Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1314

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 maart 2025

In de motie Koekkoek (Volt)[1] is gevraagd om inzichtelijk te maken hoeveel middelen jaarlijks worden besteed aan producten en diensten van grote niet-Europese techbedrijven. Daarnaast is het commissiedebat Informatiebeveiliging bij de Overheid van 12 september 2024 (Kamerstuk 26 643, nr. 1227) heeft het lid Six Dijkstra (NSC) verzocht om in te gaan op de vraag of de methodiek van de uitvoering voor de motie Rajkowski/Van Weerdenburg[2] ook ten goede kan komen aan het beeld dat de Tweede Kamer kan krijgen van programmatuur, apparatuur en systemen die binnen de overheid gebruikt worden. Op 26 november 2024 heeft het lid Kathmann (GroenLinks/PvdA) gevraagd om een globaal overzicht te geven van overheids-ICT bij niet-Europese clouddiensten. De Kamer wordt over de motie Rajkowski (VVD) en Van Weerdenburg (PVV) geïnformeerd in een separate brief en op basis van die brief zal een technische briefing plaatsvinden.[3] In deze brief ga ik in op de motie Koekkoek (Volt) en de verzoeken.

Kaders, toezicht en waarborgen voor IT-beheer bij de Rijksoverheid

De motie en de gestelde vragen verzoeken om overzichten van programmatuur, apparatuur, leveranciers en ICT-systemen binnen de gehele Rijksoverheid. Echter, elk ministerie en elke uitvoeringsorganisatie is zelf verantwoordelijk voor het beheer van zijn IT. Alle onderdelen van de Rijksoverheid dragen de verantwoordelijkheid om intern inzicht te houden in hun eigen systemen. Rijksbrede registers of overzichten zijn niet beschikbaar.

[1] Kamerstuk 36 600 VII, nr. 67.
[2] Kamerstuk 26 643, nr. 830.
[3] Kamerstukken II 2023/2024, 26 643, nr. 874.

kst-26643-1314
ISSN 0921 - 7371
's-Gravenhage 2025

Het kabinet hecht aan transparantie en verantwoording en ziet daarin een belangrijke rol voor de bestaande controlemechanismen. Departementale jaarverslagen, beleidsdoorlichtingen en verantwoordingsrapportages bieden inzicht in de uitgaven en resultaten van het beleid. Hierop wordt intern en extern controle gehouden door respectievelijk de Auditdienst Rijk en de Algemene Rekenkamer.

Het continu in kaart brengen van risico's en dreigingen is een essentieel onderdeel van de kabinetsbrede aanpak om de digitale en fysieke weerbaarheid van de overheid te versterken. De Rijksoverheid neemt passende maatregelen op basis van actuele dreigingen en ontwikkelingen.[4] Ministeries zijn daarbij gehouden aan verplichtingen zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO) en de NIS2-richtlijn. De naleving hiervan wordt getoetst en gemonitord via audits, inspecties en rapportages aan de Kamer, waaronder cybersecurityrapportages.

Voor het gebruik van clouddiensten geldt het Rijksbrede Cloudbeleid, waarin besluitvorming, risicoacceptatie en monitoring plaatsvinden via reguliere afspraken zoals de departementale mandateringsregeling en het CIO-stelsel.[5] CIO-Rijk bewaakt het Rijksbrede informatiebeveiligingsbeeld en voert jaarlijkse CIO-gesprekken. Departementaal-overstijgende registers of overzichten zijn niet voorhanden. Het opstellen van dergelijke overzichten betekent een aanzienlijke administratieve last voor de departementen, terwijl de beschikbare middelen en capaciteit hiervoor beperkt zijn. Voor de globale overzichten van overheids-ICT bij niet-Europese clouddiensten vindt u de beschikbare en deelbare informatie in de Kamerbrief evaluatie Rijksbreed cloudbeleid en het Algemene Rekenkamerrapport «Het Rijk in de cloud».[6]

Risico's, beperkingen en haalbaarheid van rijksbrede ICT-overzichten

Een gedetailleerd rijksbreed overzicht van alle ICT-assets is bovendien niet haalbaar, kent juridische en praktische beperkingen en brengt bovendien veiligheidsrisico's met zich mee. Elke dag zijn er bij de Rijksoverheid en al haar uitvoerende diensten wijzigingen in de programmatuur, apparatuur, de contracten en ICT-systemen. Op onderdelen gaat het om gevoelige informatie. Openbaarmaking kan de kans op beveiligingsincidenten vergroten en strategische keuzes van ministeries ondermijnen. De software en apparatuur wordt aangeschaft binnen de geldende wettelijke kaders, waarbij rekening moet worden gehouden met de deels vertrouwelijke aanbestedingsuitkomsten. Dit brengt tevens wettelijke belemmeringen met zich mee bij het samenstellen van een volledig overzicht.

Met bovenstaande informatie hoop ik voldoende duidelijkheid te hebben verschaft over de kaders, toezicht en waarborgen voor het IT-beheer binnen de Rijksoverheid, evenals de uitdagingen en beperkingen bij het opstellen van gedetailleerde ICT-overzichten. Ik zal u in het tweede kwartaal van 2025 verder informeren over het inzicht in Rijksbrede digitalisering. Gezien de juridische, praktische en veiligheidsrisico's die gepaard gaan met het verstrekken van dergelijke gegevens, worden de verzoeken naar aanleiding van de motie en vragen als afgedaan beschouwd.

---

[4] NCTV, Cybersecuritybeeld Nederland 2024 (CSBN 2024).
[5] Artikel 1c Implementatiekader risicoafweging cloudgebruik.
[6] Kamerstukken II 2024/25, 26 643, nr. 1225 en Algemene Rekenkamer, Het Rijk in de Cloud (Den Haag: Algemene Rekenkamer, 2025).

Het kabinet erkent de noodzaak om richting te geven aan de verantwoorde inzet van digitale technologie door de overheid. Dit is niet alleen van belang voor goede dienstverlening aan onze burgers, maar ook voor het beschermen van onze digitale autonomie en veiligheid. Deze uitgangspunten worden tot slot meegenomen in de Nederlandse Digitaliseringsstrategie, die dit voorjaar aan uw Kamer wordt gepresenteerd.

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