

Vergaderjaar 2018–2019

25 124

Nieuwe infrastructuur mobiele communicatie (C2000)

29 628

Politie

Nr. 92

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 december 2018

Met mijn brief van 17 september jl. heb ik uw Kamer geïnformeerd over de voortgang van de vernieuwing van het C2000 spraaknetwerk (Kamerstuk 25 124, nr. 91). In deze brief informeer ik u over de huidige stand van zaken van de vernieuwing van het C2000 spraaknetwerk en zal ik tevens ingaan op een aantal andere ontwikkelingen in het meldkamer-domein, waaronder de vernieuwing van de 1-1-2 infrastructuur en de invoering van locatiebepaling bij 1-1-2 meldingen door middel van de Advanced Mobile Location (AML) techniek. Daarnaast ga ik in op een toezegging aan uw Kamer tijdens het AO ICT politie.

Toezegging AO ICT politie

In het AO ICT politie van 17 oktober jl. heb ik toegezegd uw Kamer te informeren over de overgangsregeling en een kostendekkend tarief voor het gebruik van C2000 portofoons door groene boa's (Kamerstuk 29 628, nr. 821). Alle aangewezen gebruikers van het C2000 netwerk (Politie, brandweer, ambulance en Defensie) zijn zelf verantwoordelijk voor de aanschaf, de beveiliging en het gebruik van randapparatuur als portofoons en mobilofoons en dragen hier ook zelf de kosten voor. Indien de aangewezen gebruiker randapparatuur aan een gelieerde samenwerkingspartner beschikbaar stelt, blijft de aangewezen gebruiker verantwoordelijk voor het beheer en voor de naleving van het beveiligingsbeleid. Daarbij mogen de kosten voor de aanschaf, het gebruiksklaar maken, het beheer en onderhoud van het randapparaat en het gebruik van het netwerk worden doorberekend.

In het verleden zijn hierover door de 25 regionale politiekorpsen verschillende afspraken met samenwerkingspartners gemaakt. Na de vorming van de nationale politie kiest de politie hierin nu een eenduidige lijn. Dit betekent dat die partners waar de politie in het verleden de kosten van voor haar eigen rekening heeft genomen, hier nu voor worden aangeslagen.

De politie heeft mij laten weten dat zij op mijn verzoek voor 2018 en 2019, als overgangperiode, nog geen kosten voor het portofoon gebruik van groene boa's in rekening zal brengen. Ik zal tot een nieuwe kostprijsberekening komen op basis van het vernieuwde C2000 spraaknetwerk.

Vernieuwing C2000

In mijn brief van 26 april 2018¹ heb ik aangegeven hoe de continuïteit van het huidige netwerk in 2019 wordt geborgd. Daarbij moet in ogenschouw worden genomen dat vernieuwing noodzakelijk is, omdat het huidige netwerk het einde van de technologische levensduur heeft bereikt.

In mijn kamerbrief van 17 september jl.² heb ik toegelicht dat de migratie van het spraaknetwerk niet dit najaar kon plaatsvinden. Om de veiligheid van hulpverleners en burgers te kunnen blijven waarborgen, heb ik toen, in overleg met de vertegenwoordigers van de operationele diensten, besloten voldoende tijd te nemen om het nieuwe netwerk te vervolmaken en testen.

Pilot en migratie

In de nacht van 12 op 13 november jl. vond in Limburg de proefmigratie plaats van het vernieuwde C2000 spraaknetwerk. De overgang van het huidige naar het vernieuwde spraaknetwerk en weer terug is tijdens deze proefmigratie van begin tot eind succesvol uitgevoerd.

Bij de proefmigratie is het oude netwerk tijdelijk uitgeschakeld en het nieuwe netwerk aangezet. Het programma Implementatie Vernieuwing C2000 (IVC) heeft samen met de hulpdiensten en Defensie een aantal testen succesvol uitgevoerd. Daarna is het oude netwerk weer in gebruik genomen. De hulpdiensten hebben deze nacht met alternatieve middelen gecommuniceerd. Zowel de migratie zelf als het gebruik van de alternatieve middelen van communicatie, worden in nauwe samenwerking met de hulpdiensten en het Ministerie van Defensie geëvalueerd.

Veiligheid van het systeem

Bij het ontwerpen en bouwen van het nieuwe spraaknetwerk van C2000 staat de robuustheid en de betrouwbaarheid centraal. Daarbij hoort dat C2000 een veilig systeem is. De communicatie via C2000 is versleuteld en maakt gebruik van afgeschermdde verbindingen. Het beveiligingsniveau van het vernieuwde C2000 is, evenals het huidige C2000, bepaald op departementaal vertrouwelijk. Dit houdt in dat de operationele informatie die over het netwerk gaat niet openbaar is, maar geen staatsgeheime informatie betreft.

Het systeem is zonder aanvullende maatregelen niet bedoeld voor communicatie boven het niveau departementaal vertrouwelijk. Gebruikersgroepen van C2000 met hogere beveiligingsseisen kunnen gebruik maken van extra beveiligingsmaatregelen, waaronder extra versleuteling van het berichtenverkeer. Het C2000 spraaknetwerk wordt beveiligd door een combinatie van fysieke (hekken, sloten), organisatorische (screening personeel) en elektronische (alarmering, versleuteling van de radiocommunicatie) beveiligingsmaatregelen. Als bijvoorbeeld een portofoon als vermist/gestolen wordt gedetecteerd en dit wordt gemeld, dan wordt deze geblokkeerd. Dit kan een tijdelijke of een permanente blokkering

¹ Kamerstuk 25 124, nr. 89

² Kamerstuk 25 124, nr. 91

opleveren, waardoor deze randapparatuur onbruikbaar is geworden voor onbevoegden.³

Ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere derde partijen, opereert het kabinet als volgt. Op een zeer zorgvuldige en case-by-case-basis worden de risico's ten aanzien van digitale producten gezien, waarbij in ieder geval wordt betrokken of sprake is van:

- digitale diensten/producten die de Nederlandse infrastructuur of de Nederlandse economie in den brede kunnen binnendringen c.q. een essentiële/substantiële rol kunnen spelen?
- één of meer (deel)leveranciers die onder de invloed of soevereiniteit vallen van een statelijke actor die de betreffende (deel)leverancier kan verplichten in opdracht van de statelijke actor te handelen?
- aanwijzingen dat de statelijke actor zich richt tegen Nederlandse belangen?

Dit geldt ook voor de risicobeoordeling ten aanzien van het nieuwe C2000. In mijn brief van 17 september jl. heb ik u geïnformeerd dat ik specifiek voor C2000 aanvullend aan eerdere onderzoeken en de beveiligingsmaatregelen die al zijn getroffen, een security audit laat uitvoeren alsook het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD om advies heb gevraagd (Kamerstuk 25 124, nr. 91).

Het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD heb ik gevraagd, of door de betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van C2000, de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat worden geschaad. Daarnaast wordt gezien of buiten bestaande reguliere beveiligingsmaatregelen aanvullende maatregelen noodzakelijk zijn.

Het bedrijf Xebia voert momenteel een security audit uit naar de technische en organisatorische maatregelen die Hytera als onderdeel van de vernieuwing van C2000 neemt. Xebia beziet of en in welke mate de leverancier zichzelf oneigenlijke toegang zou kunnen verschaffen. Tevens beziet Xebia welke technische maatregelen zijn getroffen om oneigenlijke toegang onmogelijk te maken, en oneigenlijk gebruik te detecteren.

Nog voor het einde van dit kalenderjaar verwacht ik de oplevering van de security audit door Xebia. Het advies van de AIVD volgt begin volgend jaar. Ik zal de security audit van Xebia en het advies van de AIVD in samenhang bestuderen zodat ik een integrale afweging kan maken of, en zo ja, welke extra (beveiligings) maatregelen nodig zijn. Ik zal uw Kamer hierover rapporteren. Dit sluit aan bij de moties van het lid Laan-Geselschap (VVD) (Kamerstuk 29 628, nr. 829) en de motie van de leden Den Boer (D66), Van Dam (CDA) en Verhoeven (D66) (Kamerstuk 29 628, nr. 828).

Tot slot

Zoals ook in de technische briefing van 28 november jl. is toegelicht, komt de vernieuwing van het spraaknetwerk C2000 tot stand door de gezamenlijke inspanning van de leveranciers, de programmaorganisatie, de beheerders en de gebruikers van politie, brandweer/veiligheidsregio's, ambulancediensten en het Ministerie van Defensie. Zorgvuldigheid, veiligheid, continuïteit en risicobeheersing staan daarbij te allen tijde voorop.

³ Kamerstukken 29 628 en 25 124, nr. 631

Ontwikkelingen meldkamerdomein

Wetsvoorstel Meldkamers

Op 30 oktober jl. heeft uw Kamer het wetsvoorstel meldkamers ontvangen (Kamerstuk 35 065). Dit wetsvoorstel vormt de basis voor de nieuwe inrichting van het meldkamerdomein. Op hoofdlijnen regelt het wetsvoorstel dat het beheer van de (ten hoogste tien) meldkamers wordt ondergebracht bij de politie. Op dit moment ligt deze verantwoordelijkheid nog bij de besturen van de veiligheidsregio's. De verantwoordelijkheid voor de uitvoering van de meldkamerfunctie blijft bij de hulpdiensten zelf. Vanuit elke meldkamer kan de meldkamerfunctie zo nodig ook binnen het werkgebied van een andere meldkamer worden uitgevoerd, waarmee wordt beoogd dat elk incident in heel Nederland kan worden afgehandeld, onafhankelijk van waar het zich voordoet. Met deze wettelijke basis wordt een belangrijke stap gezet om de continuïteit van meldkamers te vergroten.

Stand van zaken 1-1-2

In mijn brief van 22 januari 2018 over de nieuwe techniek Advanced Mobile Location (AML) voor locatiebepaling bij 1-1-2 meldingen heb ik aangegeven de intentie te hebben om nog dit jaar AML in te voeren.⁴ AML voldoet aan de Algemene Verordening Gegevensbescherming, de politie heeft hier een toets op uitgevoerd. Bij telefoons die deze functie ondersteunen kan dan nauwkeurige locatie-informatie automatisch worden meegestuurd bij een 1-1-2 oproep. Door een constructieve samenwerking tussen de politie, de telecomproviders en mijn departement zijn bijna alle randvoorwaarden voor implementatie ingevuld. AML is technisch gereed. Begin 2019 wordt gestart met de gebruikers van toestellen gebaseerd op Google technologie. Later in 2019 volgen naar alle waarschijnlijkheid de gebruikers van telefoons gebaseerd op Apple technologie.

Naast de invoering van AML wordt er door politie ook gewerkt aan de invoering van een 1-1-2 app. Halverwege 2019 wordt een nieuwe technische infrastructuur voor de 1-1-2 dienstverlening in gebruik genomen. Hierover heb ik u eerder geïnformeerd in mijn «Verzamelbrief 1-1-2 aangelegenheden» van 16 maart 2016⁵. Zodra de vernieuwing van de nieuwe technische infrastructuur voor de 1-1-2 dienstverlening is gerealiseerd, kan de werking van de 1-1-2 app beproefd worden.

Daarnaast merk ik nog op dat inmiddels de afronding nadert van het onderzoek door de Inspectie Justitie en Veiligheid naar de continuïteit van de meldkamers. Ik verwacht u dit onderzoek aan het begin van 2019 te kunnen toezenden.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

⁴ Kamerstuk 29 517, nr. 138

⁵ Kamerstuk 29 517, nr. 112