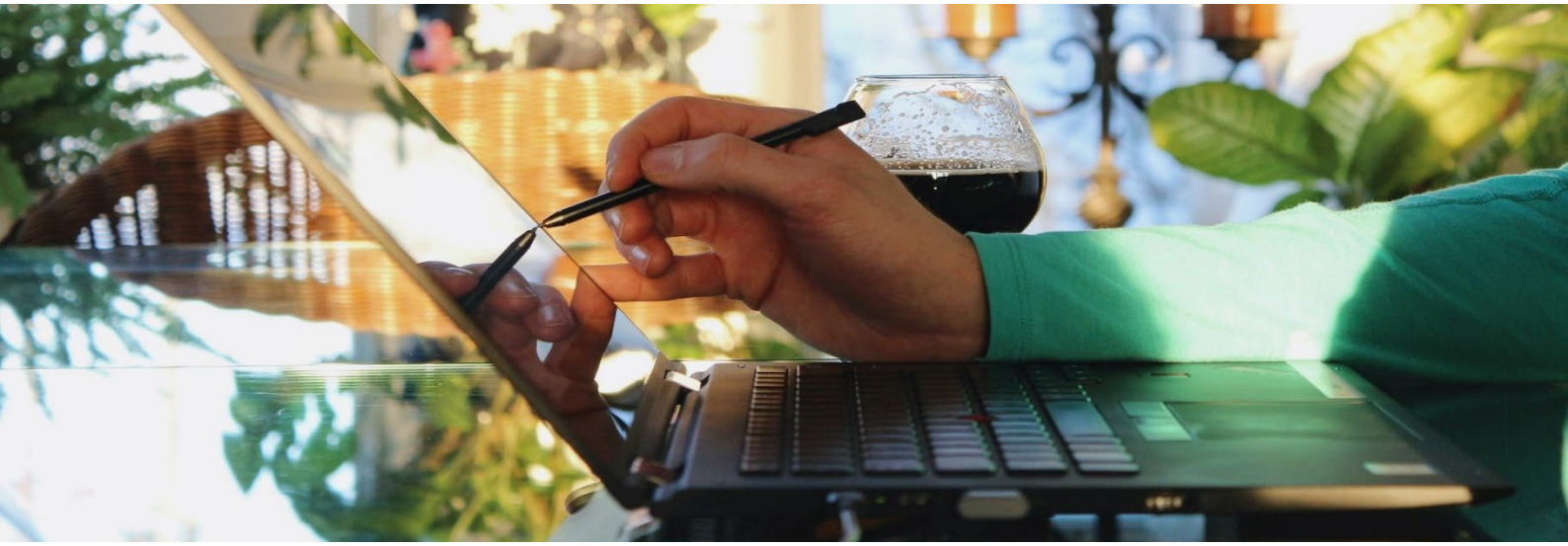
Rathenau Instituut

Overwegingen bij het Rijksbreed cloudbeleid



Bericht aan het parlement

Tot en met 2 november 2022 kan de vaste Kamercommissie Digitale Zaken inbreng leveren op het Rijksbreed cloudbeleid. In dit bericht wijst het Rathenau Instituut erop dat het kabinet kiest voor een nieuwe visie op het gebruik van clouddiensten. Het Rathenau Instituut geeft de Kamerleden ter overweging mee een debat aan te vragen, om de afweging van het kabinet zorgvuldig te toetsen en de risico's van de nieuwe cloudstrategie te verhelderen, inclusief het risico op afhankelijkheid.

Rijksbrede cloudstrategie

Met deze nieuwe strategie kiest het kabinet ervoor om overheidsorganisaties publieke clouddiensten te laten gebruiken onder bepaalde voorwaarden. Met 'publieke clouddiensten' wordt gedoeld op clouddiensten aangeboden door commerciële partijen die door meerdere klanten tegelijkertijd gebruikt kunnen worden. Bij commerciële partijen wordt volgens de Kamerbrief Rijksbreed cloudbeleid gedacht aan Microsoft,

Amazon en Google. Aan het gebruik zijn voorwaarden onderhevig, bijvoorbeeld ten aanzien van de verwerking van persoonsgegevens.

De belangenafweging valt nu anders uit dan ten tijde van de vorige cloudstrategie (2011). In de eerdere cloudstrategie werd ingezet op de ontwikkeling van een cloud voor de Rijksoverheid in eigen beheer. Redenen voor deze nieuwe strategie zijn volgens de brief onder andere de verbeterde beveiliging en privacywaarborgen in de dienstverlening door de commerciële aanbieders.

Overwegingen

Het Rathenau Instituut geeft bij deze nieuwe strategie graag de volgende overwegingen mee.

- Het goed beveiligen van data vraagt expertise en capaciteit, die bij vele partijen onvoldoende aanwezig is. Cloudaanbieders hebben die expertise en capaciteit over het algemeen wel. (Zie ook Cyberweerbaar met nieuwe technologie, p. 29 - 30). Ook zijn de nieuwe voorwaarden transparant en eenduidig voor potentiële nieuwe cloudleveranciers die diensten zouden willen aanbieden aan de Rijksoverheid.

- Er kleven ook nadelen aan deze nieuwe strategie. Met de nieuwe cloudstrategie kiest het kabinet ervoor het belang van goede beveiliging en potentiele kostenbesparing zwaarder te laten wegen dan het risico van afhankelijkheid. Deze groeiende afhankelijkheid van een klein aantal private cloudaanbieders gaat gepaard met risico's van uitval en verstoring, maar ook met het risico van verlies van controle en zeggenschap over data en dataverwerking.

- Nederland en de Europese Unie streven naar meer (digitale) strategische autonomie. Het nieuwe Rijksbrede cloudbeleid lijkt in strijd met deze ambitie. De cloud is onmisbaar geworden voor het functioneren van vele (soms kritieke) overheidsprocessen. Zeggenschap houden over de cloudinfrastructuur is een wezenlijk deel van de Nederlandse strategische autonomie (Preadvies Staatsconferentie 2020). De Rijksoverheid maakt zich met deze aanpak afhankelijk van buitenlandse technologiebedrijven en riskeert daarmee haar autonomie te verliezen op de langere termijn.

- Het kabinet beoogt met deze aanpak het gebruik van diensten van bedrijven zoals Amazon, Microsoft en Google op gecontroleerde wijze (verder) mogelijk te maken. Dit zijn bedrijven met een groot marktaandeel die partijen zoals de overheid een geïntegreerd aanbod aan diensten (die optimaal samenwerken) kunnen leveren. Eenmaal gekozen voor een van de cloudleveranciers, is het echter lastig om nadien over te stappen op een alternatieve aanbieder. Dat brengt in de praktijk vaak zeer hoge kosten met zich mee, ofwel het risico op lock-in van de gebruiker (ACM, 2022).

- Daarnaast creëert deze afhankelijkheid een zichzelf versterkend effect. Wanneer de Rijksoverheid gebruik maakt van de diensten van deze technologiebedrijven, bouwt zij de eigen kennis en capaciteit niet op en verliest daarmee de mogelijkheid om de cloud weer onder eigen controle te beheren als de omstandigheden daar om vragen. De aanzienlijke voorsprong van de eerder genoemde cloudleveranciers wordt verder vergroot en steeds moeilijker in te lopen voor kleinere (Europese) clouddiensten die de grootschaligheid van werken met meerdere overheidsinstanties nog niet aankunnen. Of ze moeten noodgedwongen gebruik maken de clouds van grote techbedrijven om hun eigen diensten op te laten draaien. Ook kan geringe kennis en expertise de onderhandelingspositie van de overheid bemoeilijken, zoals bij het formuleren van een voor de overheid gunstige exitstrategie.

- De strategie gaat beperkt in op hoe het kabinet dit risico op afhankelijkheid ziet. Bovendien lijkt het kabinet het risico op afhankelijkheid met de genoemde maatregelen niet voldoende te kunnen tegengaan. Bij dergelijke maatregelen valt te denken aan concrete eisen aan ICT-systemen om de risico's op afhankelijkheid in te dammen en te investeren in de eigen expertise en capaciteit op de lange termijn (Preadvies Staatsconferentie 2020)

- De Tweede Kamer kan vragen om een debat, om de afweging van het kabinet zorgvuldig te toetsen en de risico’s van de nieuwe cloudstrategie te verhelderen, inclusief het risico op afhankelijkheid. Wanneer alle risico’s in beeld zijn, kan ook gesproken worden over mitigerende maatregelen om de afhankelijkheid op langere termijn af te bouwen.

Kader Relevante publicaties

Beter beslissen over datacentra (Rathenau Instituut, 2022)
De stand van digitaal Nederland (Rathenau Instituut, 2021)
Cyberweerbaar met nieuwe technologie (Rathenau Instituut, 2020)

Diverse partijen waarschuwen voor de risico’s van afhankelijkheid van clouddiensten van buitenlandse techbedrijven:
ACM Marktstudie clouddiensten (2022)
TNO (2022)
Memo over de Amerikaanse Cloud Act van advocatenkantoor Greenberg Traurig aan Nationaal Cyber Security Centrum (2022)
Preadvies Staatsconferentie (2020)
