

Vergaderjaar 2016–2017

34 550 VII

Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2017

Nr. 50 HERDRUK¹

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 juli 2017

In het verantwoordingsdebat met uw Kamer van 31 mei 2017 (Handelingen II 2016/17, nr. 81, items 3 en 6) heeft de Minister van Financiën toegezegd om ten aanzien van de ministeries van Defensie, Economische Zaken en Volksgezondheid, Welzijn en Sport, specifiek aan te geven hoe het overleg met de Algemene Rekenkamer is verlopen en welk vervolg zij geven aan het oordeel van de Algemene Rekenkamer over de informatiebeveiliging. In deze brief kom ik, mede namens mijn collega-ministers van VWS, EZ en Defensie, die toezegging na.

De president van de Algemene Rekenkamer zei op verantwoordingsdag in uw Kamer (Handelingen II 2016/17, nr. 76, item 3) dat het oplossen van een probleem begint met het te onderkennen. In dit verband zei hij verder: «Helaas blijkt uit de reactie van de ministers van VWS, EZ, maar ook Defensie dat zij zich niet herkenden in de uitkomst van ons onderzoek.»

Ik wil benadrukken dat de betreffende ministers het belang van informatiebeveiliging onderkennen. Ook zijn de ministeries hard aan het werk met de verbetermogelijkheden die de Algemene Rekenkamer heeft aangedragen. De discussie ten aanzien van de uitkomst van het onderzoek betrof verschillende zienswijzen rond dossiervorming op centraal niveau bij departementen waarbij de sturing op informatiebeveiliging volgens een decentraal verantwoordingsmodel is ingericht. Deze werkwijze is in lijn met het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Samen met de Auditdienst Rijk en de Algemene Rekenkamer werk ik nu aan een set met heldere afspraken ten aanzien van de benodigde dossiervorming.

¹ Herdruk i.v.m. correctie in het opschrift

Hieronder wordt voor de drie ministeries aangegeven welke activiteiten zij verrichten om de informatiebeveiliging verder te verbeteren.

Ministerie van VWS

Het Ministerie van VWS is het met de Algemene Rekenkamer eens dat het van groot belang is om het management voor informatiebeveiliging zo ingericht te hebben dat elk onderdeel van het VWS-concern, alsook VWS op centraal niveau, in staat is om gedurende het jaar de actuele stand van de informatiebeveiliging in het concern te beoordelen en (bij) te sturen op (rest)risico's, waar dat noodzakelijk is. Het concernbrede inzicht in systemen en de genomen maatregelen zal in 2017 verder worden verbeterd met de concernbrede implementatie van een informatiemanagementsysteem (*Information Security Management System, ISMS*). Met dit managementsysteem zal VWS de informatiebeveiliging beter kunnen sturen. Daarbij zullen ook de maatregelen voor de door de Algemene Rekenkamer onderzochte bedrijfskritische systemen in 2017 versterkte aandacht krijgen. Via risicosturing wordt de noodzakelijkheid en de volgorde van maatregelen bepaald. Daarnaast neemt VWS naar aanleiding van de resultaten en inzichten uit de Planning&Control cyclus 2016 in 2017 nog een aantal aanvullende maatregelen om de informatiebeveiliging verder te versterken.

Ministerie van EZ

Op verzoek van het Ministerie van EZ heeft de Algemene Rekenkamer op 23 juni jl. een addendum verstrekt waarin de onderbouwing van het oordeel nader is toegelicht. Medio juli vindt hierover overleg plaats tussen EZ, de Algemene Rekenkamer en de Auditdienst Rijk. De actiepunten naar aanleiding van dit addendum worden door EZ opgenomen in het interne informatiebeveiligingsjaarplan van 2017. EZ erkent dat informatiebeveiliging een cruciaal thema is voor de bedrijfsvoering. Het departement werkt eraan om dit thema steviger te verankeren binnen de organisatie. De toenemende digitalisering vraagt dit ook van EZ. De verbeterpunten die zijn beschreven door de Algemene Rekenkamer en de Auditdienst Rijk helpen EZ deze positie van informatiebeveiliging nader te verstevigen en uit te bouwen. Bij EZ zijn de hoofden van dienst zelf verantwoordelijk voor informatiebeveiliging. Maandelijks vindt er overleg plaats tussen het CIO-office en de IB-coördinatoren van de verschillende diensten. Belangrijke signalen naar aanleiding van dit overleg worden door de pSG/CIO nader behandeld met het betreffende hoofd van dienst.

Ministerie van Defensie

De aanbevelingen van de Algemene Rekenkamer spitsen zich bij het Ministerie van Defensie toe op de werking van het managementsysteem waarmee de informatiebeveiliging wordt gestuurd, waaronder ook de dossiervorming bij kritieke systemen. In een gesprek met de Algemene Rekenkamer op 21 juni jl. is de aanpak van Defensie voor het oplossen van de onvolkomenheid besproken. Hierbij zijn geen verschillen van inzicht gebleken. De voortgang van de verbeteringen zal in het najaar wederom met de Algemene Rekenkamer worden besproken.

De CIO Rijk zal in zijn halfjaarlijkse gesprekken met de departementale CIO's aandacht besteden aan de onvolkomenheden en de verbeteringen monitoren die de ministeries in gang zetten.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk