Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

25 124 Nieuwe infrastructuur mobiele communicatie (C2000)

29 628 Politie

Nr. 84 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 maart 2017

In de brief «Stand van Zaken C2000 en Landelijke Meldkamerorganisatie» van 2 november 2016 (Kamerstukken 25 124 en 29 517, nr. 81) heeft mijn ambtsvoorganger uw Kamer geïnformeerd dat de auditdienst Rijk (ADR) de beveiligingsmaatregelen, zoals geformuleerd in het beveiligingsbeleid C2000, zou toetsen. Eveneens heeft hij in het AO Nationale Veiligheid van 10 november 2016 (Kamerstuk 29 517, nr. 118) uw Kamer toegezegd te zullen informeren of een verbod op apparatuur als «Target Blu Eye» noodzakelijk is. In deze brief informeer ik u over de uitkomst van beide trajecten.

Beveiligingsbeleid C2000

De ADR heeft op mijn verzoek een toets uitgevoerd naar de naleving van het beveiligingsbeleid C2000. Zoals ik u vorig jaar heb aangegeven vormden de vernieuwing van C2000, de berichtgeving over de Target Blu Eye en een signaal over internationaal geldende beveiligingsstandaarden hiervoor de concrete aanleiding. Voor dit onderzoek heeft de ADR een aantal thema's uit het beveiligingsbeleid geselecteerd. Daarbij is bij een beperkt aantal gebruikers onderzoek gedaan. Dit onderzoek doet daarom geen algehele uitspraak over de beveiliging van C2000 als geheel, desalniettemin levert dit onderzoek inzichten op waarmee de beveiliging van C2000 verder kan worden verbeterd. Het rapport Onderzoek beveiliging C2000 treft u als bijlage aan[1].

In het rapport constateert de ADR dat bij de gebruikers, beheerders en het Ministerie van Veiligheid en Justitie (VenJ) de laatste jaren vooral de focus heeft gelegen op capaciteit en dekking van het netwerk, organisatorische wijzigingen, het gebruik en de vernieuwing van het systeem. Hierdoor heeft de naleving van het beveiligingsbeleid niet altijd de aandacht gehad die het nodig heeft. De ADR signaleert verbeterpunten ten aanzien van het beleggen van taken en verantwoordelijkheden, het doorvertalen van de

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-25124-84
ISSN 0921 - 7371
's-Gravenhage 2017

gemaakte Afhankelijkheids- en Kwetsbaarheidsanalyse in vernieuwd beleid, de invulling van de toezichthoudende rol, de controle op de inventaris en aandacht voor de beveiligingseisen en bewustwording bij de gebruikers.
Naast deze verbeterpunten constateert de ADR overigens een sterk «vakmanschap» op operationeel niveau. De ADR stelt dat, ondanks dat de eindgebruikers niet altijd expliciet op de hoogte zijn van de geldende voorschriften, er doorgaans wel intrinsiek een relatief hoog beveiligingsbewustzijn aanwezig is.

De ADR adviseert om de verbeterpunten te verwerken in een roadmap waarbij, samen met de verschillende C2000-gebruikers, vanuit een risicogerichte benadering wordt bezien welke maatregelen nog getroffen moeten worden en in welke volgorde. Zij geven daarbij aan dat gekeken moet worden naar een optimaal niveau van beveiliging. Het maken van keuzes hierin is onontbeerlijk.

Ik onderschrijf deze bevindingen en aanbevelingen uit het rapport. De komende periode zal VenJ samen met de C2000 gebruikers werken aan een roadmap «beveiliging C2000». Het is de doelstelling om deze roadmap voor de zomer 2017 gereed te hebben om vervolgens maatregelen op te laten volgen met het oog op de vernieuwing van het C2000 netwerk.

