

Vergaderjaar 2021–2022

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 813

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 januari 2022

Met deze brief informeer ik uw Kamer voor een laatste maal over de voortgang van de maatregelen uit de Strategische I-agenda voor de Rijksdienst 2019–2021. De opvolging van de (oude) I-agenda is met een meerjarig perspectief vorm gegeven in de (nieuwe) I-strategie Rijk 2021–2025¹ die op 6 september 2021 met uw Kamer gedeeld is. Daarnaast ga ik ook in op enkele moties en toezeggingen in dit domein.

De Strategische I-agenda is onderverdeeld in vijf paragrafen, langs welke structuur deze rapportage is opgezet:

- Informatiebeveiliging en privacy
- Informatiehuishouding en data
- ICT
- Kennis en kunde
- Versterken van het CIO-stelsel

Informatiebeveiliging en privacy

Informatiebeveiliging

In het kader van de Strategische I-agenda zijn de afgelopen kabinetsperiode meerdere stappen gezet op het gebied van informatiebeveiliging. Zo startte in november 2020 de eerste Chief Information Security Officer (CISO) Rijk. Het Besluit CIO-stelsel Rijksdienst dat op 1 januari 2021 in werking trad, heeft ook bij de ministeries geleid tot meer aandacht voor en verbeteringen in de sturing op informatiebeveiliging. In samenwerking met de departementale CISO's is een Standard Operating Procedure opgesteld die de werkwijze beschrijft bij opvolging van dringende beveiligingsadviezen. Hierin staan de wegingscriteria voor een interdepartementale uitvraag en is de informatie beschreven die de CISO Rijk nodig heeft om een rijksbreed beeld op te stellen.

¹ Kamerstuk 26 643, nr.779

Vanuit de directie CIO Rijk is de afgelopen periode in samenwerking met een groep experts binnen de rijksoverheid en de ministeries een handreiking opgesteld en gecommuniceerd voor het inrichten van een doorlopende kwetsbaarheidsscans bij rijksoverheidsorganisaties, waarbij software beschikbaar is gesteld om organisaties hierbij te helpen. Ook is het aantal organisaties dat is aangesloten op het Nationaal Detectienetwerk (NDN) gestegen tot 85% van de rijksdienst. In samenwerking met CIO Rijk ontwikkelt het NCSC het NDN verder zodat steeds meer netwerken binnen de rijksdienst worden gemonitord op digitale aanvallen.

Om ervoor te zorgen dat ambtenaren intuïtiever zorgvuldig met gevoelige informatie omgaan is de «*Gedragsregeling voor de digitale werkomgeving*» vernieuwd. De gedragsregeling is in het najaar verspreid onder de werknemers van de rijksdienst.

Tijdens het debat Online veiligheid en cybersecurity op 1 december 2021 (Kamerstuk 26 643, nr. 807) vroeg PVV-kamerlid Van Weerdenburg of Rijksambtenaren op hun apparaten programma's mogen sideloaden – dat wil zeggen downloaden buiten de officiële appstore van de fabrikant van het apparaat om. De werkomgeving van medewerkers bij de rijksoverheid is afgeschermd en zelf installeren van programma's door gebruikers binnen die omgeving is niet toegestaan en niet mogelijk. Op apparatuur zoals mobiele telefoons en tablets zijn buiten de werkomgeving meer mogelijkheden. Afspraken over het juiste gebruik hiervan zijn opgenomen in de Rijksbrede Gedragsregeling voor de digitale werkomgeving en de gebruikersovereenkomsten bij ingebruikname van mobiele apparatuur. De CISO Rijk onderzoekt met de departementale CISO's de behoefte aan aanvullend beleid op dit gebied en mogelijkheden om dit technisch uit te voeren.

Uw Kamer heeft mij via de motie van de leden Özütoğ en Paternotte² gevraagd om u te informeren over de borging van de Nationale Cryptostrategie. De besturing van de Nationale Cryptostrategie loopt via een interdepartementale stuurgroep, waardoor het een breed gedragen initiatief is. De samenwerking tussen meerdere ministeries heeft geleid tot afspraken over de financiering van de Nationale Cryptostrategie voor de komende periode. Meerjarige financiering behoeft een besluit van het volgende kabinet.

In het kader van monitoring heeft de Auditdienst Rijk inmiddels voor de vierde keer onderzoek gedaan naar de sturing en beheersing van informatiebeveiliging op centraal departementaal niveau. Daaruit is op te maken dat er een lichte groei in volwassenheid is te zien.

Uitfasering Kaspersky

Graag informeer ik uw Kamer over de stand van zaken ten aanzien van de uitfasering van de antivirussoftware van Kaspersky bij de rijksoverheid. In mijn brief van 23 maart 2020³ heb ik uw Kamer bericht dat alle ministeries gemeld hebben dat de betreffende software bij geen van de onder die ministeries ressorterende dienstonderdelen (meer) in gebruik is.

In diezelfde brief kondigde ik aan dat ik zou onderzoeken of het risico van gebruik van deze software door externe ICT-leveranciers ondervangen kan worden binnen de bestaande ICT-inkoopvoorwaarden. Een interdepartementaal team heeft in de tussentijd onderzocht of de risico's die door gebruik van Kaspersky antivirussoftware worden geïntroduceerd nog

² Kamerstuk 35 570 VII, nr.13

³ Kamerstukken 30 821 en 26 643, nr. 109

steeds bestaan na het doorvoeren van een aantal aanpassingen door het bedrijf. De conclusie van dat onderzoek is dat er geen aanleiding is om de genomen maatregelen te herzien en dat Kaspersky antivirussoftware daarom bij de rijksoverheid buiten gebruik blijft.

Het onderzoek naar risico's bij gebruik van deze software door externe ICT-leveranciers gaat hierna plaatsvinden en ik zal uw Kamer over de resultaten informeren zodra deze bekend zijn.

Privacy

Om ervoor te zorgen dat de privacy van rijksbrede bedrijfsvoeringstrajecten wordt gewaarborgd is een vernieuwde procedure vastgesteld. Hiermee worden de privacyrisico's en benodigde maatregelen in afstemming met de Functionaris Gegevensbescherming (FG) van alle ministeries vastgelegd en daarna ter goedkeuring en instemming aan de interdepartementale overleggen en de Groepsondernemingsraad Rijk aangeboden.

Eén van de onderdelen in de nieuwe procedure is het opstellen van een rijksbreed privacy advies (de PAR-procedure) bij een rijksbrede ontwikkeling. Het afgelopen jaar leidde dat al tot zo'n 30 adviezen. Tenslotte zijn, als onderdeel van de nieuwe procedure, ook het Rijksmodel Privacy Impact Assessment (PIA) en de hieraan gerelateerde modelverwerkersovereenkomst geactualiseerd.

Informatiehuishouding en data

Archiveren, veiligstellen van informatie

In het meerjarenplan van het Rijksprogramma voor Duurzame Digitale Informatievoorziening (RDDI)] was toegezegd⁴ de openbare overheidswebsites van rijksoverheden, inclusief hun zelfstandige bestuursorganen (de zbo's), en van de Hoge Colleges van Staat te archiveren in 2021. De implementatie verloopt volgens schema, de eerste organisaties zijn nu in de afrondende fase.

Ook is toegezegd te zorgen voor een oplossing om e-mails veilig te stellen. Bij het merendeel van de ministeries is het veiligstellen van e-mailberichten binnen de e-mail exchange omgeving inmiddels ingericht. Voor het automatisch archiveren van e-mailberichten volgens de richtlijn is nu nog geen volledig technische oplossing beschikbaar. Er zijn op dit moment vier potentiële technische oplossingen voorhanden die dit jaar verder uitgewerkt en getest worden.

Voor het veiligstellen van berichtenapps heeft een meerderheid van de ministeries procedures en afspraken vastgelegd. Uit een praktijkproef met het geautomatiseerd opslaan van berichtenapps blijkt dat er (nog) geen voldoende bevredigende rijksbreed toe te passen oplossing is. Hier wordt voortvarend aan gewerkt, waarbij de ingezette acties doorlopen in 2022.

Met de aankomende kabinetswissel in het verschiet wordt door alle ministeries samengewerkt aan de pilot «veiligstellen sociale media bewindslieden Rutte III». Dit traject is gericht op het veiligstellen en archiveren van berichten op sociale media. Het doel is driedelig: service aan de ministeries in het kader van veiligstellen sociale media bewindslieden (eenmalig), praktijkkennis opdoen en het ontwikkelen van een rijksbrede manier van werken voor volgende kabinetten. Ik verwacht voor

⁴ Het Meerjarenplan RDDI (6 juni 2018) was een bijlage bij de brief van de Minister van BZK d.d. 3 januari 2019 over de Woo (Kamerstuk 35 112, nr. 4)

het aantreden van het nieuwe kabinet de laatste social mediaberichten van de huidige bewindspersonen veilig te hebben gesteld.

Data en artificiële intelligentie (AI)

Afgelopen jaren is zowel vanuit de Strategische I-agenda 2019–2021⁵, als vanuit de Data Agenda Overheid⁶ – als onderdeel van de Nederlandse Digitaliseringsstrategie – gewerkt aan de vraag hoe data en AI op een bewuste wijze kunnen bijdragen aan het verbeteren en efficiënter inrichten van datagedreven beleid binnen de rijksoverheid⁷. Daarbij is in kaart gebracht welke data initiatieven er lopen⁸. Zo is er een toolbox datagedreven werken ontwikkeld⁹, waarin bijvoorbeeld ook een white paper over datavirtualisatie¹⁰ is opgenomen. Op deze manier wordt actief kennis gedeeld.¹¹

Daarnaast is onder meer onderzoek gedaan naar de opkomende rol van een Chief Data Officer (CDO) en de manier waarop deze functie binnen het CIO-stelsel kan worden geborgd¹². Incidenten met gegevensbestanden, maar ook nieuwe wetgeving zoals de Wet Open Overheid, de nieuwe Archiefwet en Europese wet- en regelgeving, vereisen dat de informatiehuishouding een steviger verankering krijgt binnen het CIO-stelsel. Daarom is in de nieuwe I-strategie Rijk 2021–2025 afgesproken om de rol van de Chief Data Officer te formaliseren.

Op basis van het adviesrapport van de Algemene Bestuursdienst «Tussen droom en data ...; verkenning ecosysteem voor een data gedreven overheid»¹³ is een interbestuurlijke aanpak ontwikkeld om vervolgstappen te zetten in het ontwikkelen van datagedreven werken aan maatschappelijke opgaven. Uw Kamer heeft deze «Interbestuurlijke Datastrategie Nederland» op 18 november jl. ontvangen.

Terecht constateerde de Algemene Rekenkamer begin 2021 dat er in een digitaliserende overheid meer aandacht voor algoritmen moet zijn¹⁴. Daarom heb ik, samen met de Staatssecretaris van Economische Zaken en Klimaat en de Minister voor Rechtsbescherming, uw Kamer afgelopen zomer de beleidsagenda van dit kabinet gepresenteerd op het thema AI en algoritmen¹⁵.

Ik heb daarnaast de Auditdienst Rijk verzocht om rijksbreed de geleerde lessen op te halen uit algoritme-inzet. Dit onderzoek wordt naar verwachting begin 2022 afgerond en zal helpen bij het prioriteren van de te nemen maatregelen¹⁶.

Vooruitlopend op deze maatregelen heb ik een initiatief gefinancierd van een consortium van twaalf overheidsorganisaties die al zijn begonnen met de invoering van maatregelen om publieke controle op algoritmen te

⁵ Kamerstuk 26 643, nr. 591

⁶ Kamerstuk 26 643, nr. 675

⁷ Kamerstuk 26 643, nr. 713

⁸ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/het-led/overzicht-data-initiatieven/>

⁹ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/het-led/toolbox/>

¹⁰ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/het-led/toolbox/de-juiste-methode-voor-het-juiste-doel/>

¹¹ Kamerstuk 26 643, nr. 797

¹² <https://www.digitaleoverheid.nl/led-nieuws/chief-data-officer-cdo-aanjager-van-de-datagedreven-organisatie/>

¹³ <https://www.algemenebestuursdienst.nl/documenten/publicatie/2020/12/21/tussen-droom-en-data>

¹⁴ Kamerstuk 26 643, nr. 737

¹⁵ Kamerstuk 26 643, nr. 765

¹⁶ Kamerstuk 26 643, nr. 713

versterken¹⁷. De resultaten van deze pilot zullen worden gebruikt om het toezicht op algoritmen binnen de rijksoverheid verder vorm te geven.

ICT

Cloudbeleid en Gaia-X

De concretisering van de uitkomsten van de verkenning van het cloudbeleid van de rijksdienst is zo goed als afgerond. Ik verwacht dat het cloudbeleid begin 2022 wordt vastgesteld waarna ik u direct zal informeren.

Via de motie Middendorp¹⁸ heeft uw Kamer mij verzocht u te informeren hoe bestaande kennis en kunde bij kunnen dragen aan het ontwikkelen van rijksbrede overheidsclouddiensten en -datadiensten en de versterking van de Nederlandse positie in het Gaia-X project. In relatie tot eventuele deelname aan het Gaia-X project wordt onderzocht of, met het recent toetreden van een groot aantal leveranciers – waaronder Microsoft, Google, Amazon en Huawei – aan de behoefte aan «digitale soevereiniteit» van de Nederlandse overheid voldoende inhoud kan worden gegeven. Voor samenwerking op het gebied van kennis, kunde en infrastructuur rond clouddiensten is de ontwikkeling van een rijksbrede strategie essentieel. Voor de komende periode is inmiddels een koers uitgezet via een van de thema's van de nieuwe I-strategie Rijk: bestendigen ICT-landschap.

Hybride werken (kantoor en thuis)

Er zijn zowel op de (digitale) werkplek als in de rijkskantoren voorzieningen getroffen om hybride werken mogelijk te maken. Hierbij gaat het om videovergaderen en andere middelen die het samenwerken op afstand makkelijker maken. Voor rijksbreed videovergaderen is een verwerkersovereenkomst afgesloten. Ook is er een stappenplan waarmee de functionaliteiten in de loop der tijd aangevuld worden. Recent is de *secure chat* aan het productaanbod toegevoegd. Voor de uitbreiding van Single Sign On (voor het versneld thuiswerken) met toegang tot clouddiensten had ik toegezegd om zorgvuldigheid toe te passen voor noodzakelijke beveiligingseisen. In samenwerking met dienstenaanbieders en specialisten worden implementatiemogelijkheden verder uitgewerkt.

Interoperabiliteitskaders Digitale Werkomgevingen & Rijkskantoren (IDWOR)

Het doel van het programma IDWOR is de samenwerking in rijkskantoren en tussen dienstverleners te verbeteren. Dat gebeurt door het realiseren van beleidskaders die ervoor zorgen dat rijksmedewerkers tijd-, plaats- en apparaatafhankelijk kunnen werken en dat ze kunnen samenwerken met alle rijksmedewerkers ongeacht de ICT-dienstverlener. Aanvullend wordt gewerkt aan een rijksbrede producten- en dienstencatalogus, een rijks-PDC, voor gebouwgebonden ICT-diensten. Dat wil zeggen, een gestandaardiseerde definitie van de diensten en dienstverleningsniveaus die ministeries in elk rijkskantoor kunnen verwachten. Deze rijks-PDC bevat zowel diensten die in alle rijkskantoren aanwezig moeten zijn (basisdiensten), als optionele diensten die op verzoek van de gebruikers geleverd kunnen worden (plusediensten). In het najaar van 2021 is gestart met een ingrijpende herziening van de rijks-PDC waarin onder andere de invloed van hybride werken wordt meegenomen.

¹⁷ <https://publiekecontrole.com>

¹⁸ Kamerstuk 35 570 VII, nr. 11

Kennis en kunde

Voor een goed werkende digitale rijksoverheid, zijn voldoende ICT-kennis en -kunde een randvoorwaarde. De overheid digitaliseert steeds sneller en de gevolgen van de coronacrisis hebben deze beweging verder versterkt. Ook buiten de overheid is deze ontwikkeling te zien en de verwachting is dat het aantal ICT-banen met 6% toeneemt¹⁹. Het programma Versterking HR ICT Rijksdienst zet in op het aanpakken van het tekort aan I-kennis met diverse rijksbrede initiatieven.

- Zo trekken het Rijk en het Hoger Onderwijs met elkaar op binnen het rijksbrede samenwerkingsverband I-Partnerschap op het gebied van ICT-onderzoek en onderwijs. Sinds de start in 2020 zijn op deze manier meer dan honderd samenwerkingsopdrachten afgerond of in uitvoering en zijn nog eens bijna honderd opdrachten in voorbereiding. Niet alleen wordt op deze manier kennis van buiten naar binnen gebracht, ook wordt de instroom van jong ICT-talent vanuit het Hoger Onderwijs gestimuleerd.
- In september 2021 is de zesde lichting van het I-Traineeship van de rijksoverheid van start gegaan met zo'n 70 beginnende talenten op het gebied van ICT, data en cyber.
- Verder is, om het inzicht te verbeteren in de in-, door-, en uitstroom van ICT'ers bij het Rijk, in het voorjaar van 2021 besloten het Kwaliteitsraamwerk Informatievoorziening (KWIV) rijksbreed te implementeren. Het KWIV vult het Functiegebouw Rijk aan en richt zich op competenties en kwaliteit van IV-personeel bij de rijksoverheid.
- Voor de ontwikkeling van ICT-ers binnen de rijksoverheid is een pilot opgezet waarin leerpaden worden ontwikkeld voor verschillende ICT-expertises.
- De Rijksacademie voor Digitalisering en Informatisering (RADIO) heeft het afgelopen jaar de omslag gemaakt naar vraaggericht werken. De (digitale) opleidingen en leermiddelen, zoals podcasts en e-learnings, sluiten naadloos aan bij de dagelijkse praktijk van rijksorganisaties. Leren van elkaar en met elkaar is daarbij het uitgangspunt. Daarnaast is sterker ingezet op het aanleren van digitale vaardigheden van ambtenaren. Dit slaat goed aan en heeft geleid tot een verviervoudiging van het aantal opdrachten, waaronder een opleidingsverzoek voor de bestuurders bij de Rechtspraak.
- Verder is afgelopen zomer de intensieve IT-cursus voor de topmanagement groep (TMG) van de Algemene Bestuursdienst gestart.

Versterken van het CIO-stelsel

Besluit CIO-stelsel Rijksdienst 2021

In de beleidsreactie onderzoeken «IV-Governance Rijk en Besluit toekomst BIT»²⁰ heb ik uw Kamer toegezegd het CIO-stelsel de komende jaren te versterken. Het Besluit CIO-stelsel Rijksdienst 2021 dat hiervoor in de maak was, is in het kalenderjaar 2021 in werking getreden²¹ en de implementatie is inmiddels van start gegaan. Ministeries weten elkaar steeds beter te vinden en leren van elkaars organisatie van CIO's en CISO's en de daarbij behorende taken. Het doel is om over drie jaar alle onderdelen van het Besluit CIO-stelsel te hebben geïmplementeerd. Daarbij wordt – in lijn met het besluit – rekening gehouden met departementale verschillen en rechtspositionele uitgangspunten.

