Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1225

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Den Haag, 16 oktober 2024

Evaluatie Rijksbreed Cloudbeleid

Zoals aangekondigd in de Kamerbrief Rijksbreed Cloudbeleid 2022 (hierna «cloudbeleid») is er een jaar na vaststelling gestart met evaluaties van dit cloudbeleid. Bijgaand treft u de evaluatie van CIO Rijk aan. De evaluaties hebben nu, na een korte implementatieperiode geleid tot rapportage van de ADR en een evaluatie van CIO Rijk. In de evaluatie is ook het «Implementatiekader risicoafweging cloudgebruik» (hierna «implementatiekader») meegenomen.

Voor deze evaluatie is ook gebruikgemaakt van de informatie die de departementen gedeeld hebben met de Algemene Rekenkamer (ARK) en de Auditdienst Rijk (ADR) in het kader van hun cloud onderzoeken, informatie uit de informatiebeveiligingsrapportages van de departementen, de zogenaamde IB-beelden, en informatie uit de monitoringsgesprekken met de departementale Chief Information Security Officers (CISO's). De rapportage van het onderzoek dat de ADR op verzoek van mij heeft uitgevoerd is als bijlage toegevoegd.

Samenvatting

Na twee jaar is de essentie van het Rijksbrede Cloudbeleid nog steeds valide. Er is een aantal onderwerpen waaraan bij de herziening aandacht geven zal worden. Deze punten zullen nader worden uitgewerkt in een rapportage aan uw Kamer in Q4 waarin zowel resultaten van het onderzoek van CIO Rijk, de ARK en de ADR zullen worden meegenomen. De hoofdlijnen van de inzichten zijn:

- *Marktconcentratie*
  Er is sprake van marktconcentratie bij enkele (Amerikaanse) cloudproviders. Deze marktconcentratie brengt aanvullende strategische risico's met zich mee. Door de concentratie van informatie bij enkele aanbieders is er een verhoogde dreiging op inbreuken. Dit risico zou in samenhang beoordeeld moeten worden.

kst-26643-1225
ISSN 0921 - 7371
's-Gravenhage 2024

- *Digitale soevereiniteit, exit strategie en continuïteit*
  Digitale soevereiniteit is van belang als afweging voor het gebruikmaken van cloudvoorzieningen. Dit start bij het sourcingsbesluit over nut en noodzaak, het cloudbeleid begint na de strategische keuze voor ondersteuning door een clouddienst. Dit heeft ook een relatie met de exitstrategie en het borgen van continuïteit. Daarnaast werkt iedereen zelf aan exitstrategieën en is er behoefte aan een rijksbrede best-practices en beleid op deze gebieden.
- *AI en algoritmes en andere nieuwe technologieën*
  Steeds vaker worden in de public clouddiensten gebruikgemaakt van AI. Het gebruik van AI en geeft ook een hogere vraag naar clouddiensten. Met betrekking tot gebruik van AI moet rekening worden gehouden met het kabinetsstandpunt waarover u in een Kamerbrief bent geïnformeerd.[1] Dit geldt ook voor andere nieuwe technologieën zoals kwantum computing waarvoor wordt voorzien dat dit voornamelijk als clouddienstverlening op de markt zal komen.
- *Volledige implementatie cloudbeleid*
  Het cloudbeleid is nog niet overal binnen de Rijksoverheid in alle details geïmplementeerd. Dit heeft specifiek betrekking op:
  - *Departementaal beleid en strategie*
    De rijksorganisaties hebben stappen gezet om het rijksbeleid te adopteren in eigen cloudbeleid, maar dit heeft niet in alle organisaties geleid tot een formeel beleid. In het Rijksbreed cloudbeleid is hiervoor geen implementatietermijn opgenomen.
  - *Advisering basisregistraties*
    De meeste basisregistraties vallen onder ZBO's en daarmee buiten de reikwijdte van het cloudbeleid. Hiermee vervallen de verplichtingen uit het cloudbeleid waaronder het voorafgaand advies. Dit is een aandachtspunt vanwege het grote belang van basisregistraties.
- *Rapportage en registratie*
  Rapportage over cloudgebruik via het Informatiebeveiligingsbeeld blijft nog achter als dit wordt vergeleken met de opgave aan de ARK. Ook ontbreekt een overzicht of in een SAAS-dienst gebruik wordt gemaakt van bijvoorbeeld een hyperscaler.
  Ook is aangegeven dat nog niet duidelijk hoe een Shared Service Organisatie (SSO) zou moeten rapporteren naar haar afnemers. De afnemende partijen zijn hierdoor niet volledig in staat een integraal risicobeeld te maken.
- *Inkoopvoorwaarden en resellers*
  SLM Rijk heeft voor diverse hyperscalers aangescherpte voorwaarden afgesproken. Cloudgebruik gaat vaak via resellers of SAAS-diensten en de registratie laat daardoor niet altijd zien dat er achterliggend gebruik wordt gemaakt van een hyperscaler.
  De contractafspraken die rijksbreed zijn opgesteld tussen de grote dienstverleners en het rijk worden door SAAS-leveranciers of resellers mogelijk niet overgenomen waardoor de in de standaard voorwaarden opgenomen risico mitigerende maatregelen niet van toepassing zijn.
- *Inhoud, effectiviteit en efficiënte risicoweging*
  De effectiviteit en efficiëntie van de risicoweging kan beter. Zo kan er bijvoorbeeld overlap ontstaan tussen de risicoanalyse en de DPIA. Elke organisatie moet zijn eigen risicoafweging maken, er is echter behoefte om rijksbrede afspraken te maken over deze processen en best practices of uitgevoerde analyses te delen. Daarnaast is aangegeven dat de verplichting tot het opnemen van de C2000-criteria onvoldoende expliciet is waardoor die niet altijd worden voorgelegd aan het management.

[1] Kamerbrief over voorlopig standpunt voor Rijksorganisaties bij het gebruik van generatieve AI | Kamerstuk | Rijksoverheid.nl

- *Inhoud en doelgroep cloudbeleid en -strategie*
  Er zijn geen afspraken gemaakt over de inhoud van het departementale cloudbeleid en -strategie zoals bijvoorbeeld aandacht voor samenwerkingsverbanden en ketenregie. Dit heeft aandachtspunten met betrekking tot efficiëntie, hergebruik en vergelijkbaarheid. Daarnaast is de vraag gesteld of en zo ja voor welke onderdelen van departement een eigen cloudbeleid en -strategie ook wenselijk zijn.
- *Verhelderen termen en begrippen*
  Van diverse begrippen en artikelen wordt aangegeven dat die verheldering nodig hebben. Dit heeft onder meer betrekking op de definitie van materialiteit, de situaties en voorwaarden van artikel 10 en 11, de voorbeelden van wet- en regelgeving, de wijze en inhoud van de openbaarmaking, verwijzingen vanuit het cloudbeleid naar het implementatiekader en de handreiking en een consistente documentatieset.

Vervolgstappen Cloudbeleid

Aan de hand van de hier beschreven aandachtspunten en de geplande rapportage van de Rekenkamer, zullen voor het eind van 2024 in rijksbrede samenwerking herzieningsvoorstellen worden opgesteld voor het Rijksbreed Cloudbeleid en het bijbehorende Implementatiekader. Zodat in de eerste helft van 2025 het hernieuwd rijksbrede cloudbeleid kan worden vastgesteld.

Hiernaast zal er gestart worden met het proces om samen met de medeoverheden te komen tot een nieuw cloudbeleid met het uitgangspunt dat dit zal gelden voor de gehele overheid.

Ten tijde van schrijven van deze evaluatie is tevens de initiatiefnota «Wolken aan de horizon» gepubliceerd van de leden Kathmann (GL-PvdA) en Six Dijkstra (NSC)[2]. Hoewel over deze initiatiefnota separaat een appreciatie opgesteld wordt, zijn er op punten vergelijkingen te trekken tussen deze evaluatie en de aanbevelingen in de initiatiefnota.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
F.Z. Szabó

[2] https://www.tweedekamer.nl/downloads/document?id=2024D25526

Toelichting resultaten evaluatie door CIO Rijk

Enkele kernresultaten van de evaluatie worden hieronder nader toegelicht. Daar waar van toepassing is aangegeven of dit een resultaat is vanuit de door CIO Rijk uitgevoerde evaluatie of vanuit de door de ADR opgestelde auditrapportage dan wel de resultaten uit de evaluatie van de ARK.

Rapportage

In het *Implementatiekader risicoafweging cloudgebruik*[3] is benoemd dat departementen materieel gebruik van clouddiensten[4] bijhouden en dat er opgave aan CIO Rijk moet plaatsvinden. Dit rapportageproces is beschreven als onderdeel van het reeds bestaande IB-beeld proces. Dit moet nog geëffectueerd worden. Ondertussen is in de jaarlijkse CISO-gesprekken om dit overzicht gevraagd. Uit de evaluatie blijkt dat CISO's onvoldoende informatie hebben om te rapporteren. De interne rapportagefunctie binnen de departementen, en daarmee de externe rapportage naar CIO Rijk moet worden verbeterd om binnen het rapportageproces voor het IB-beeld de juiste informatie te kunnen delen.

De rapportage rechtstreeks aan CIO Rijk conform het cloudbeleid en implementatiekader is nog beperkt. Dit proces lijkt nog niet voldoende te zijn ingericht bij alle departementen.

Uit de opgaven aan de Rekenkamer blijkt dat een registratie van cloud en cloudgebruik bij departementen aanwezig is. Het niveau en het detailniveau van de uitwerking is niet congruent en wisselt qua omvang en diepgang sterk tussen de verschillende rapporterende departementen (zie ook de punten onder «registraties»).

Registraties

In de opgaven zijn niet alle clouddiensten volledig uitgewerkt. Bij SAAS-diensten is bijvoorbeeld wel de leverancier van die dienst benoemd, maar niet altijd of en zo ja welke clouddienst gebruikt wordt voor de levering. Hierdoor kan er een grotere afhankelijkheid zijn van enkele grote leveranciers dan uit een eerste lezing blijkt en is de marktconcentratie mogelijk sterker dan hierna is aangegeven. Tevens is daarmee niet duidelijk of de cloudvoorzieningen worden aangeboden onder de voorwaarden die SLM voor de overheid heeft bedongen, of onder andere afwijkende voorwaarden. Hierdoor is er een risico dat in de door SLM bedongen contracten opgenomen mitigerende maatregelen niet van toepassing zijn op deze verwerkingen.

De overzichten laten zien dat het public cloudgebruik is nog niet aan alle voorwaarden van het cloudbeleid voldoet. Dit betreft ook bestaand cloudgebruik. Dit betekent dat de risico's niet voldoende bekend zijn. Er is dus een inhaalslag nodig op de bestaande clouddiensten om te beoordelen of de risico's in voldoende mate beheerst worden. Voor deze inhaalslag is in het Implementatiekader Risicoafweging Cloudgebruik een periode van drie jaar opgenomen.

Marktconcentratie

Een eerste analyse van de gegevens geeft een bevestiging van het al bestaande beeld dat er in meerdere processen gebruikgemaakt wordt van

---

[3] https://open.overheid.nl/documenten/ronl-734f947ec6465e4f75a56bed82fe64a1135f71a8/pdf

[4] Materieel public cloudgebruik is gebruik van public clouddiensten ten behoeve van het uitvoeren van de primaire taak van een organisatie.

de grote cloudaanbieders (hyperscalers). Dit kan mogelijk leiden tot een ongewenst afhankelijkheid en zou bij een verstoring bij een van deze aanbieders een gevolg kunnen hebben voor de continuïteit van overheidsprocessen. Dit moet nader onderzocht wordt om te beoordelen hoe groot die afhankelijkheid en het risico zijn om vervolgens een aanpak uit te werken om het risico te verminderen.

Advisering en basisregistraties

Er is door een aantal organisaties collegiaal advies gevraagd over uitgevoerde risicoanalyses met betrekking tot cloudgebruik. Dit heeft in geen van de gevallen geleid tot een formeel advies zoals bedoeld in het Rijksbreed Cloudbeleid. De oorzaak hiervan is dat niet alle basisregistraties worden beheerd door organisaties die binnen het bereik van het Rijksbreed Cloudbeleid vallen. De bredere werking van het beleid is positief te noemen en ik zal waar nodig of mogelijk dit versterken.

De Unit Weerbaarheid van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) heeft verschillende vragen uit de Rijksoverheid ontvangen over algemene en statelijke dreiging op SaaS en IaaS clouddiensten en mogelijke maatregelen voor weerbaarheid. Daarnaast heeft de Unit Weerbaarheid verschillende rapporten over cloudrisico en weerbaarheid geschreven, die binnen de Rijksoverheid zijn verspreid. De AIVD houdt de ontwikkelingen actief bij en geeft hier regelmatig presentaties over binnen de Rijksoverheid.

Materialiteit

In het cloudbeleid en het implementatiekader wordt de term «materieel cloudgebruik» gebruikt. Dit omvat cloudgebruik binnen processen en voorzieningen van enige omvang die relevant zijn voor de werking van elk departement en daarmee van de staat. Hierin zit bewust ruimte zodat de focus ligt op het cloudgebruik dat ertoe doet. Echter, in de gesprekken komt naar voren dat de term materialiteit onduidelijkheid geeft. Hierdoor wordt er geworsteld met de beoordeling van public cloudgebruik. CIO Rijk zal in het beleid, het implementatiekader of de handreiking dit verder verduidelijken.

Departementaal cloudbeleid en -strategie

Niet alle departementen hebben ten tijde van deze evaluatie een eigen cloudbeleid opgesteld. Reeds vastgestelde departementale cloudbeleidsvormen zijn als aanpassing van reeds eerder bestaand cloudbeleid aan de hand van het Rijksbreed Cloudbeleid opgesteld, of het Rijksbreed Cloudbeleid is geadopteerd en organisatie specifiek is gemaakt. Hierdoor is het mogelijk dan niet alle voorwaarden uit het rijksbrede cloudbeleid zijn vertaald of overgenomen in uitvoering bij die organisaties. De organisaties zijn nog niet bevraagd op hun cloudstrategie.

