Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 620

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 juli 2019

De Algemene Rekenkamer constateert in haar Verantwoordingsonderzoek 2018[1] een toename in het aantal onvolkomenheden op het gebied van informatiebeveiliging (11) en ICT (9) binnen de rijksoverheid.
Zowel het kabinet als uw Kamer hebben bij het Verantwoordingsdebat op 6 juni jongstleden (Handelingen II 2018/19, nr. 90, items 5 en 12) aangegeven deze situatie zorgelijk te vinden. Uw Kamer heeft mij in dit verband verzocht om nog voor het AO Functioneren Rijksdienst van 3 juli te laten weten hoe het kabinet de geconstateerde problemen gezamenlijk gaat aanpakken. Bij het WGO van 20 juni heb ik u tevens toegezegd om u te informeren over de voorziene doorontwikkeling van het Rijks ICT Dashboard, om ook het inzicht en de bruikbaarheid van de daar beschikbare verantwoordings-informatie structureel te verbeteren. Dat doe ik middels deze brief.

Aanpak onvolkomenheden

Bij de aanpak van de problematiek rond informatiebeveiliging en ICT zet het kabinet noodzakelijke stappen, zowel rijksbreed als binnen de eigen bedrijfsvoering van departementen. In deze brief ga ik in op beide typen maatregelen en hun onderlinge samenhang.
Hierbij staat voorop dat het kabinet de gevoelens van uw Kamer deelt dat de situatie op deze onderwerpen volgend jaar significant beter moet zijn dan het afgelopen jaar. Ik heb daarom met mijn kabinetscollega's, aanvullend op de rijksbrede maatregelen in de Strategische I-agenda 2019–2021[2], gesproken over een gerichte aanpak van de onvolkomenheden op ICT en informatiebeveiliging in 2019.
Elk ministerie heeft de Rekenkamer reeds in een bestuurlijke reactie op het Verantwoordingsonderzoek 2018 laten weten hoe ze die onvolkomenheden binnen de eigen bedrijfsvoering willen aanpakken. Het volledige

[1] Brief Algemene Rekenkamer, Kamerstuk 35 200 VII, nr. 6.
[2] *Kamerstuk* 26 643, nr. 591.

kst-26643-620
ISSN 0921 - 7371
's-Gravenhage 2019

overzicht van maatregelen op deze onvolkomenheden, uitgesplitst per departement, deel ik graag met u als bijlage bij deze brief[3].
Afspraak binnen het kabinet is dat ik de opvolging van deze acties dit jaar en in volgende jaren centraal ga coördineren, waarbij ik uw Kamer zoals toegezegd[4] nog dit najaar van een tussentijdse voortgangsrapportage zal voorzien.
Daarbij zal ik ook ingaan op de voortgang van de rijksbrede maatregelen in de Strategische I-agenda 2019–2021.

Meerjarenstrategie

Deze verdere invulling van mijn coördinerende rol is in lijn met de voornemens die ik in oktober vorig jaar met uw Kamer heb gedeeld. Ik heb u toen, in reactie op de eerdere bevindingen van de Rekenkamer over 2017, een brief gestuurd met de aankondiging van versterkte coördinerende bevoegdheden voor de Minister van BZK en een nieuw pakket aan sturingsmaatregelen voor het I-domein van het Rijk[5].
In februari heb ik uw Kamer tevens de strategische I-agenda 2019–2021 toegestuurd (Kamerstuk 26 643, nr. 591), waarin naast deze nieuwe sturingsmaatregelen ook andere initiatieven in samenhang worden gepresenteerd. Hierbij gaat het bijvoorbeeld om initiatieven zoals de ontwikkeling van een meerjarig samenwerkingsplan tussen ICT-opleiders in het hoger onderwijs en de Rijksdienst, waarbij beoogd wordt nog in 2019 te starten met de uitvoering hiervan.

De uitvoering van deze meerjarenstrategie is in 2019 met grote urgentie gestart. Geprioriteerde sturingsmaatregelen met voorziene oplevering in 2019 zijn onder meer de herziening van het functieprofiel van de departementale CIO's en een kwaliteitskader voor departementale I-plannen.
Zoals ook aangegeven in mijn brief van 11 oktober (Kamerstuk 26 643, nr. 591) leggen deze maatregelen de basis voor de verbetering van de sturing en verantwoording over ICT binnen de Rijksdienst. De verbetering van het Rijks ICT Dashboard, die binnen de planperiode van de Strategische I-agenda 2019–2021 wordt uitgevoerd, moet volgen uit de implementatie van deze maatregelen.

Het Rijks ICT Dashboard is de afgelopen jaren ontwikkeld op basis van de informatiebehoefte van uw Kamer, waarbij de focus ligt op informatievoorziening over grote ICT-vernieuwingsprojecten. De Algemene Rekenkamer merkt in dit verband terecht op dat op het Rijks ICT Dashboard nu nog geen verantwoordingsinformatie beschikbaar is over ICT-beheeraspecten[6].
Met voorgenoemde sturingsmaatregelen wordt de aansluiting van de departementale informatieplanning op de begrotings- en beleidscyclus verbeterd en fungeert de CIO voortaan als eigenaar van het departementale I-plan. De CIO krijgt daarmee een concrete bevoegdheid, verantwoordelijkheid en een verbeterde informatiepositie in de hele levenscyclus van ICT; inclusief ICT-beheeraspecten.
Om de kosten die hiermee samenhangen beter in beeld te krijgen is in 2019 ook een pilot gestart die zich richt op beheeractiviteiten met een meerjarig ICT-component van ten minste € 5 miljoen.
Gekeken wordt naar modernisering, doorontwikkeling, onderhoud (preventief en correctief) en jaaraanpassingen van de bestaande ICT-systemen. De uitkomsten van deze pilot zijn relevant om te komen tot een uitgebreidere informatievoorziening op het Rijks ICT Dashboard.

---

[3] Raadpleegbaar via www.tweedekamer.nl.
[4] *Handelingen II* 2018/19, nr. 90, items 5 en 12.
[5] *Kamerstuk* 26 643, nr. 573.
[6] Brief Algemene Rekenkamer, Kamerstuk 35 200 VII, nr. 6.

Voor een effectieve aanpak van informatiebeveiliging is een belangrijke taak weggelegd voor de departementale Chief Information Security Officers (CISO's). Parallel aan de herziening van het functieprofiel van de CIO wordt het functieprofiel van de departementale CISO's geformaliseerd.
In 2019 wordt gewerkt aan de ontwikkeling van een nieuw informatiebeveiligingsniveau, waarmee actieve weerstand wordt geboden tegen digitale dreigingen van statelijke actoren. Tevens is in april de nieuwe Baseline Informatiebeveiliging Overheid gepubliceerd[7], waarvan ik de rijksbrede implementatie binnen de planperiode van de Strategische I-agenda ga faciliteren en coördineren.

Al deze maatregelen hebben tijd nodig voor ontwikkeling en implementatie. Om die reden heeft de Strategische I-agenda ook een meerjarig karakter. Het kabinet zet hiermee de noodzakelijke stappen, maar zoals ook aangegeven bij het Verantwoordingsdebat over 2018, wil ik voorkomen dat het beeld ontstaat dat we hiermee alle problemen rond informatiebeveiliging en ICT volgend jaar hebben opgelost[8]. Daar is deze problematiek te complex en te dynamisch voor. Digitale innovaties en dreigingen veranderen snel en dit vereist continue aandacht.

Extra Rijksbrede maatregelen

In het CIO-beraad zal de voortgang op de aanpak van onvolkomenheden en de voortgang op de Strategische I-agenda continu aandacht krijgen. Hierbij wordt een goede balans gezocht tussen enerzijds monitoring van de voortgang en anderzijds versterking van de uitvoering. Ik heb CIO Rijk daarnaast verzocht om in het licht van de bevindingen van de Algemene Rekenkamer te bezien of en waar aanvullende rijksbrede maatregelen nodig zijn.
Daarbij kijken we onder andere op welke plekken meer acute capaciteit nodig is, waarbij een beroep gedaan kan worden op de pool van ICT-experts van I-interim Rijk. Ook verwacht ik voor de Rijksdienst veel meerwaarde van het nieuwe Cyber Traineeship, waarvan de eerste lichting in september dit jaar start. Die aanvullende expertise geeft een extra stimulans aan het realiseren van voorgenoemde acties.

De Algemene Rekenkamer constateert dat de rijksbrede coördinatie op informatiebeveiliging nog verder kan worden versterkt[9]. Het kabinet vindt dit ook zeer belangrijk en hecht er in dit verband aan dat de rijksbrede samenwerking tussen CISO's centraal wordt gecoördineerd. Ik kan u daarom melden dat ik, in afstemming met mijn kabinetscollega's, in lijn met aanbevelingen van de Algemene Rekenkamer en gelet op de benodigde structurele aandacht voor deze problematiek, besloten heb om de nieuwe rol van Chief Information Security Officer Rijk (CISO Rijk) te creëren. Deze functionaris zal onder directe verantwoordelijkheid van de CIO Rijk zorg dragen voor een integrale borging van informatiebeveiliging binnen het rijksbrede ICT-beleid. De CISO Rijk wordt tevens voorzitter van het reeds bestaande CISO-overleg binnen de Rijksdienst en zal bij de uitvoering van zijn taken nauw samenwerken met de Rijks Beveiligingsambtenaar (Rijks BVA).

---

[7] Stcrt. 2019, nr. 26526.
[8] *Handelingen II* 2018/19, nr. 90, items 5 en 12.
[9] Brief Algemene Rekenkamer, Kamerstuk 35 200 VII, nr. 6.

Eind 2019 ontvangt uw Kamer ten slotte de volgende actualisatie van de Strategische I-agenda 2019–2021 waarin de extra rijksbrede maatregelen worden opgenomen.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren