29 628 Politie

30 821 Nationale Veiligheid

Nr. 1069 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 februari 2022

In het Vragenuur van 8 februari jl. heb ik lid Van Nispen (SP) toegezegd in te gaan op de wijze waarop wordt omgegaan met veiligheids- en spionagerisico's bij het gebruik van apparatuur door politie en de inlichtingendiensten (Handelingen II 2021/22, nr. 47, Mondelingen vragen van het lid Rajkowski over het bericht 'Russische en Chinese diensten gebruiken Linkedin voor spionage bij Nederlandse bedrijven).

Het uitgangspunt is dat het gebruik van apparatuur en programmatuur altijd veilig moet zijn en eventuele risico's gemonitord en beperkt worden. Het risicobeleid ten aanzien van nationale veiligheid bij inkoop en aanbesteding is daarom constant in ontwikkeling en heeft blijvende aandacht. De afgelopen jaren zijn zowel door het Rijk als door de politie aanvullende en verscherpte maatregelen genomen om de veiligheid te blijven waarborgen.
In deze brief ga ik allereerst in op de bestaande risico's en het daarop ingerichte risicobeleid bij inkoop en aanbesteding van systemen. De heer Van Nispen refereerde specifiek aan het tapsysteem van politie. In deze brief geef ik aanvullend aan hoe risico's bij dit systeem worden beperkt.

Bestaande risico's ten aanzien van nationale veiligheid bij inkoop en aanbesteding
Zoals in het Dreigingsbeeld Statelijke Actoren (DBSA) van de NCTV en inlichtingendiensten is beschreven (Bijlage bij Kamerstuk 30 821, nr. 124), is een toenemende afhankelijkheid van buitenlandse technologie een gegeven, aangezien geen land beschikt over alle kennis en productiemiddelen om technologisch onafhankelijk te opereren. Wel bestaat het risico dat met technologische toeleveringen de digitale spionage- en sabotagemogelijkheden toenemen. Risico's voor de nationale veiligheid kunnen met name ontstaan wanneer deze technologie de Nederlandse vitale infrastructuur raakt, of wanneer deze technologie raakt aan gevoelige kennis en informatie. Een aanvullend risico kan ontstaan als er betrokkenheid is van leveranciers uit bepaalde landen die via nationale wet- en regelgeving gedwongen kunnen worden tot medewerking aan inlichtingenactiviteiten. De risico's voor de nationale veiligheid worden ten slotte vergroot als het landen betreft die een offensief cyberprogramma voeren tegen de Nederlandse belangen en wanneer (technische) mogelijkheden om risico's te adresseren niet voorhanden zijn.

Risicobeleid ten aanzien van nationale veiligheid bij inkoop en aanbesteding
In algemene zin geldt dat eind 2018 ten aanzien van nationale veiligheidsrisico's een verscherpt inkoop- en aanbestedingsbeleid is geïmplementeerd voor de rijksoverheid. Hierin is opgenomen dat bij inkoop en aanbesteding mogelijke risico's voor de nationale veiligheid per inkoopopdracht worden meegewogen. Bij de aanschaf en implementatie van gevoelige apparatuur of programmatuur wordt volgens dit beleid rekening gehouden met zowel risico's in relatie tot een

leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld als het gaat om de toegang tot systemen door derden.

Ter ondersteuning van dit beleid is aanvullend instrumentarium ontwikkeld door de NCTV dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen. Ook de politie is bekend met dit instrumentarium.

Per praktijksituatie moet worden bezien hoe eventuele risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Een belangrijk uitgangspunt hierbij is dat maatregelen die hiertoe genomen worden proportioneel zijn. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiginginschatting en de (huidige) weerbaarheid.

Met bovenstaand beleid wordt stevig ingezet om de veiligheid ten aanzien van de continuïteit van vitale processen, de integriteit en exclusiviteit van kennis en informatie en de ongewenste opbouw van strategische afhankelijkheden te waarborgen.

Tapsysteem politie
Zoals uw Kamer eerder is bericht[1] is de inzet van een commerciële partij een bewuste keuze vanwege de complexiteit, investeringsgrootte en de specialistische capaciteit, kennis en kunde die daar voor nodig is. Zelfbouw is daarom geen optie. Daar komt bij dat de telecom-wereld zich continu ontwikkelt, wat betekent dat ook het tappen continu moet meebewegen. Dit vraagt een constante innovatieve ontwikkeling van systemen. Bij de aanbesteding heeft politie de Europese aanbestedingsregels in acht genomen. Dit maakte onder andere dat inschrijving ook voor partijen buiten Nederland openstond. In de brieven van 1 juli 2019[2] en 27 mei 2020[3] heeft mijn voorganger laten weten dat de politie op dit moment een tapsysteem implementeert van Cyber Intelligence Ltd., dochterbedrijf van Elbit Systems uit Israël. Deze leverancier is als beste partij naar voren gekomen na een zorgvuldig doorlopen aanbestedingstraject. Hierbij waren de criteria onder meer functionaliteit, de mogelijkheden voor doorontwikkeling, security-eisen alsook de kosten.

In het kader van de aan uw Kamer toegezegde transparantie is gekozen voor zowel een open als een gesloten fase in het proces van de aanbesteding. Daarin zijn ook eisen meegenomen met betrekking tot toegang, logging en monitoring zodat eventuele risico's op deze onderwerpen beheersbaar worden gemaakt.

De totstandkoming van het hiervoor genoemde verscherpte inkoop- en aanbestedingsbeleid ten aanzien van nationale veiligheidsrisico's vond plaats na de aanschaf van het tapsysteem van politie. Het tapsysteem betreft geen vitale infrastructuur zoals is gedefinieerd in het overzicht vitale processen van de NCTV.

---

[1] Kamerstuk 30 517, nr. 31.
[2] Kamerstuk 29 628, nr. 890.
[3] Kamerstuk 29 628, nr. 948.

Nadat het instrumentarium beschikbaar kwam is vastgesteld dat de politie met de getroffen maatregelen rondom het tapsysteem reeds had gehandeld overeenkomstig het verscherpte beleid zoals geadviseerd door NCTV en AIVD.

De politie heeft dit systeem gekocht en is daarmee de eigenaar. Waar in het in het oktober jl. aan uw Kamer verstrekte rapport van de Auditdienst Rijk[4] wordt gesproken over systeemeigenaarschap wordt gedoeld op een bevinding dat niet duidelijk was vastgelegd welk organisatieonderdeel bij de politie verantwoordelijk is voor het wijzigingsproces. Naar aanleiding van het ADR-rapport heeft de politie de governance rond interceptie opnieuw vastgelegd met de portefeuillehouder specialistische opsporing als eigenaar.

Concluderend is de aanbesteding van het tapsysteem zorgvuldig doorlopen, is het overeenkomstig het verscherpte veiligheidsbeleid en is de politie zelfstandig en als enige eigenaar van het tapsysteem.

Toezicht en beveiliging tapsysteem politie
Het tapsysteem staat in het hoogbeveiligde rekencentrum van de politie. Tijdens de huidige implementatieperiode als ook na ingebruikname van het systeem door de politie heeft de leverancier geen fysieke en logische toegang tot productiedata (tapdata). De leverancier levert software maar verwerkt geen tapdata en heeft dan ook geen toegang tot de tapdata. Een verwerkersovereenkomst met de leverancier is derhalve niet aan de orde. De politie verwerkt zelf de tapdata. Binnen de politie hebben alleen de daartoe bevoegde politiemedewerkers toegang tot de voor hen bestemde gegevens. Met betrekking tot het tapsysteem zijn contractuele afspraken gemaakt en interne beheermaatregelen getroffen ter voorkoming van toegang door de leverancier tot gevoelige locaties en infrastructuur van de politie.

Ter borging hiervan zijn onder andere diverse eisen met betrekking tot logging en monitoring contractueel vastgelegd. Verder voeren de beveiligingsexperts periodiek beveiligingsonderzoeken waaronder pentesten uit en is er constante monitoring van ongewenst netwerkverkeer. Hiermee worden kwetsbaarheden en risico's in kaart gebracht. Daarnaast geldt het kader van de Normstelling Inrichting Interceptieketen, waarop audits door de ADR worden uitgevoerd. De normstelling is onderdeel van de informatiebeveiligingsregeling van de politie. Afhankelijk van de bevindingen worden passende maatregelen getroffen.

Met de hiervoor genoemde maatregelen is er sprake van intensief intern en extern toezicht op het tapsysteem van de politie.

Ik ga ervan uit dat ik u hiermee voldoende heb geïnformeerd.

De minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

[4] Kamerstuk 29 628, nr. 1047