Afweging publieke waarden, soevereiniteit en inkoop van clouddiensten

In de onderzoeken van de ADR en ARK en de uitvraag is geen opgave gevraagd van afweging publieke waarden. In de komende CISO-gesprekken zal hier aandacht aan worden gegeven Op basis hiervan zal worden bepaald op welke punten het cloudbeleid of het implementatiekader moeten worden aangepast.

Ook is er behoefte aan extra uitgangspunten en mogelijke afwegingen op het gebied van soevereiniteit en afweging van noodzakelijkheid cloudge-

bruik bij inkoop van diensten. Ook bestaat de vraag om additionele aandacht voor (en inzicht in) risico's van concentratierisico's en digitale soevereiniteit zowel vanuit het oogpunt van nationale veiligheid als vanuit noodzakelijkheid van beschikbaarheid van kritieke overheidsprocessen te benoemen in het cloudbeleid.

Digitale soevereiniteit

Inmiddels wordt er op diverse plekken onderzoek gedaan naar digitale soevereiniteit om te bepalen waar en in welke mate de noodzaak voor een soevereine vorm van cloud nodig is, en hoe we daar invulling aan kunnen geven. Recent is er bijvoorbeeld in opdracht van het NBV een onderzoek uitgevoerd door het Instituut Clingendael over Europese cloudsoevereiniteit. Clingendael benoemt de noodzaak om bij het gebruik van publieke clouddiensten een balans tussen efficiëntie en soevereiniteit te vinden. Dit sluit aan op de beleidsdoelen van het kabinet in de Agenda Digitale Open Strategische Autonomie (DOSA)[5].

Kengetallen uit opgaven[6]

Op basis van een eerste opgave gedaan door departementen voor het onderzoek van de Algemene Rekenkamer, zoals deze eind 2023 zijn uitgevraagd, is door CIO Rijk een beperkte analyse uitgevoerd en is de data verrijkt. Op basis daarvan is het onderstaande overzicht gemaakt van het gekende cloudbeleid.[7]

Tabel 1 – overzicht public cloudgebruik

Aantal clouddiensten die rijksorganisaties in totaal hebben opgegeven	936
Aantal public of hybride clouddiensten hiervan die als materieel zijn beoordeeld	121
Aantal clouddiensten dat gebruikmaakt van een hyperscaler	179
Aantal materiële diensten ondergebracht bij een hyperscaler	67
Aantal basisregistraties in public cloud	0

De eerste regel in de tabel geeft een overzicht van alle clouddiensten, hieronder vallen ook naast public of hybride clouddiensten ook private cloud omgevingen bij leveranciers waaronder ook overheidsleveranciers. Van het totaal van de 936 opgeven diensten zijn 179 clouddiensten (materieel en niet materieel) die direct of indirect gebruikmaken van een van de grote (Amerikaanse) hyperscalers.[8]

Uit de opgaven blijkt dat binnen de departementen 121 materiële clouddiensten worden gebruikt, hiervan is opgegeven dat het bij 67 diensten public cloudgebruik betreft.

---

[5] Agenda Digitale Open Strategische Autonomie | Rapport | Rijksoverheid.nl

[6] Van twee departementen is de opgave nog niet meegenomen in deze tussentijdse uitvraag door de Rekenkamer. De opgave van één departement is onvolledig ingevuld waardoor die diensten niet volledig zijn meegenomen in deze opgave.

[7] De Rekenkamer heeft al het cloudgebruik uitgevraagd en niet alleen het materiële public cloudgebruik.

[8] Zijnde: Adobe, Akamai, Amazon, Apple, Google, Meta, en Microsoft.

Er zijn geen meldingen of opgaven van basisregistraties die gebruikmaken van publieke cloudvoorzieningen.

Marktconcentratie

Hoewel door de ARK niet rechtstreeks is uitgevraagd in de opgaven welke diensten zijn ondergebracht bij een hyperscaler, is er een eigen indeling gemaakt van het gebruik van hyperscalers voor als materieel benoemde diensten.

Tabel 2 – Marktconcentratie

Hyperscaler	Aantal gebruik	Hiervan opgegeven als materieel
Adobe	2	Geen
Akamai	1	1
Amazon	55	15
Apple	2	Geen
Google	15	6
Meta	1	Geen
Microsoft	102	45

In deze tabel staat een overzicht hoe de herkende diensten zijn verdeeld over de grote leveranciers (hyperscalers). Hieruit blijkt dat er een concentratie van diensten (zowel niet materieel als materiële diensten) is bij de leveranciers Microsoft en, in mindere mate, Amazon.