
Chemie	Grootschalige productie, verwerking en/of opslag (petro)chemische stoffen	
Nucleair	Opslag, productie en verwerking nucleair materiaal	
Financiën	Toonbankbetalingsverkeer	Financiën
	Massaal giraal betalingsverkeer	
	Hoogwaardig betalingsverkeer tussen banken	
	Effectenverkeer	
Overheid	Basisregistraties personen en organisaties	Binnenlandse Zaken en Koninkrijksrelaties
	Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)	
	Elektronisch berichtenverkeer en informatieverschaffing aan burgers	
Openbare orde en veiligheid	Communicatie met en tussen hulpdiensten middels 112 en C2000	Justitie en Veiligheid
	Inzet politie	
Defensie	Inzet defensie	Defensie

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
Ministerie van Economische Zaken en Klimaat en de Nationaal
Coördinator Terrorismebestrijding en Veiligheid

December 2023 | Publicatienr. 23407255