Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 646

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 oktober 2019

De Rijksdienst staat voor grote uitdagingen op het gebied van digitalisering. In de Strategische I-agenda Rijksdienst 2019–2021[1] heb ik mijn ambities met u gedeeld op onderwerpen als informatiebeveiliging, informatiehuishouding, ICT, kennis en kunde, en sturing op I.

Zoals toegezegd in het Algemeen Overleg Functioneren Rijksdienst op 3 juli 2019 (Kamerstuk 31 490, nr. 257) informeer ik u middels deze brief, mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, over de voortgang van de uitvoering van deze agenda. Ook ga ik in op de door de Algemene Rekenkamer geconstateerde onvolkomenheden en op diverse onderwerpen waar uw Kamer specifiek aandacht voor heeft gevraagd, zoals de beleidsvoornemens rond ICT-aanbestedingen, actuele HR-ontwikkelingen op ICT-gebied en de opvolging van de motie van het lid Özütok van 20 juni jl.[2]

Aanpak onvolkomenheden

In het licht van de door de Algemene Rekenkamer geconstateerde onvolkomenheden op informatiebeveiliging en ICT zijn nieuwe afspraken gemaakt over de coördinatie, waar ik u in mijn brief van 2 juli jl.[3] over heb geïnformeerd. Afspraak binnen het kabinet is dat de situatie op deze onderwerpen volgend jaar significant moet verbeteren en dat alle bewindspersonen zich maximaal zullen inspannen om dit te realiseren. Tevens is afgesproken dat ik de opvolging van deze acties dit jaar en komende jaren centraal ga coördineren. Bij mijn brief van 2 juli jl. ontving u een overzicht van de onvolkomenheden en de acties per departement. De afgelopen maanden zijn er gesprekken gevoerd met de acht departementen waar de onvolkomenheden zijn geconstateerd. In de bijlage vindt

[1] *Kamerstuk* 26 643, nr. 591.
[2] *Kamerstuk* 35 200 VII, nr. 13.
[3] *Kamerstuk* 26 643, nr. 620.

kst-26643-646
ISSN 0921 - 7371
's-Gravenhage 2019

u de afgesproken tussenrapportage over de voortgang van de aanpak van de onvolkomenheden uitgesplitst per departement. In veel gevallen zijn interne procedures op het terrein van informatiebeveiliging bijgesteld en geïmplementeerd. Dit gaat om zaken als risicomanagement, incidentmanagement, autorisatiebeheer en de kwaliteit van de informatiesystemen. Op basis van de gevoerde gesprekken en het bijgesloten overzicht[4] constateer ik dat elk departement voortvarend met de bevindingen en de aanbevelingen van de Algemene Rekenkamer aan de slag is gegaan. Er bestaat echter nog steeds een risico dat de kabinetsdoelstelling niet volledig gehaald wordt, gezien de omvang van deze opgave. Daarom heb ik in september deze stand van zaken met mijn kabinetscollega's besproken in de ministerraad. Daar heb ik het aanbod gedaan om waar nodig extra rijksbrede kennissessies en capaciteit van I-Interim Rijk beschikbaar te stellen. Ik blijf de voortgang nauwgezet monitoren, waarbij ik intensief met de Algemene Rekenkamer afstem.

Informatiebeveiliging

Voor een veilige en goed functionerende overheid is informatiebeveiliging cruciaal en essentieel. Technologische ontwikkelingen en de toename van digitale dreigingen vragen om blijvende aandacht, zoals eerder dit jaar ook benoemd in het Cybersecuritybeeld Nederland 2019[5] en het WRR-rapport Digitale Ontwrichting.[6] Daarom licht ik informatiebeveiliging apart uit in deze brief.

Om de feitelijke veiligheid te verhogen zijn verschillende initiatieven opgenomen in de Strategische I-agenda Rijksdienst. Hieronder ga ik in op de voortgang van een aantal van deze initiatieven. Daarnaast kan ik melden dat ik in reactie op de motie van het lid Özütok (Kamerstuk 35 200 VII, nr. 13) van 20 juni jl. concrete doelstellingen voor de rijksbrede informatiebeveiliging en digitale infrastructuur heb opgenomen in de begroting voor het jaar 2020. [7]

Nationaal Detectie Netwerk (NDN)

Het Nationaal Detectie Netwerk (NDN) helpt om digitale dreigingen te detecteren. Voor een goede informatiebeveiliging binnen de Rijksdienst is het NDN effectiever als meer partijen aansluiten. Om dit te realiseren heeft het Nationaal Cyber Security Centrum (NCSC, onderdeel van het Ministerie van JenV) aanvullende capaciteit ingezet en heb ik extra budget uit de BZK-begroting beschikbaar gesteld voor de implementatie van sensoren. Ik kan u melden dat waar eind vorig jaar nog 52 Rijksorganisaties (inclusief ZBO's) waren aangesloten (dekkingsgraad 29%), nu inmiddels 100 Rijksorganisaties zijn aangesloten (dekkingsgraad van 55%). Ik blijf mij inzetten om meer partijen aan te laten sluiten op het NDN om de digitale dreigingen gezamenlijk het hoofd te bieden.

BBN3

Zoals aangegeven in mijn brief van 2 juli jl. is in 2019 gewerkt aan een nieuw informatiebeveiligingsniveau (BBN3) om betere weerstand te bieden tegen de toegenomen digitale dreigingen. In de Strategische I-agenda Rijksdienst 2019–2021 heb ik aangekondigd dat BBN3 nog dit jaar zal worden opgeleverd. Die planning was gebaseerd op de voortgang die op dat moment werd geboekt met de ontwikkeling van BBN3. Uit

---

[4] Raadpleegbaar via www.tweedekamer.nl.
[5] *Kamerstuk* 26 643, nr. 614.
[6] https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.
[7] *Kamerstuk* 35 300 VII, nr. 2; Hoofdstuk 2, paragraaf «ICT binnen de Rijksdienst».

interdepartementale afstemming blijkt dat deze planning moet worden bijgesteld. Zo is het NAVO-kader, waarop BBN3 wordt gestoeld, nog in ontwikkeling en zijn de uitvoeringsimplicaties nog onvoldoende inzichtelijk.

Het vervolgtraject van BBN3 zal dit najaar interdepartementaal worden besproken. Over de uitkomst hiervan zal ik de Kamer informeren.

Vulnerability scanning

In de Kamerbrief over Sturing op informatiebeveiliging en ICT binnen de Rijksdienst[8] heb ik aangekondigd dat een rijksbrede faciliteit zal worden ontwikkeld voor vulnerability scanning om kwetsbaarheden voor externe dreigingen in systemen geautomatiseerd in kaart te brengen. In dit verband is de afgelopen maanden binnen het Rijk een eerste verkenning uitgevoerd. Op korte termijn inventariseer ik de eisen waaraan een faciliteit zal moeten voldoen om geautomatiseerd zicht te houden op de kwetsbaarheden en breng ik de faciliteiten die reeds beschikbaar zijn binnen de overheid in kaart. Ook zal ik kennisdeling op dit thema tussen departementen stimuleren. Dit moet leiden tot een meer gestandaardiseerde wijze van scanning, monitoring, kennisuitwisseling en aanpak van kwetsbaarheden.

De optie om één rijksbrede faciliteit voor vulnerability scanning te ontwikkelen, aanvullend op de faciliteiten die nu reeds in gebruik zijn binnen de Rijksdienst, houd ik in overweging. Indien onverhoopt zou blijken dat voorgenoemde maatregelen onvoldoende verbetering laten zien of veranderingen in het dreigingsbeeld hier aanleiding toe geven, kan dit een volgende stap zijn.

Informatiehuishouding en openbaarheid

Actieve openbaarmaking van overheidsinformatie is van groot belang voor de controleerbaarheid van de overheid en de herbruikbaarheid van overheidsinformatie door burgers en bedrijven. We staan hier voor grote uitdagingen, zowel wat betreft veranderingen in de ICT als in de werkwijze van ambtenaren. Een solide en toegankelijke informatiehuishouding is een essentiële randvoorwaarde om een snellere, laagdrempeligere en betere toegang voor burgers en bedrijven tot overheidsinformatie mogelijk te maken.

Rijksprogramma Duurzaam Digitale Informatiehuishouding

In januari 2019 is het Meerjarenplan verbetering informatiehuishouding Rijk[9] aan de Tweede Kamer gestuurd, deze wordt op dit moment geactualiseerd voor 2020 en zal ik na oplevering met uw Kamer delen. De Ministeries van BZK en OCW hebben ter ondersteuning van de uitvoering het Rijksprogramma Duurzaam Digitale Informatiehuishouding (RDDI) opgezet. Alle departementen participeren in dit programma en leveren een bijdrage. De departementen richten eigen programma's in voor het verbeteren van de informatiehuishouding, met aandacht voor zowel de opgaven van de eigen organisatie als voor de actielijnen van het Meerjarenplan.

Vijf departementen zijn inmiddels gestart met de implementatie van de nieuwe werkwijze voor e-mailarchivering. Een aantal uitvoeringsorganisaties toetst momenteel of deze werkwijze past bij hun werkprocessen.

---

[8] *Kamerstuk* 26 643, nr. 574.
[9] Zie bijlage bij *Kamerstuk* 35 112, nr. 4.

Verder zijn er vijf pilots op het gebied van actieve openbaarmaking gestart. Het doel is verschillende aspecten van openbaarmaking uit te testen en deze inzichten rijksbreed te delen.

ICT

De intensivering van ICT bij het Rijk heeft ook als gevolg dat we slim moeten omgaan met onze ICT-voorzieningen en -infrastructuur.

In de Strategische I-agenda stond de doelstelling om voor 2020 de oorspronkelijk 64 departementale datacenters af te sluiten en alle apparatuur te hebben overgebracht naar vier overheidsdatacenters (ODC's). Er zijn nu in totaal 50 datacenters gesloten, waarbij geconstateerd moet worden dat enige uitloop in 2020 noodzakelijk is om dit doel te behalen. De doelstelling om, conform de duurzaamheidsagenda, het energieverbruik van de vier ODC's met minimaal 50% terug te brengen is inmiddels wel gerealiseerd.

ICT-inkoop en -aanbesteding

Met de komst van Strategisch Leveranciersmanagement is de rijksbrede sturing op ICT-inkoop en aanbestedingen de afgelopen jaren slimmer georganiseerd. Dit heeft bijgedragen aan een stevigere positie van het Rijk als opdrachtgever, verbeterde kennisopbouw en een gezamenlijk optreden richting grote ICT-leveranciers, waardoor de relatie gelijkwaardiger is geworden. Een recent voorbeeld van de werking van Strategisch Leveranciersmanagement zijn de afspraken die de rijksoverheid met Microsoft heeft gemaakt over aanvullende privacy-waarborgen rond het gebruik van Office 365. Om naleving van deze afspraken te kunnen controleren zijn tevens verbeterde audit-mogelijkheden afgesproken. Hierover is uw Kamer per brief op 1 juli jl.[10] door de Minister van JenV geïnformeerd.

De Staatssecretaris van BZK heeft uw Kamer in het AO van 22 november 2018 over Operatie BRP toegezegd te kijken hoe de opgedane leereffecten m.b.t de aanbestedingsstrategie rijksbreed kunnen worden ingezet. Hij komt hier voor het eind van dit jaar nog bij u op terug. Deze leereffecten zullen worden opgenomen in het rijksbrede «Afwegingskader ICT-opdrachten».

Kennis en kunde

Het Rijk wordt steeds ICT-intensiever. In de I-agenda is daarom het versterken van de ICT-kennis en -kunde binnen het Rijk een belangrijke pijler.

HR ICT

Een onderdeel van de pijler Kennis en kunde is het versterken van de positie van de Rijksdienst als ICT-werkgever. Bij het AO Functioneren Rijksdienst op 3 juli heeft uw Kamer verzocht om nader in te gaan op de actuele ontwikkelingen in dit verband.

Binnen het programma «Versterking HR ICT Rijksdienst 2018–2021» zijn onder meer wervingscampagnes georganiseerd waarmee de rijksoverheid als aantrekkelijke ICT-werkgever duidelijk op de kaart wordt gezet. Van 20 mei tot en met eind juni 2019 is een landelijke rijksbrede ICT-campagne

[10] *Kamerstuk* 26 643, nr. 622.

gevoerd. Tijdens deze campagne is het aantal bezoekers van de website Werken voor Nederland toegenomen met 550%.

Het Rijks I-Traineeship is dit jaar uitgebreid tot een programma met drie verschillende tracks: het breder georiënteerde ICT-track, een data science track en, sinds september dit jaar, een specialistische track voor cybersecurity. Dit jaar zijn er via het Rijks I-Traineeship 75 nieuwe talenten gestart. Van de lichting trainees die het programma in 2019 heeft afgerond, is ruim 90% ingestroomd bij de rijksoverheid.

Dit jaar start tevens een eerste omscholingsklas op het gebied van cybersecurity-management, wat bijdraagt aan het vergroten van de ICT-capaciteit bij het Rijk en meer kennis en kunde op het gebied van cybersecurity.

In mijn brief van 2 juli jl. over externe inhuur van (ICT) personeel bij het Rijk[11] heb ik aangegeven dat in 2019 zal worden gestart met de ontwikkeling en uitvoering van een meerjarig samenwerkingsplan tussen ICT-opleiders in het hoger onderwijs en de Rijksdienst. Dat traject is volgens planning in 2019 gestart en zal volgend jaar met deze partijen in een nieuwe Taskforce nadere invulling krijgen. Doel hierbij is om ICT-kennis en -kunde bij het Rijk in zowel kwantitatief als kwalitatief opzicht een impuls te geven.

RADIO

Het initiatief RADIO (RijksAcademie voor Digitalisering en Informatisering Overheid) bouwt haar curriculum uit om ambtenaren in beleid, uitvoering en toezicht voldoende inzicht te geven in de mogelijkheden en effecten van digitalisering op hun werk. Naast klassikale masterclasses zijn een e-learningserie en een serie webinars over nieuwe technologieën gemaakt om zo meer ambtenaren te bereiken. Daarnaast is verdiepend aanbod ontwikkeld op het gebied van privacy, datagebruik en algoritmen. RADIO zet deze ontwikkeling door met nieuwe thema's en (digitale) onderwijsmethoden.

Sturing op I

In het aangepaste Coördinatiebesluit organisatie, bedrijfsvoering en informatie-systemen rijksdienst[12] is een aantal instrumenten aan mij als Minister van BZK toegekend, uiteraard met inachtneming van het uitgangspunt van de individuele ministeriële verantwoordelijkheid zoals vastgelegd in artikel 44 van de Grondwet.

In artikel 3a van het Coördinatiebesluit is sinds oktober 2018 geregeld dat de benoeming en het ontslag van een Chief Information Officer (CIO) van een ministerie alleen kan plaatsvinden na overleg met de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Op deze manier kan ik mijn coördinerende taak op het gebied van informatievoorziening van de Rijksdienst uitvoeren door advies te geven over onder meer de invulling van vereiste competenties van een CIO. Hier heb ik invulling aan gegeven door actieve betrokkenheid bij de werving en het aanstellen van nieuwe CIO's bij het Ministerie van Defensie en bij mijn eigen ministerie. Daarnaast zit de CIO Rijk inmiddels standaard in de aanstellingscommissie voor nieuwe CIO's.

---

[11] *Kamerstuk* 31 490, nr. 254.
[12] Zie bijlage bij *Kamerstuk* 26 643, nr. 573.

Functieprofielen CIO's en CISO's

De afgelopen periode is in samenwerking met de andere departementen gekeken hoe de CIO-functie binnen departementen versterkt kan worden door de herziening van het CIO-profiel. Daarnaast wordt in samenhang gewerkt aan de formalisering van het profiel van de CISO (Chief Information Security Officer). Uitgangspunt hierbij is dat door dit functieprofiel meer te standaardiseren, de sturing op informatiebeveiliging binnen de Rijksdienst strakker wordt georganiseerd. Deze profielen worden bezien in samenhang met de opvolging van aanbevelingen uit het (nog te verschijnen) onderzoek t.b.v. motie van het lid Middendorp, over nut en noodzaak van een Rijksinspectie Digitalisering.[13]

In mijn brief van 2 juli jl. heb ik u tevens geïnformeerd over mijn voornemen om een CISO Rijk aan te stellen, die zorg moet dragen voor een integrale borging van informatiebeveiligingsbeleid binnen het rijksbrede ICT-beleid. Ik kan u melden dat de vacaturetekst voor deze functie momenteel wordt opgesteld.

Kwaliteitskader departementale I-plannen

In 2019 is gewerkt aan een kwaliteitskader voor departementale I-plannen, dat moet bijdragen aan een betere meerjarige strategische sturing op I binnen departementen. Dit kwaliteitskader is inmiddels in concept gereed en zal de komende periode interdepartementaal worden afgestemd. Ik verwacht dat het kwaliteitskader gelijktijdig met de functieprofielen van CIO's en CISO's kan worden vastgesteld.

Rijks ICT-dashboard

Zoals aangegeven bij het Verantwoordingsdebat eerder dit jaar en in mijn brief van 2 juli jl. ben ik van plan om de bruikbaarheid van het Rijks ICT-dashboard in de komende jaren stapsgewijs te verbeteren. Nog voor Verantwoordingsdag 2020 wil ik in dit verband een eerste, zichtbare stap zetten, door de inzichtelijkheid van de informatie die reeds op het Rijks ICT-dashboard aanwezig is te verbeteren. Daarbij kijk ik onder meer naar een betere visuele presentatie van rijksbrede informatie en trendgegevens. In lijn met de Jaarrapportage Bedrijfsvoering Rijk leg ik de focus op inzichtelijkheid van doorlooptijd en kosten.

Een bredere doorontwikkeling van het Rijks ICT-dashboard wordt in 2020 gestart, waarbij ik ten behoeve van gebruikerswensen ook uw Kamer zal consulteren.

Tot slot

Op diverse dossiers ligt nog een behoorlijke opgave. Zoals ik u eerder liet weten hebben de diverse maatregelen uit de Strategische I-agenda Rijksdienst tijd nodig voor de ontwikkeling en volledige invoering. Daarom heeft deze agenda ook een meerjarig karakter. Begin 2020 stuur ik u de volgende update van de Strategische I-agenda Rijksdienst waarin ik ook op de overige thema's inga.

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

---

[13] *Kamerstuk* 35 000 VII, nr. 34.