Op korte termijn zal in ieder geval met de implementatie van een aantal prioritaire en of snel te realiseren maatregelen gestart worden:
– Het actief monitoren op verdachte patronen van randapparatuur. Ik heb de politie gevraagd hiervoor een aantal pragmatische voorstellen te doen waarbij rekening wordt gehouden met effectiviteit, kosten en vigerend informatiebeveiligingsbeleid van de gebruikersorganisaties.
– Het verbeteren van het zicht op de randapparatuur door middel van een regelmatig uit te voeren inventarisatie en controle van de registratie van de randapparatuur. Ik zal de gebruikers verzoeken hier aandacht aan te besteden en waar nodig maatregelen te nemen.
– Het verduidelijken van de incidentenprocedure voor C2000 om duidelijk te maken dat bij eventuele beveiligingsincidenten het bekend is bij wie eindgebruikers melding kunnen maken van verlies of diefstal van apparatuur. Ik zal de gebruikers verzoeken hier aandacht aan te besteden.

Ik zal daarnaast bezien of de beleidsregels beveiligingsbeleid C2000 (2012) nog aanpassing behoeven en waar nodig deze aanpassen.

Target Blu Eye

In het voorjaar van 2016 heeft mijn ambtsvoorganger aan uw Kamer aangegeven dat hij nader onderzoek zou laten doen naar de noodzaak van een verbodsbepaling voor de «Target Blu Eye» en dat hij u op basis van dit onderzoek nader zou berichten over eventuele vervolgstappen (Kamerstukken 29 628 en 25 124, nr. 631). Deze toezegging is gedaan naar aanleiding van de motie van de leden Kooiman en Tellegen (Kamerstuk 29 628, nr. 613).

Om een goede afweging te kunnen maken over het al dan niet invoeren van een verbodsbepaling op apparatuur als de «Target Blu Eye» is door een extern onderzoeksbureau een analyse gemaakt naar de aard van het gebruik van dergelijke apparatuur (Kamerstukken 25 124 en 29 517, nr. 81). Het onderzoeksrapport «Target Blu Eye» is gerubriceerd als «Departe-

mentaal Vertrouwelijk». Bij deze bied ik u dit rapport aan ter vertrouwelijke inzage tot 31 december 2017[2].

Het rapport gaat in op de aard en omvang van het gebruik van apparatuur als de «Target Blu Eye», de potentiële negatieve effecten daarvan voor de politie en mogelijke opties om het ongewenste effect aan te pakken waaronder de verbodsbepaling. In het rapport wordt geconstateerd dat apparatuur als de «Target Blu Eye» hinderlijk kan zijn voor de opsporing en dat er ten aanzien van misbruik een duidelijke link is met georganiseerde criminaliteit.

Zoals mijn ambtsvoorganger u reeds eerder heeft gemeld (Kamerstukken 29 628 en 25 124, nr. 631), is het nu al mogelijk inbeslagneming en verbeurdverklaring als ondersteunende juridische maatregelen in te zetten om tegen het gebruik op te treden, mits het apparaat aantoonbaar wordt gebruikt als hulpmiddel om een strafbaar feit te plegen. Het rapport geeft aan dat vanuit de opsporingspraktijk een verbod niet als meerwaarde wordt gezien als toevoeging op de huidige juridische mogelijkheden voor inbeslagname.

Het rapport stelt verder dat potentiële negatieve effecten van het gebruik van apparatuur voor de opsporing beter op een andere manier kunnen worden beperkt, o.a. door middel van verdere bewustwording en werkwijze. Met de politie onderschrijf ik de conclusies van het rapport en zie daarom op dit moment onvoldoende reden om een verbod te initiëren. De politie heeft aangegeven er in haar werkwijze nu al rekening mee te houden dat apparatuur als de «Target Blu Eye» voorhanden kan zijn bij criminelen. De bevindingen van het rapport zullen waar nodig verder bijdragen aan bewustwording binnen de politie en het nemen van alternatieve maatregelen.

De Minister van Veiligheid en Justitie,
S.A. Blok

[2] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer.