

Eindrapport

In het kader van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers voor het ministerie van Economische Zaken

Ons kenmerk: A2400031906 / Definitieve versie

—
16 augustus 2024



Inhoud



Samenvatting

- 01** Introductie
- 02** Geïdentificeerde gaps
- 03** Oplossingsrichtingen en aanbevelingen

Bijlagen

Samenvatting

Samenvatting

KPMG heeft een gapanalyse uitgevoerd op het Europese*/Nederlandse cloudprovider en het Amerikaanse hyperscaler aanbod.

De gapanalyse is uitgevoerd in de vorm van een quickscan. Deze quickscan heeft als doel inzicht te krijgen in de huidige staat van de Europese/Nederlandse cloudmarkt in vergelijking met de Amerikaanse marktleiders. Een quickscan geeft de mogelijkheid om in een korte periode van drie maanden een beeld te krijgen van de belangrijkste gaps, maar heeft ook beperkingen in de diepgang. Daarmee omvat deze quickscan geen oordeel of conclusie over de kwaliteit, afdwingbaarheid of compliance met wet- en regelgeving van de juridische voorwaarden die door de geselecteerde cloudproviders worden gehanteerd.

Het quickscan-onderzoek is uitgevoerd op basis van een onderzoekskader en richt zich op 39 technische en functionele criteria en 36 juridische en organisatorische aspecten.

Hierbij is het dienstenaanbod van acht Europese/Nederlandse cloudaanbieders vergeleken met het aanbod van drie Amerikaanse hyperscalers.

De informatievoorziening en het dienstenaanbod van cloudproviders veranderen over de tijd. De uitkomsten van deze gapanalyse moeten daarom ook worden gezien als een weergave van de situatie op het moment van het onderzoek.



Er zijn gaps in het aanbod geïdentificeerd

Uit de gapanalyse blijkt dat er op dit moment gaps bestaan tussen het aanbod van Europese/Nederlandse cloudproviders en het aanbod van de Amerikaanse hyperscalers. Individuele organisaties moeten zelf vaststellen of de geïdentificeerde gaps invloed hebben op de organisatie-specifieke criteria.

Europese providers bieden een beperkt geïntegreerd dienstenaanbod. De geselecteerde Nederlandse providers bieden voornamelijk IaaS-diensten en beperkt PaaS-diensten. Moderne en innovatieve diensten worden meer en sneller aangeboden bij Amerikaanse hyperscalers. Om te komen tot een breed pallet aan functionaliteiten dat volledig vergelijkbaar is met dat van de Amerikaanse hyperscalers, zou een combinatie van meerdere Europese/Nederlandse aanbieders gekozen moeten worden. Verder bieden de Amerikaanse hyperscalers veel informatie aan op hun website over het aanbod van clouddiensten en de juridische voorwaarden. Bij Europese/Nederlandse cloudproviders is niet al deze informatie publiek beschikbaar. Dit is een aandachtspunt en vraagt van een organisatie meer interactie met de cloudprovider om te kunnen komen tot een afgewogen keuze van dienstverlening.

Oplossingsrichtingen voor het versterken van de positie van Europese/Nederlandse cloudproviders

De Agenda Digitale Open Strategische Autonomie beschrijft dat het wenselijk is om de Europese digitale afhankelijkheid van derden te borgen. Om het voor organisaties aantrekkelijker te maken om te kiezen voor een Europese/Nederlandse cloudprovider, worden drie oplossingsrichtingen aanbevolen, welke verder worden toegelicht in hoofdstuk 3:

1. Het verbeteren van de informatievoorziening en communicatie over het dienstenaanbod.
2. Het verstevigen van het dienstenaanbod en innovatie van Europese/Nederlandse cloudproviders.
3. Het stimuleren van de vraag naar Europese/Nederlandse cloudproviders.



01

Introductie

Introductie

Achtergrond

Er is brede aandacht voor de inrichting van een digitale Europese infrastructuur die onafhankelijk kan functioneren. In de Agenda Digitale Open Strategische Autonomie, die als doel heeft de Europese digitale afhankelijkheid van derden te beheersen¹, zijn cloud- en netwerktechnologie twee beleidsprioriteiten. Zo worden ook 'digitale toepassingen' gezien als één van de vier strategische autonomiegebieden waarvoor extra aandacht gewenst is². Er lopen verschillende Europese initiatieven om het Europese cludaanbod te stimuleren (waaronder IPCEI CIS, European Alliance for Industrial Data, Edge and Cloud, Gaia-X) en er is wetgeving ingericht om de digitale interne markt beter te laten functioneren (zoals de AVG, DMA (Digital Markets Act), DA (Data Act) en de Wbni).

De Directie Digitale Economie (hierna: DE) van het ministerie van Economische Zaken (hierna: EZ) wenst een beter inzicht te krijgen in de huidige staat van de Nederlandse en Europese cloudmarkt. Hiertoe is aan KPMG Advisory N.V. (hierna: KPMG) gevraagd om een quickscan uit te voeren op de Europese en Nederlandse cloudmarkt. Het doel van deze quickscan is het krijgen van inzichten met betrekking tot hoe de Europese/Nederlandse cloudproviders zich verhouden tot de Amerikaanse marktleiders (de Amerikaanse 'hyperscalers'), in hoeverre er door Europese/Nederlandse cloudproviders aan de eisen van SIDN voldaan kan worden, en welke maatregelen getroffen kunnen worden om het Europese/Nederlandse cludaanbod te stimuleren.

In dit quickscan-onderzoek staan de volgende twee onderzoeksvragen centraal:

1. In termen van technische functionaliteit en kwaliteit van clouddiensten, hoe scoort Nederlands, respectievelijk Europees aanbod van clouddiensten op de verschillende lagen (IaaS, PaaS en SaaS) in de stack in vergelijking met het aanbod van de Amerikaanse marktleiders? Met andere woorden, waaruit bestaat het verschil in het aanbod ('gap-analyse')?
2. Wat zijn de juridische en organisatorische aspecten c.q. gevolgen die overwogen moeten worden bij de keuze voor Europese/Nederlandse cloudproviders, ten opzichte van het afnemen van een geïntegreerd cludaanbod van een van de Amerikaanse marktleiders?

Aanpak

KPMG heeft in de periode mei t/m augustus 2024 een quickscan-onderzoek uitgevoerd overeenkomstig de overeengekomen opdrachtvoorwaarden. Hiervoor zijn – naast drie Amerikaanse hyperscalers (Microsoft Azure, Amazon Web Services en Google Cloud Platform) – acht Europese/Nederlandse cloudproviders geselecteerd. Dit betreffen T-Systems Open Telekom Cloud, Orange Flexible Engine, OVHcloud, IONOS, Scaleway, KPN CloudNL, Leaseweb en ODC-Noord. In bijlage 1 zijn de selectiecriteria opgenomen. Voor deze cloudproviders is een analyse uitgevoerd op basis van een onderzoekskader dat is opgesteld in consultatie met een voor dit onderzoek samengestelde klankbordgroep. Het onderzoekskader is opgenomen in bijlage 2, de daarbij gehanteerde definities zijn opgenomen in bijlage 3.

Het onderzoekskader bestaat uit technische en functionele criteria en de juridische aspecten die overwogen kunnen worden bij de selectie van een cloudprovider. De analyse in deze quickscan is uitgevoerd op basis van openbare bronnen en publiek beschikbare informatie. Uit de eerste resultaten blijkt dat bij de Europese/Nederlandse providers informatie over een deel van de criteria niet publiek beschikbaar is. Daarom is de analyse aangevuld met vragenlijsten die zijn uitgezet naar vijf cloudproviders (Leaseweb, KPN CloudNL, ODC-Noord, Scaleway en IONOS). De analyse resulteert in een overzicht van de (relatieve) omvang van het technische en functionele dienstenaanbod van deze Europese/Nederlandse cloudproviders, afgezet tegen de Amerikaanse hyperscalers.

Op basis van de geïdentificeerde gaps zijn inpassingsmaatregelen gedefinieerd die organisaties kunnen nemen om de keuze voor een Europese of Nederlandse cloudprovider mogelijk te maken. Tevens zijn maatregelen gedefinieerd om het Europese/Nederlandse cludaanbod te stimuleren. De financiële impact van deze maatregelen op de korte, middellange en lange termijn is in het kader van deze quickscan niet onderzocht en maakt ook geen deel uit van de resultaten.

Dit eindrapport bevat de resultaten van het quickscan-onderzoek.

- Bron: 1 Kamerbrief 'Aanbieden Agenda Digitale Open Strategische Autonomie', 17 oktober 2023
2 Kamerbrief 'Kabinetsaanpak Strategische Afhankelijkheden', 12 mei 2023

02

Geïdentificeerde gaps

Toelichting op de uitgevoerde analyse

Op de volgende pagina's worden de uitkomsten van de analyse weergegeven. In deze analyse is op basis van openbare bronnen en publieke informatie vastgesteld in hoeverre de cloudproviders voldoen aan enerzijds functionele en technische criteria en anderzijds juridische en organisatorische aspecten uit het onderzoekskader. Daarnaast zijn de uitkomsten aangevuld met antwoorden op vragenlijsten die zijn uitgezet naar vijf Europese/Nederlandse cloudproviders (Leaseweb, KPN CloudNL, ODC-Noord, Scaleway en IONOS).

Toelichting op het onderzoekskader

In het onderzoekskader zijn functionele en technische criteria benoemd, alsmede juridische en organisatorische aspecten. Deze criteria en aspecten zijn gecategoriseerd. Voor iedere categorie is een toelichting gegeven.

Toelichting op de observaties

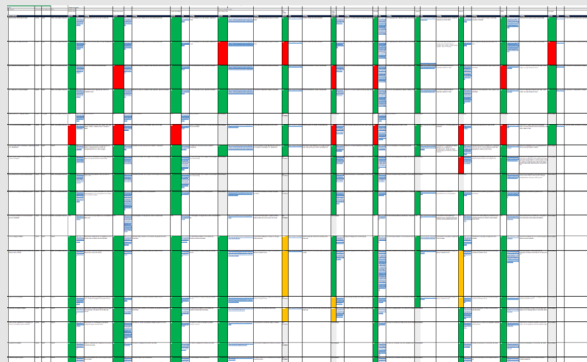
In de observaties is weergegeven:

1. In hoeverre de geselecteerde cloudproviders invulling geven aan de functionele en technische criteria.
2. In hoeverre publiek beschikbare informatie en opgehaalde informatie uit interviews de juridische en organisatorische aspecten afdekt.

Toelichting op de gaps en aandachtspunten

Op basis van de analyse en observaties zijn gaps geïdentificeerd tussen het clouदानbod van Europese/Nederlandse cloudproviders en dat van Amerikaanse hyperscalers. Hierbij worden de aandachtspunten benoemd voor organisaties die gebruik willen maken van Europese/Nederlandse cloudproviders.

Quickscan clouदानbod



Onderzoekskader

Beschrijving analyse criteria/aspecten

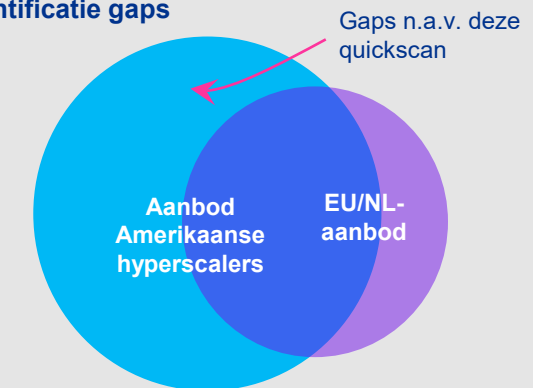
- Het criterium wordt (grotendeels) ingevuld/de beschikbare/opgehaalde informatie dekt het aspect af.

- Het criterium wordt deels ingevuld/de beschikbare/opgehaalde informatie dekt het aspect deels af.

- Het criterium wordt niet ingevuld/de beschikbare/opgehaalde informatie dekt het aspect niet af.

- Niet bekend, geen/te beperkte informatie beschikbaar/opgehaald voor dit criterium/aspect.

Identificatie gaps



Illustratief verschil in aanbod van Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers

Observaties technische en functionele criteria

Samenvatting van de criteria

Observaties

Geïdentificeerde gaps en aandachtspunten

De technische en functionele criteria zijn geclusterd in de volgende categorieën:

- Locatie
- Generieke dienstverlening
- Functionaliteit – Beveiliging
- Functionaliteit – Algemeen
- Functionaliteit – PaaS
- Functionaliteit – SaaS

1. De Amerikaanse hyperscalers bieden wereldwijd diensten aan, de Europese cloudproviders beperken zich meestal tot (enkele landen in) Europa. Twee van de drie Nederlandse onderzochte cloudproviders bieden alleen diensten aan vanuit Nederlandse datacenters.
2. De generieke dienstverlening (m.b.t. ondersteuning, exit/portabiliteit en klanttevredenheid) lijkt voor zowel Amerikaanse hyperscalers als Europese/Nederlandse cloudproviders grotendeels aan dezelfde criteria te voldoen. Wel bieden Nederlandse cloudproviders meer ondersteuning gericht specifiek op Nederland (bijvoorbeeld op het gebied van compliance en support), en hebben de Amerikaanse hyperscalers meer focus op innovatie (nieuwe functionaliteiten).
3. De Europese/Nederlandse cloudproviders bieden voor de onderzochte criteria vergelijkbare beveiligingsdiensten als de Amerikaanse hyperscalers. Geïntegreerde compliance monitoring (zoals een dashboard waaruit compliance met – bijvoorbeeld ISO-normeringen – blijkt) wordt door de Europese/Nederlandse cloudproviders niet of in beperkte mate aangeboden.
4. Over het algemeen bieden de Amerikaanse hyperscalers een breder en innovatiever dienstenaanbod dan de Europese/Nederlandse cloudproviders. Everything-as-a-code is een voorbeeld van een dienst die door weinig Europese/Nederlandse providers wordt aangeboden. Alle onderzochte providers bieden IaaS-diensten aan, die in de basis op hoofdlijnen vergelijkbare functionaliteit bieden.
5. Het aanbod van PaaS-diensten is verschillend per provider, waarbij het Europese/Nederlandse aanbod beperkter is dan dat van Amerikaanse hyperscalers.
6. Europese/Nederlandse cloudproviders bieden over het algemeen geen of zeer beperkt additionele SaaS-diensten aan.

- A. Europese providers bieden een beperkt geïntegreerd dienstenaanbod. De Nederlandse providers bieden voornamelijk IaaS-diensten en beperkt PaaS-diensten. Om te komen tot een breed pallet aan functionaliteiten dat volledig vergelijkbaar is met dat van de Amerikaanse hyperscalers, zou een combinatie van meerdere Europese/Nederlandse aanbieders gekozen moeten worden. Dit vraagt ook om een additionele integratie tussen deze providers, het opbouwen van kennis van meerdere platforms en het aansturen van meerdere leveranciers, maar zorgt wel voor minder internetcentralisatie.
- B. De Amerikaanse hyperscalers bieden veel online documentatie aan over het aanbod van clouddiensten. Bij Europese/Nederlandse cloudproviders is niet alle informatie publiek beschikbaar. Dit is een aandachtspunt en vraagt om meer interactie met de cloudprovider over de exacte dienstverlening, voorwaarden, etc. om te kunnen komen tot een afgewogen keuze van dienstverlening.
- C. Moderne en innovatieve clouddiensten zijn bij de Amerikaanse hyperscalers breed beschikbaar. Bij de Europese/Nederlandse cloudproviders zijn deze niet altijd beschikbaar (bijvoorbeeld wanneer een organisatie Everything-as-a-Code als functionaliteit beschikbaar wil hebben in de afgenomen cloudomgeving).
- D. Europese/Nederlandse cloudproviders worden beperkt vermeld in marktrapporten van gerenommeerde onderzoeksbureaus. Hierdoor staan deze providers minder 'op de radar' wanneer organisaties deze rapporten gebruiken bij de selectie van een cloudprovider.
- E. De ontwikkelsnelheid van nieuwe diensten is lager bij Europese/ Nederlandse cloudproviders dan bij Amerikaanse hyperscalers, waardoor voor nieuwe toepassingen (bijvoorbeeld op het gebied van AI) er vaak een beperkt geïntegreerd alternatief is voor de Amerikaanse hyperscalers.

Observaties juridische en organisatorische aspecten

Samenvatting van de aspecten Observaties

De juridische en organisatorische aspecten zijn geclusterd in de volgende categorieën:

- Algemeen*
- Bescherming persoonsgegevens
- Intellectueel Eigendom (IE), bedrijfsgeheimen & data
- Beveiliging & certificering
- Kunstmatige Intelligentie (AI)
- Environmental, Social & Governance (ESG)

1. Over het algemeen bieden de Amerikaanse hyperscalers veel informatie over de algemene (juridische) voorwaarden, de bescherming van persoonsgegevens, en IE-rechten en bedrijfsgeheimen. Deze informatie is publiek beschikbaar en veelal eenvoudig (online) te raadplegen. Bij de Europese/Nederlandse cloudproviders is dat in mindere mate het geval. In sommige gevallen is nadere uitvraag bij de Europese/Nederlandse cloudproviders nodig om alsnog de benodigde informatie verkrijgen.
2. De aanwezigheid van certificering is bij Europese/Nederlandse cloudproviders beperkt ten opzichte van de Amerikaanse hyperscalers, al zijn de essentiële (beveiligings)waarborgen aanwezig. Het is opvallend dat de Europese/Nederlandse providers die meegenomen zijn in dit onderzoek geen compliance met de EU Cloud Code of Conduct benoemen en niet beschikken over specifieke privacy certificeringen zoals ISO 27701, terwijl de meeste Amerikaanse hyperscalers hier wel over beschikken.
3. Beleid en informatie over maatregelen ten aanzien van ESG (Environmental, Social & Governance) en AI zijn bij de Amerikaanse hyperscalers publiek beschikbaar. Dit in tegenstelling tot Europese/Nederlandse cloudproviders, die over dergelijke thema's minder informatie over beleid of visie publiek beschikbaar maken.

Geïdentificeerde gaps en aandachtspunten

- A. Inzichten in algemene aspecten, waaronder toepasselijke wet- en regelgeving, aansprakelijkheid en details van de dienstverlening van Europese/Nederlandse cloudproviders, zijn beperkt beschikbaar in vergelijking tot de Amerikaanse hyperscalers. Om een beter beeld te krijgen, was het noodzakelijk om deze informatie nader op te vragen bij de Europese/Nederlandse cloudproviders. Minder beschikbare publieke informatie betekent niet automatisch dat de kennis en informatie niet aanwezig is bij de Europese/Nederlandse cloudproviders. Bij de Amerikaanse hyperscalers is deze informatie veelal direct te raadplegen via de websites van deze providers, al brengt dit niet zonder meer afdwingbaarheid en/of compliance met wet- en regelgeving met zich mee.
- B. De Amerikaanse hyperscalers maken doorgaans informatie over hun beleid rond (persoons)gegevensbescherming publiek beschikbaar. Dit brengt echter niet automatisch afdwingbaarheid of compliance met wet- en regelgeving met zich mee. Bij de Europese/Nederlandse cloudproviders blijft de publieke informatievoorziening achter, al is deze meestal wel beschikbaar op aanvraag. Bovendien betekent de (publieke) afwezigheid van deze informatie bij Europese/Nederlandse cloudproviders niet automatisch dat de gegevensbescherming minder vergaand of goed is.
- C. De publiek beschikbare juridische voorwaarden van Europese/ Nederlandse providers bevatten niet altijd informatie over IE-rechten, bedrijfsgeheimen en eigendom of controle van gegevens en data die bij de cloudprovider wordt opgeslagen. Deze informatie is wel (gedetailleerd) aanwezig bij de Amerikaanse hyperscalers.
- D. Certificeringen lopen erg uiteen. Bij de Amerikaanse hyperscalers zijn relatief veel certificeringen aanwezig ten opzichte van de Europese/ Nederlandse cloudproviders. Welke certificaten noodzakelijk zijn voor de beoogde dienstverlening is uiteindelijk afhankelijk van de vereisten van een klant.
- E. Het is moeilijk om vast te stellen in hoeverre de Amerikaanse hyperscalers hun beleid omtrent ESG (Environmental, Social & Governance) en AI daadwerkelijk volgen. Deze thema's zijn echter zeer actueel en specifieke wet- en regelgeving voor deze thema's zal binnen afzienbare tijd van toepassing zijn.

* Omvat o.a. aspecten als toepasselijk recht, aansprakelijkheid, lokalisatie en dienstverlening.

Samenvatting uitkomsten gapanalyse cloudaanbod

Samenvatting analyse technische en functionele criteria en juridische en organisatorische aspecten

| Categorie | Microsoft Azure | Amazon Web Services | Google Cloud Platform | T-Systems Open Telekom Cloud | Orange Flexible Engine | OVHcloud | IONOS | Scaleway | KPN CloudNL | Leaseweb | ODC-Noord |
|------------------------------|--|---------------------|-----------------------|------------------------------|------------------------|----------|-------|----------|-------------|----------|-----------|
| Technisch en functioneel | Locatie | | | | | | | | | | |
| | Generieke dienstverlening | | | | | | | | | | |
| | Functionaliteit – Beveiliging | | | | | | | | | | |
| | Functionaliteit – Algemeen | | | | | | | | | | |
| | Functionaliteit – PaaS | | | | | | | | | | |
| | Functionaliteit – SaaS | | | | | | | | | | |
| Juridisch en organisatorisch | Algemeen* | | | | | | | | | | |
| | Bescherming persoonsgegevens | | | | | | | | | | |
| | IE, bedrijfsgeheimen & data | | | | | | | | | | |
| | Beveiliging & certificering | | | | | | | | | | |
| | Kunstmatige Intelligentie (AI) | | | | | | | | | | |
| | Environmental, Social & Governance (ESG) | | | | | | | | | | |

* Omvat o.a. aspecten als toepasselijk recht, aansprakelijkheid, lokalisatie en dienstverlening.

03

Oplossings- richtingen en aanbevelingen

Oplossingsrichtingen en aanbevelingen

Uit de resultaten van het quickscan-onderzoek blijkt dat er zowel technische en functionele verschillen zijn, als verschillen in de aangeboden dienstverlening tussen de Europese/Nederlandse cloudproviders en de Amerikaanse hyperscalers.

De Agenda Digitale Open Strategische Autonomie beschrijft dat het wenselijk is om de Europese digitale afhankelijkheid van derden te borgen. Om het voor Europese/Nederlandse organisaties aantrekkelijker te maken om te kiezen voor een Europese/Nederlandse cloudprovider, worden daartoe in dit hoofdstuk oplossingsrichtingen en aanbevelingen gegeven. Deze oplossingsrichtingen en aanbevelingen kunnen zorgen voor een versterking van de informatie- en marktpositie van de Europese/Nederlandse cloudproviders. Tevens zijn ze gericht op het aantrekkelijker maken voor Europese/Nederlandse organisaties om te kiezen voor een Europese/Nederlandse cloudprovider.

De oplossingsrichtingen en aanbevelingen zijn geclusterd in drie categorieën:

1. Het verbeteren van informatievoorziening en communicatie over het dienstenaanbod.
2. Het verstevigen van het dienstenaanbod en innovatie van Europese/Nederlandse cloudproviders.
3. Het stimuleren van de vraag naar Europese/Nederlandse cloudproviders.

Oplossingsrichting 1: Het verbeteren van informatievoorziening en communicatie over het dienstenaanbod

Aanbeveling 1.1: Stimuleren van cloudproviders om informatievoorziening over producten, diensten en voorwaarden uit te breiden

Uit het quickscan-onderzoek blijkt dat een deel van de informatie over de criteria uit het onderzoekskader niet publiek beschikbaar is bij de Europese/Nederlandse cloudproviders. Hierdoor moeten (potentiële) klanten informatie opvragen bij de cloudproviders.

SIDN-casus

Uit de gapanalyse blijkt – voor zover het de SIDN-casus betreft – dat Europese/Nederlandse cloudproviders de door SIDN opgestelde technische en functionele criteria evenals de juridische aspecten slechts gedeeltelijk kunnen invullen. Daarnaast geldt dat er over het algemeen gaps bestaan tussen het aanbod van Europese/Nederlandse cloudproviders en het aanbod van de Amerikaanse hyperscalers. Individuele organisaties moeten zelf vaststellen of de geïdentificeerde gaps invloed hebben op de organisatiespecifieke criteria en of daarmee een keuze voor een Europese/Nederlandse cloudprovider mogelijk is.

Het is aannemelijk dat ook andere organisaties die een keuze gaan maken voor het afnemen van publieke clouddiensten een vergelijkbare afweging moeten maken en vergelijkbaar onderzoek moeten uitvoeren. De SIDN-casus biedt aanknopingspunten voor de bredere (semi)publieke sector voor het evalueren van het publieke cloudaanbod. In dit hoofdstuk is een aantal aanknopingspunten opgenomen.

Het stimuleren van cloudproviders om de informatievoorziening over producten, diensten en voorwaarden te verbeteren leidt tot een betere informatiepositie voor (potentiële) klanten, zodat zij eenvoudiger en beter geïnformeerd een keuze kunnen maken.

Aanbeveling 1.2: Uitvoeren van een marktstudie om het inzicht in de Europese/Nederlandse cloudmarkt te vergroten

In de marktstudies die gebruikt zijn in dit quickscan-onderzoek zijn de Amerikaanse hyperscalers prominent vertegenwoordigd. Europese/Nederlandse cloudproviders worden in mindere mate genoemd. Deze marktstudies worden mogelijk door potentiële klanten gebruikt bij het selecteren van een cloudprovider.

