Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

25 124 **Nieuwe infrastructuur mobiele communicatie (C2000)**

29 517 **Veiligheidsregio's**

Nr. 109 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 februari 2022

Hierbij stuur ik u het rapport «Informatiebeveiliging van meldkamersystemen» dat ik op 16 december 2021 heb ontvangen van de Inspectie Justitie en Veiligheid (hierna: Inspectie)[1]. Ik dank de Inspectie voor het rapport en de gedane aanbevelingen. Ik neem de constateringen van de Inspectie zeer serieus en in deze brief beschrijf ik hoe ik de aanbevelingen van de Inspectie oppak. Graag wijs ik u erop dat deze brief in lijn is met en aansluit op mijn eerdere brief van 23 september 2021[2] over de ontwikkelingen en continuïteit in het meldkamerdomein.

Conclusies Inspectie

De belangrijkste conclusie van de Inspectie is dat het risicomanagement voor de informatiebeveiliging van meldkamersystemen nog niet voldoende is ingericht en geborgd. De inspectie constateert dat:

1) niet wordt gestuurd op basis van risicomanagement;
2) het proces voor het vaststellen van basiscriteria voor het inrichten, toepassen en borgen van het risicomanagement nog niet volledig is doorlopen;
3) de risico's voor informatiebeveiliging van de meldkamersystemen nog niet volledig zijn beoordeeld en vergeleken met de criteria voor het evalueren en accepteren van risico's;
4) de maatregelen die zijn getroffen voor risicobeperking zijn gekozen op basis van de meest voorkomende bedreigingen, hierdoor bestaat het risico dat het ontbreekt aan de juiste informatie voor het gericht aansturen op risico beperkende maatregelen;
5) voor het inrichten en borgen van risicomanagement nog geen criteria zijn vastgesteld voor het accepteren van rest-risico's.

De Inspectie beveelt aan het commitment voor informatiebeveiliging te borgen en prioriteit te geven aan het versneld ontwikkelen en toepassen

[1] Raadpleegbaar via www.tweedekamer.nl.
[2] Kamerstuk 25 124 en 29 517, nr. 108.

kst-25124-109
ISSN 0921 - 7371
's-Gravenhage 2022

van risicomanagementsystematiek op de meldkamersystemen door de risico's te waarborgen met rapportages, audits en door gerichte sturing op de voortgang van verbetering van het beheer.

Ik onderschrijf de conclusies van de Inspectie dat we nog flinke stappen moeten zetten op het gebied van risicomanagement voor de beveiliging van meldkamersystemen. Het onderwerp staat daarom hoog op de agenda van alle betrokken partijen[3]. Graag zet ik hieronder uiteen welke lopende en toekomstige ontwikkelingen bijdragen aan het inrichten en borgen van het risicomanagement voor de beveiliging van meldkamersystemen. Ik schets een beeld hoe we in algemene zin omgaan met de beveiliging van meldkamersystemen. Daarna ga ik specifiek in op een van de belangrijke systemen in de meldkamers, het missiekritische communicatiesysteem C2000. Dit doe ik omdat we, zoals ook beschreven in het Inspectierapport, voor dit systeem al verder zijn in de ontwikkeling van het risicomanagement.

Borging en inrichting risicomanagement in de meldkamers

Zoals de Inspectie aangeeft dient het ontwikkelen van informatiebeveiligingsbeleid en het in kaart brengen van de te nemen maatregelen voor de beveiliging van meldkamersystemen plaats te vinden op basis van een risicomanagementsystematiek. Het Strategisch Meldkamer Beraad heeft daar onlangs een vervolg-stap gezet door het vaststellen van de kaders voor informatiebeveiliging en het basisbeveiligingsniveau voor de meldkamersystemen[4]. Belangrijk daarbij is dat de disciplines gezamenlijk tot een kader zijn gekomen.

Mijn ministerie werkt op dit moment aan de ontwikkeling van strategische kaders voor informatiebeveiligingsbeleid voor de meldkamersystemen. De disciplines en de Landelijke Meldkamer Samenwerking richten zich op de invulling van het informatiebeveiligingsbeleid en implementatie van de concrete elementen uit de Baseline Informatiebeveiliging Overheid binnen de meldkamer. De korpschef is verantwoordelijk en voert dit uit vanuit zijn verantwoordelijkheid voor het beheer. Het Strategisch Meldkamer Beraad ziet toe op de uitwerking en stuurt in dit kader daar waar het gaat om het beheer van ICT voorzieningen van de meldkamers. De disciplines zijn zelfstandig verantwoordelijk voor de implementatie en uitvoering daar waar het gaat over de eigen discipline. De eerstvolgende stap die we nu gezamenlijk moeten zetten, is het systematisch inventariseren van de risico's per meldkamersysteem om de verdere invulling voor de beveiliging op basis van maatwerk op orde te krijgen.

Informatiebeveiliging C2000

Het programma Implementatie Vernieuwing C2000 van mijn ministerie en de Landelijke Meldkamer Samenwerking werken met prioriteit aan het risicomanagement voor de informatiebeveiliging van centrale en decentrale infrastructuur van het meldkamersysteem C2000. Op basis van eerder uitgevoerde onderzoeken[5] zijn de grootste risico's op het gebied van informatiebeveiliging voor C2000 geïnventariseerd. Het programma Implementatie Vernieuwing C2000 werkte het afgelopen jaar aan de

---

[3] de Minister voor Medische Zorg en de Regionale Ambulancevoorzieningen voor zover het de ambulancezorg betreft, de besturen van de veiligheidsregio's voor zover het de brandweertaak, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening betreft, de Minister van Defensie voor zover het de Koninklijke marechaussee betreft en de politie.

[4] De disciplines hebben met elkaar de Baseline Informatiebeveiliging Overheid vastgesteld als kader. Het basisbeveiligingsniveau is vastgesteld op BBN2+.

[5] ADR, onderzoek Beveiliging C2000, 2017. Kamerstuk 25 124, nr. 96.

implementatie van de benodigde maatregelen bij zowel de leveranciers als de beheerorganisatie van C2000 met als doel de beveiliging van C2000 verder op orde te krijgen. Het merendeel van de technische en een groot deel van de organisatorische maatregelen is op dit moment geïmplementeerd. Het programma Implementatie Vernieuwing C2000 en de Landelijke Meldkamer Samenwerking werken momenteel aan verdere de borging van deze maatregelen.

Daarnaast is in opdracht van het Strategisch Meldkamer Beraad een verkenning gestart naar de inrichting van een programma voor de beveiliging van de gehele C2000 keten waarbij ook de gebruikers van randapparatuur en centralisten een plek krijgen. Deze verkenning moet een voorstel opleveren met concrete resultaten en projecten die moeten leiden tot een geheel beveiligde keten voor C2000. Ik verwacht dat deze verkenning het eerste kwartaal van 2022 is afgerond.

Continuïteit meldkamers

Het meldkamerveld werkt samen met mijn ministerie ook aan de nadere invulling en borging van risico- en continuïteitsmanagement ten behoeve van de continuïteit van de meldkamers. Dit sluit aan bij en is in lijn met de in gang gezette ontwikkelingen waarover uw Kamer eerder per brief op 23 september 2021 is geïnformeerd. In aanvulling op deze eerdere brief kan ik u mededelen dat het Strategisch Meldkamer Beraad heeft besloten om de continuïteitsmonitor verder te ontwikkelen en dat informatiebeveiliging integraal onderdeel wordt van deze monitor.

Verantwoordelijkheden informatiebeveiliging

Hierboven heb ik aangegeven welke partijen betrokken zijn in het meldkamerdomein en verantwoordelijkheid dragen voor de informatiebeveiliging van meldkamersystemen. Het netwerk voor het beheer van meldkamers vindt plaats in een uniek multidisciplinair samenwerkingsverband met 52+ partijen in de wereld van noodhulp en crisisbeheersing. Een samenwerkingsverband met zoveel partijen vraagt veel van alle betrokkenen. Met alle partijen is bij de inwerkingtreding van de Wijzigingswet meldkamers per 1 juli 2020 afgesproken dat we de governance voor het beheer van de meldkamers na één jaar evalueren en ervaringen en eventuele lacunes in de borging van verantwoordelijkheden op een rij zetten. Het Wetenschappelijk Onderzoek- en Documentatiecentrum voert op dit moment het onderzoek uit. De aanbevelingen uit dit onderzoek worden meegenomen in het verder vervolmaken van de governance van de meldkamers. Ik verwacht de uitkomsten van de evaluatie medio 2022 en zal ik u infomeren in een volgende voortgangsbrief over ontwikkelingen in het meldkamerdomein.

Tot slot

Ook de komende jaren liggen er belangrijke opgaven voor het verder ontwikkelen van het risicomanagement voor het meldkamerdomein voor zowel informatiebeveiliging als ook continuïteit. Daarbij blijven de veiligheid van burgers en hulpverleners, de ondersteuning van de inzet van de hulpdiensten en de kwaliteit, continuïteit en robuustheid centraal staan.

Via mijn halfjaarlijkse voortgangsbrief over de meldkamers en missiekritische communicatie houd ik u graag op de hoogte van de verschillende ontwikkelingen in het meldkamerdomein en de informatiebeveiliging van meldkamersystemen.

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