¹⁹ Arbeidsmarktprognose UWV

²⁰ Kamerstuk 26 643, nr. 656

²¹ Besluit CIO-stelsel Rijksdienst 2021, stcrt. 2020, nr. 62488

Kwaliteitskader Meerjarige Departementale IV-plannen

Het Kwaliteitskader Meerjarige Departementale IV-plannen geeft ministeries een kader om beter zicht te krijgen op de consequenties van beleid voor het gehele bestaande ICT- en gegevenslandschap. In 2021 is het kwaliteitskader vastgesteld. Daarbij zijn de afgelopen maanden benut als aanloopperiode, waarin de ministeries proefversies van de informatieplannen opgesteld hebben. Het kwaliteitskader is op 1 januari 2022 in werking getreden.

Doorontwikkeling Rijks ICT-dashboard

Op het Rijks ICT-dashboard staan alle projecten van de rijksoverheid met een ICT-component van tenminste € 5 miljoen over de hele looptijd van het project. Het dashboard wordt stapsgewijs doorontwikkeld. De toezegging dat de kosten voor ICT-beheer en onderhoud worden opgenomen op het dashboard van 2021 heb ik bevestigd tijdens het Verantwoordingsdebat 2020. Dit dashboard wordt voor Verantwoordingsdag 2022 bijgewerkt. In 2022 wordt het in 2021 ontwikkelde prototype voor het «dashboard van de toekomst» stapsgewijs verder ontwikkeld.

Adviescollege ICT-toetsing

De voorbereiding van het Wetsvoorstel Adviescollege ICT-toetsing zijn op een haar na klaar. De internetconsultatie van het wetsvoorstel is afgerond. Voor de voorlaatste fase is overeenstemming tussen de ministeries vereist, dat iets meer tijd kostte dan ik bij de planning vermoedde. Ik meldde uw Kamer toen ernaar te streven het wetsvoorstel eind 2021 bij uw Kamer in te kunnen dienen²². Ik verwacht dit nu medio maart 2022 te kunnen doen.

Onvolkomenheden ICT

Zoals gebruikelijk²³ informeer ik uw Kamer periodiek over de rijksbrede status van de door de Algemene Rekenkamer geconstateerde onvolkomenheden op ICT en informatiebeveiliging. Monitoring van de opvolging van de ernstige onvolkomenheid van het Ministerie van Buitenlandse Zaken heeft plaatsgevonden op basis van periodiek ontvangen rapportages. Na afschaling van de ernstige onvolkomenheid tot onvolkomenheid in het Verantwoordingsonderzoek 2020 is de opvolging bewaakt in het reguliere monitoringproces. Met alle ministeries ben ik in gesprek over de geconstateerde problematiek en de ingezette verbetertrajecten. Ik zie dat voortgang wordt gemaakt en dat iedereen aandacht heeft voor het oplossen van deze onvolkomenheden. Waar mogelijk wordt vanuit mijn ministerie een bijdrage geleverd qua kennis, kunde en capaciteit om te helpen dit te realiseren. Bijgesloten bied ik uw Kamer een overzicht van maatregelen en stand van zaken op deze onvolkomenheden, uitgesplitst per ministerie²⁴.

Tenslotte

Afgelopen september heb ik u de I-strategie Rijk 2021–2025 gestuurd als opvolger van de Strategische I-agenda 2019–2021. Om die reden

²² Kamerstuk 26 643, nr. 734, p. 20

²³ Handelingen II 2019/20, nr. 74, item 23

²⁴ Raadpleegbaar via www.tweedekamer.nl

informeer ik u hierbij voor de laatste keer over de voortgang op de «oude» I-agenda.

Voor een analyse van de uitgevoerde maatregelen en ingezette verbeteringen in de gehele looptijd van de agenda zal ik opdracht geven tot het uitvoeren van een externe evaluatie. Zodra deze evaluatie gereed is, zal deze met uw Kamer gedeeld worden. Ook zal de evaluatie benut worden bij de verdere activiteiten van de I-strategie Rijk 2021–2025.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops