Rijksoverheid

Risicoanalyse nationale veiligheid bij inkoop en aanbesteden

Identificeren van nationale veiligheidsrisico's voortkomend uit dreigingen door statelijke actoren.

2

Deze handleiding voor het uitvoeren van een risicoanalyse is een vervolg op de 'Quickscan nationale veiligheid bij inkoop en aanbesteden'. Bij het uitvoeren van de risicoanalyse brengt u in kaart of de leverancier toegang heeft tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken en of misbruik daarvan een nationaal veiligheidsrisico kan vormen. Daarbij onderzoekt u vervolgens welke beheersmaatregelen mogelijk en realiseerbaar zijn om de nationale veiligheidsrisico's voldoende te beperken. Deze handleiding is bedoeld als hulpmiddel voor de opdrachtgever van de inkoopopdracht of aanbesteding. In deze handleiding wordt u meegenomen in het proces van het opstellen van een risicoanalyse, van de voorbereiding ervan tot de vragen die u kunt beantwoorden om te beoordelen of er een risico is en vervolgens hoe groot dit risico is.

Verantwoordelijkheid
De opdrachtgever is verantwoordelijk voor de uitvoering van de risicoanalyse (inclusief voorbereiding, rapportage en follow up). De verantwoordelijkheid voor het maken van een afweging ten aanzien van welke mitigerende maatregelen passend zijn bij geïdentificeerde risico's ligt bij (het bestuur van) uw organisatie.

Rubricering
De analyses hebben een vertrouwelijk karakter, waardoor er selectief omgegaan dient te worden met het delen van de informatie uit de analyse. Indien er geheime informatie in de analyse wordt opgenomen dient de analyse een daarop aangepaste rubricering te krijgen.

Voorbereiding

Om de risicoanalyse goed te kunnen uitvoeren is het raadzaam aan te sluiten bij een breder risicomanagementproces van uw organisatie. Als u weet wat u in uw organisatie wilt beschermen (welke 'Te Beschermen Belangen' uw organisatie heeft), welke risico's op dit moment gelden en wat de huidige weerbaarheidsmaatregelen zijn, kunt u een betere inschatting maken ten aanzien van een specifieke inkoopopdracht of aanbesteding.

Voor het uitvoeren van een risicoanalyse kunnen ter voorbereiding de volgende stappen doorlopen worden:

1. Maak afspraken over de opzet van de risicoanalyse: welke scope en welk abstractieniveau wordt gehanteerd en binnen welke termijn moet de risicoanalyse zijn afgerond?
2. Maak aan de hand van bovenstaande de benodigde capaciteit voor een risicoanalyse beschikbaar:

Intern
- Benoeming van een moderator (begeleidt het proces van de risico- analyse) en een notulist.
- Inhoudelijke expertise ten aanzien van de opdracht: bepaalde expertise kan nodig zijn om in kaart te brengen welke risico's een opdracht met zich mee kan brengen. Bij een opdracht gericht op het ontwikkelen van een nieuwe netwerkomgeving kan bijvoorbeeld worden gedacht aan het betrekken van een IT-architect en IT-beheerder.
- Expertise inkoop en aanbesteding: betrek bijvoorbeeld een aanbestedingsjurist of inkoopadviseur bij de risicoanalyse die kennis heeft van de juridische mogelijkheden om risico's te mitigeren.

Extern
Indien nodig kunt u ook externe expertise betrekken bij de risicoanalyse. Bijvoorbeeld om meer informatie te verkrijgen over dreigingen vanuit statelijke actoren[1].

3. Verzamelen van benodigde documenten/informatie, onder andere:
- Quickscan
- Aard en omvang van het gebruik van de dienst of het product.
- Ketenafhankelijkheden in kaart brengen; op welke (vitale) processen (ook buiten uw organisatie) heeft de opdracht betrekking? Kan de opdrachtnemer bijvoorbeeld via uw netwerkomgeving ook bij andermans informatie, systemen of andere zaken?
- Marktscan: welke partijen zijn potentiële opdrachtnemers? Sommige risico's zijn leverancier afhankelijk. Om de risico's goed te kunnen identificeren en mitigeren is het van groot belang om een zo realistisch mogelijke marktscan uit te voeren om de potentiële opdrachtnemers in kaart te brengen.

4. Opstellen van een startnotitie met daarin een korte omschrijving van de opdracht en de relevante beschikbare informatie, onder andere verkregen door beantwoording van bovenstaande vragen. Deze notitie dient als het startpunt van de risicoanalyse.

[1] Denk aan het Dreigingsbeeld Statelijke Actoren 2, Cybersecuritybeeld Nederland 2023 en de jaarverslagen van de AIVD en MIVD.

Risicoanalyse

In dit onderdeel wordt toegelicht welke vragen beantwoord moeten worden om te komen tot een risicoanalyse.

De thema's die worden behandeld zijn ook aan bod gekomen in de Quickscan. Bij de risicoanalyse wordt hier uitgebreider bij stilgestaan door o.a. in kaart te brengen:

- Welke processen, systemen, informatie e.d. zijn toegankelijk via de opdracht?;
- Hoe kan het risico zich manifesteren: welke stappen moet een opdrachtnemer zetten om daadwerkelijk toegang te verkrijgen tot deze zaken?;
- Wat is de impact op het moment dat dit risico zich manifesteert?

1. Welke reële risico's voor de nationale veiligheid kunnen ontstaan door de opdracht?

a. Verstoring van de continuïteit van de vitale infrastructuur.	*Hoofdvraag: bestaat er een risico dat de opdracht ertoe leidt dat de continuïteit van levering, dienstverlening of productie van vitale processen in gevaar komt?*	• 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?
b. Het weglekken van gevoelige kennis, technologie en informatie.	*Hoofdvraag: heeft de opdrachtnemer (of diens onderaannemers) 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)? • Is er sprake van toegang tot informatie die is geclassificeerd als (TLP) gerubriceerd, staatsgeheim, EU-classified of NATO-classified? • Is er sprake van toegang tot bedrijfsvertrouwelijke informatie, zoals strategie-documenten, intellectueel eigendom, blauwdrukken, formules, datasets etc.? • Is er sprake van toegang tot informatie die inzicht geeft in de ICT-infrastructuur? • Is er sprake van toegang tot informatie die inzicht geeft in de digitale of fysieke beveiliging van een (gevoelige) locatie? • Is er sprake van toegang tot informatie die inzicht geeft in de Nederlandse positie of de positie van bondgenoten op een thema dat interessant kan zijn voor statelijke actoren? • Is er sprake van toegang tot de persoonsgegevens van personen die over een VGB beschikken en daarmee toegang hebben tot gevoelige informatie? • Wordt er gevoelige kennis, data of informatie opgeslagen op (buitenlandse) servers/ locaties? • Krijgt het personeel van de opdrachtnemer (en/of diens onderaannemers) toegang tot fysieke gevoelige locaties van de opdrachtgever? Denk hierbij aan de volgende vragen: - Wordt er op die locatie gewerkt met staatsgeheime, EU-classified, NATO-classified of bedrijfsvertrouwelijke informatie? - Wordt er toegang gegeven tot ruimtes waar computers staan en is er een mogelijkheid dat (zonder toezicht) op deze computers wordt ingelogd? - Wordt er toegang gegeven tot gebouwen van de inlichtingen- en veiligheids-diensten? - Wordt er toegang gegeven tot werkplekken van bewindspersonen of bestuurders? - Wordt er toegang gegeven tot een locatie waarbij inzage wordt gegeven in gevoelige delen van het vitale proces (zie ook vraag 1)?
c. Een strategische afhankelijkheid van partijen en landen met wie Nederland niet dezelfde geopolitieke belangen deelt.	*Hoofdvraag: ontstaat er door de opdracht een risicovolle strategische afhankelijkheid van een – al dan niet door een buitenlandse overheid aangestuurde – marktpartij of diens onderaannemers? Een afhankelijkheid is strategisch wanneer het betreffende product of dienst invloed uit kan oefenen op de vitale infrastructuur of toegang geeft tot gevoelige kennis, technologie en informatie (zie voorgaande vragen). Een afhankelijkheid is risicovol wanneer er geen of zeer weinig alternatieven voorhanden zijn.*	• Bestaat de mogelijkheid dat de leverancier, om wat voor reden dan ook, niet meer in staat is om het product of de dienst te leveren? • Zijn er alternatieve dienstverleners of leveranciers voorhanden voor deze aanbesteding?

Te beschermen belangen
Op basis van bovenstaande vragen heeft u geïdentificeerd of de aanbesteding raakt aan vitale infrastructuur of gevoelige kennis, technologie of informatie. Dit zijn de 'Te Beschermen Belangen' (TBB). Deze kunt u nader specificeren tot een lager abstractieniveau: bijvoorbeeld specifieke hardware of software die noodzakelijk is voor het draaiende houden van de vitale infrastructuur, of specifieke componenten waarop gevoelige data aanwezig is. Specificeer uw TBB´s zo nauwkeurig mogelijk.

2. Welke dreigingen van kwaadwillende actoren zijn er tegen de te beschermen belangen?

Om dit in kaart te brengen kunt u gebruik maken van de volgende (openbare) producten:

- Jaarverslagen AIVD en MIVD
- Dreigingsbeeld Statelijke Actoren (DBSA)
- Cybersecurity Beeld Nederland (CSBN)

Denk na over de vraag op welke wijze een kwaadwillende actor via het product of dienst bijvoorbeeld systemen kan saboteren of bepaalde data kan extraheren. En welke andere manieren zijn er, buiten de levering van het product of dienst om, waarop een kwaadwillende actor hetzelfde kan bereiken?

3. Welke maatregelen zijn beschikbaar om risico's af te dekken?'

Denk na over de maatregelen die uw organisatie op dit moment al treft om deze risico's af te dekken. Indien deze risico's (nog) niet voldoende worden afgedekt zijn er verschillende manieren om aanvullende maatregelen te treffen:

- Bijvoorbeeld binnen de aanbestedingsrechtelijke kaders, zoals specifieke aanbestedingsprocedures, uitsluitingsgronden en het stellen van geschiktheids- eisen en (bijzondere) contractvoorwaarden. Zie hiervoor ook de '**Quickguide**', samenvatting van het document 'Handvatten risicomitigatie[2]'.
- Denk ook aan beveiligingsmaatregelen die uw organisatie kan nemen om risico's te beheersen. Hiervoor kunt (of moet) u ook gebruik maken van de eisen zoals opgenomen in de Baseline Informatiebeveiliging Overheid (BIO)[3] en de Inkoopeisen Cybersecurity Overheid (ICO)[4].
- Ook is het relevant om afspraken te maken met de opdrachtnemer over o.a. de inzet van personeel, het bestuur en organisatie van de opdrachtnemer, fysieke beveiliging en digitale beveiliging. Ter inspiratie kan hiervoor ook worden gekeken naar de Algemene Beveiligingseisen Defensieopdrachten (ABDO)[5].

4. Zijn de aanvullende maatregelen afdoende in verhouding tot de onderkende risico's?

Is het risico afgedekt of is er sprake van een restrisico? Als er een restrisico is moet worden bepaald of dit acceptabel is. Dit hangt af van de opdracht en het waardeoordeel ten aanzien van het (rest)risico. Betreft een opdracht bijvoorbeeld de gedeeltelijke vervanging van een netwerk waardoor risico's minder impact hebben, of betreft de opdracht een volledig nieuw netwerk waardoor de impact groot kan zijn? Dit is een inschatting die per opdracht moet worden gemaakt.

[2] 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.
[3] Home NL - bio-overheid
[4] ICO Wizard - bio-overheid
[5] ABDO 2019 | Beleidsnota | Defensie.nl

Rapportage

De notulist stelt een rapportage op en stemt deze af met betrokkenen.

Conclusie
De volgende conclusies kunnen uit de risicoanalyse komen:

- De risico's kunnen voldoende worden beheerst (bijvoorbeeld door het opstellen van uitsluitingsgronden, contractvoorwaarden of door een opdracht geheim te verklaren);
- De risico's kunnen onvoldoende worden beheerst of er is aanvullend onderzoek nodig om een juiste conclusie te kunnen trekken. Denk bijvoorbeeld aan informatie die meer inzicht geeft in de dreiging en werkwijze van statelijke actoren. Neem hiervoor contact op met ev@nctv.minjenv.nl

Follow up

Na vaststelling van de risicoanalyse wordt aan de hand van de conclusie het vervolg van de opdracht bepaald.

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