Het uitvoeren van een specifieke marktstudie naar de Europese/Nederlandse publieke cloudmarkt kan helpen bij het creëren van inzichten in deze markt en de marktpositie van de Europese/Nederlandse cloudproviders. Dit kan bijvoorbeeld resulteren in een longlist van cloudproviders. Een dergelijk initiatief kan organisaties helpen bij het maken van een keuze voor een cloudprovider (een voorbeeld hiervan is de Distributed Open Marketplace for Europe, een catalogus van het aanbod van Europese cloud- en edge-diensten).

Oplossingsrichtingen en aanbevelingen (vervolg)

Oplossingsrichting 2: Het verstevigen van het dienstenaanbod en innovatie van Europese/Nederlandse cloudproviders

Aanbeveling 2.1: Cloudproviders stimuleren om een breder dienstenaanbod te leveren zodat dit meer in lijn komt met het aanbod van de Amerikaanse hyperscalers

Het uitbreiden van het dienstenaanbod stelt Europese/Nederlandse cloudproviders in staat om een completere en concurrerende dienstverlening aan te bieden.

Aanbeveling 2.2: Bundelen en ondersteunen van Europese projecten voor het aanbieden van clouddiensten

Een clouddienstenaanbod dat vergelijkbaar is met de Amerikaanse hyperscalers vraagt om forse investeringen, bijvoorbeeld in research & development. Het bundelen en ondersteunen van deze investeringen biedt cloudproviders de mogelijkheid tot schaalvergroting en verdere innovatie van het cloudaanbod.

Waar het niet mogelijk is om diensten via een commerciële publieke cloudprovider aan te bieden, kan de rijksoverheid ervoor kiezen om – voor de rijksoverheid – diensten aan te bieden via de Shared Service Centers (SSC's) of Overheidsdatacenters (ODC's).

Aanbeveling 2.3: Ondersteunen van cloudproviders bij certificering

Uit het quickscan-onderzoek blijkt dat Europese/Nederlandse cloudproviders beschikken over verschillende sets van certificaten en verklaringen op het gebied van informatiebeveiliging, gegevensbescherming en ESG. Amerikaanse hyperscalers beschikken over een brede set van verklaringen en certificeringen.

Het verstrekken van informatie aan cloudproviders over gangbare certificeringen en verklaringen, en hoe deze te verkrijgen, kan hen helpen om (potentiële) klanten meer comfort te geven over de kwaliteit van de dienstverlening.

Oplossingsrichting 3: Het stimuleren van de vraag naar Europese/Nederlandse cloudproviders

Aanbeveling 3.1: Spreiding van het publieke cloudgebruik door de rijksoverheid tussen Amerikaanse hyperscalers en Europese/Nederlandse cloudproviders

Binnen de rijksoverheid wordt voor publieke clouddiensten momenteel ook gebruikgemaakt van het aanbod van de Amerikaanse hyperscalers.

Om de afhankelijkheid van de Amerikaanse hyperscalers te verminderen en het gebruik van diensten tussen verschillende leveranciers te balanceren, kan de rijksoverheid ervoor kiezen om – waar mogelijk binnen o.a. de aanbestedingskaders en beveiligingsvereisten – clouddiensten af te nemen van Europese/Nederlandse cloudproviders. Hiermee stimuleert de rijksoverheid (direct en indirect) het gebruik van clouddiensten van Europese/Nederlandse cloudproviders.

Aanbeveling 3.2: Ondersteunen van organisaties bij keuzes voor Europese digitale onafhankelijkheid

Organisaties kunnen de behoefte hebben om Europese digitale onafhankelijkheid na te streven. Om deze partijen te ondersteunen bij de keuze voor een cloudprovider, kunnen keuzehulpen en richtlijnen worden opgesteld. Deze ondersteunen organisaties bijvoorbeeld bij het definiëren van de criteria met betrekking tot soevereiniteit (bijv. zoals het SURF afwegingskader 'Grip op de clouds', beschreven in de 'Cloud sourcing strategie' voor het SURF cloud event 2024).

Bijlagen

1. Geselecteerde cloudproviders voor de quickscan
2. Onderzoekskader
3. Gehanteerde definities
4. SIDN-casus
5. Scenario's voor het kiezen van een Europese/Nederlandse cloudprovider

B1

**Geselecteerde
cloudproviders
voor de
quicksan**

Geselecteerde cloudproviders voor de quickscan

De analyse is gestart met een longlist van cloudproviders

Er is een longlist van relevante cloudproviders opgesteld. Naast de drie Amerikaanse hyperscalers, zijn Nederlandse en Europese cloudproviders toegevoegd. Deze zijn geselecteerd op basis van suggesties van het ministerie van EZ, de klankbordgroep en leden van verenigingen van Europese cloudproviders, en op basis van cloudproviders die zijn benoemd in marktrapporten van analisten. Dit heeft geresulteerd in een longlist van 51 cloudproviders.

De selectie heeft plaatsgevonden op basis van kaders en prioritering

Voor de selectie van cloudproviders die worden geanalyseerd in de quickscan zijn de volgende kaders gehanteerd:

- Naast drie Amerikaanse hyperscalers worden maximaal acht Europese cloudproviders geselecteerd. Dit aantal is beperkt tot acht vanwege de beperkte omvang van de quickscan.
- Van deze acht Europese cloudproviders worden minimaal drie Nederlandse cloudproviders geselecteerd.
- De volgende twee minimale vereisten zijn gehanteerd:
 1. De cloudprovider heeft een primaire vestigingsplaats binnen de EU.
 2. De cloudprovider levert ten minste IaaS- en PaaS-services ('doorgeleverde' publieke clouddiensten van de Amerikaanse hyperscalers worden uitgesloten).

De resterende cloudproviders zijn geprioriteerd op basis van de volgende criteria:

- Totale omzet van de organisatie.
- Marktaandeel in Europa.
- Vermelding in marktrapporten van analisten.

De overgebleven cloudproviders zijn in meer detail onderzocht en waar nodig uitgesloten, gebaseerd op de aangeboden dienstverlening.

Acht Europese/Nederlandse cloudproviders zijn geselecteerd

Op basis van deze analyse zijn de volgende cloudproviders geselecteerd:

| Geselecteerde Europese/Nederlandse cloudproviders voor de quickscan | | |
|---|------------------------------|---|
| ID | Cloudprovider | Toelichting |
| 1 | T-Systems Open Telekom Cloud | Europese aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 2 | Orange Flexible Engine | Europese aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 3 | OVHcloud | Europese aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 4 | IONOS | Europese aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 5 | Scaleway | Europese aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 6 | KPN CloudNL | Nederlandse aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 7 | Leaseweb | Nederlandse aanbieder met een significant marktaandeel, die IaaS/PaaS-diensten aanbiedt |
| 8 | ODC-Noord | Belangrijke aanbieder in de Nederlandse publieke sector |

B2

**Onderzoeks-
kader**

Onderzoekskader – Technische en functionele criteria

De technische en functionele criteria (aangeduid met ID's die beginnen met een 'T') die gebruikt zijn tijdens de quickscan worden in de volgende tabellen weergegeven. De toepassing geeft aan op welk type cloudservicemodel het criterium van toepassing is (IaaS, PaaS en/of SaaS). De criteria zijn gebaseerd op het KPMG Cloud Adoption Framework, aangevuld met suggesties voor additionele criteria aangedragen door het ministerie van EZ en de klankbordgroep.

| Technische en functionele criteria | | |
|------------------------------------|---|----------------|
| ID | Criterium | Toepassing |
| Locatie | | |
| T1 | Biedt de provider diensten aan in Europa? | IaaS+PaaS+SaaS |
| T2 | Biedt de provider wereldwijd diensten aan? | IaaS+PaaS+SaaS |
| T3 | Zijn er datacenters in Nederland beschikbaar? | IaaS+PaaS+SaaS |
| T4 | Zijn er datacenters in Europa beschikbaar? | IaaS+PaaS+SaaS |
| Generieke dienstverlening | | |
| T5 | Klanttevredenheid o.b.v. rapportage-analyses | IaaS+PaaS+SaaS |
| T6 | Is de servicedesk in het Nederlands beschikbaar? | IaaS+PaaS+SaaS |
| T7 | Heeft de provider concrete doelstellingen en maatregelen m.b.t. duurzaamheid? | IaaS+PaaS+SaaS |
| T8 | Biedt de provider technische ondersteuning voor een eventuele exit/migratie? | IaaS+PaaS+SaaS |
| T9 | Zijn de diensten die de leverancier aanbiedt portable? | IaaS+PaaS+SaaS |
| T10 | Wordt een SLA voor hoge beschikbaarheid geleverd? | IaaS+PaaS+SaaS |
| T11 | Hoeveel nieuwe clouddiensten heeft de provider afgelopen jaar (2023) uitgebracht? | IaaS+PaaS+SaaS |

Onderzoekskader – Technische en functionele criteria (vervolg)

| Technische en functionele criteria | | |
|--------------------------------------|---|----------------|
| ID | Criterium | Toepassing |
| Functionaliteit – Beveiliging | | |
| T12 | Is DDOS-beveiliging beschikbaar? | IaaS+PaaS+SaaS |
| T13 | Biedt de provider mogelijkheden tot het maken van back-ups van de cloudomgeving? | IaaS+PaaS+SaaS |
| T14 | Is Disaster Recovery beschikbaar? | IaaS+PaaS+SaaS |
| T15 | Is ransomwarebeveiliging beschikbaar? | IaaS+PaaS+SaaS |
| T16 | Biedt de provider monitoring tools om wijzigingen van resources overzichtelijk te maken voor klanten? | IaaS+PaaS+SaaS |
| T17 | Is sleutelbeheer beschikbaar? | IaaS+PaaS+SaaS |
| T18 | Wordt data-encryptie toegepast? | IaaS+PaaS+SaaS |
| T19 | Is authenticatie-integratie beschikbaar? | IaaS+PaaS+SaaS |
| T22 | Zorgt de provider voor geïntegreerde beveiliging en compliance? | IaaS+PaaS+SaaS |
| Functionaliteit – Algemeen | | |
| T20 | Biedt de provider de mogelijkheid voor een privénetwerkverbinding tussen de on-premise-infrastructuur en de cloudinfrastructuur van de leverancier? | IaaS+PaaS |
| T21 | Zijn er meerdere opslagopties (tiers) beschikbaar? | IaaS+PaaS |
| T23 | Is de infrastructuur schaalbaar en elastisch? | IaaS+PaaS |
| T24 | Zijn er mogelijkheden voor geautomatiseerde provisioning en configuratie van de infrastructuur? | IaaS+PaaS |
| T25 | Ondersteunt de provider populaire besturingssystemen en applicaties? | IaaS+PaaS |
| T26 | Is Infrastructure as Code beschikbaar? | IaaS+PaaS |
| T27 | Is Everything as Code beschikbaar? | IaaS+PaaS |
| T28 | Zijn er tools voor geautomatiseerde deployment beschikbaar? (CI/CD) | IaaS+PaaS |

Onderzoekskader – Technische en functionele criteria (vervolg)

| Technische en functionele criteria | | |
|------------------------------------|--|------------|
| ID | Criterium | Toepassing |
| Functionaliteit – PaaS | | |
| T29 | Is de Serverless-functionaliteit beschikbaar? | PaaS |
| T30 | Is Managed Database beschikbaar? | PaaS |
| T31 | Is Managed Webserver beschikbaar? | PaaS |
| T32 | Is Managed Container Platform beschikbaar? | PaaS |
| T33 | Is Managed Data Platform beschikbaar? | PaaS |
| T34 | Is Managed Internet of Things (IoT) platform beschikbaar? | PaaS |
| T35 | Ondersteunt de provider veelgebruikte/gangbare ontwikkelingsplatforms? | PaaS |
| Functionaliteit – SaaS | | |
| T36 | Biedt de provider clouddiensten in SaaS-vorm aan (of ondersteunt deze)? | SaaS |
| T37 | Zijn er integratiemogelijkheden met andere software- en cloudservices? | SaaS |
| T38 | Zijn er mogelijkheden om de functionaliteit uit te breiden en aan te passen? | SaaS |
| T39 | Is SaaS Load Balancer beschikbaar? | SaaS |

Onderzoekskader – Juridische en organisatorische aspecten

De juridische en organisatorische aspecten (aangeduid met ID's die beginnen met een 'J') die gebruikt zijn tijdens de quickscan, zijn in onderstaande tabel weergegeven. Deze aspecten zijn gebaseerd op verplichtingen en aandachtspunten uit voor clouddiensten geldende wet- en regelgeving op algemeen bekende standaarden die zien op (informatie)beveiliging en gegevensbescherming. De juridische criteria zijn onderverdeeld in diverse categorieën die zien op verschillende juridische aspecten van clouddienstverlening. De criteria zijn gekozen met het oog op de toegankelijkheid van de informatie.

| Juridische en organisatorische aspecten | |
|---|---|
| ID | Criterium |
| Algemeen | |
| J1 | Nederlands recht (of ander passend EU-recht) van toepassing. |
| J2 | Geeft de provider inzicht in hoe hij omgaat met de Data Act? |
| J3 | Geeft de provider inzicht in hoe hij omgaat met de Data Governance Act? |
| J4 | Wat is de standaard totale aansprakelijkheid van de provider? |
| J5 | Wat is de standaard totale aansprakelijkheid van de ontvanger van de dienst? |
| J6 | CSP (of concern) is enkel actief binnen de EU. Indien nee, licht toe. |
| J7 | De leverancier biedt Incident Management als onderdeel van de dienstverlening. |
| J8 | De leverancier biedt Service Level Reporting als onderdeel van de dienstverlening. |
| Bescherming persoonsgegevens | |
| J9 | Is er een (eventueel naar Nederlands recht aangepaste) privacyverklaring beschikbaar? |
| J10 | Is er een verwerkersovereenkomst incl. dienstspecifieke informatie beschikbaar? Check of de volgende onderdelen aanwezig zijn: (i) Onderwerp en duur van verwerking, (ii) Aard en doel van de verwerking, (iii) Soort persoonsgegevens. |
| J11 | Is er beleid omtrent cookies beschikbaar? |
| J12 | Is er een Data Protection Impact Assessment (DPIA) beschikbaar? |
| J13 | Is er een Data Transfer Agreement (DTA) beschikbaar? |
| J14 | Indien van toepassing, is er sprake van een geldig doorgiftemechanisme (in het bijzonder met de VS), bijvoorbeeld op grond van modelclausules? |

Onderzoekskader – Juridische en organisatorische aspecten (vervolg)

| Juridische en organisatorische aspecten | |
|---|--|
| ID | Criterium |
| <i>Zijn de volgende certificaten/verklaringen beschikbaar?</i> | |
| J15 | EU Cloud Code of Conduct |
| J16 | ISO 27018 |
| Intellectueel Eigendom (IE), bedrijfsgeheimen & data | |
| J17 | Is en blijft de ontvanger van de dienst rechthebbende c.q. eigenaar van het intellectuele eigendom en bedrijfsgeheimen die zijn opgeslagen op de clouddiensten van de provider? |
| J18 | Is en blijft de ontvanger van de dienst rechthebbende c.q. eigenaar van de gegevens (data) die zijn opgeslagen op de clouddiensten van de provider, in het bijzonder metagegevens en gebruiksgegevens? |
| J19 | Bevat de overeenkomst met de provider een beperking ten aanzien van het gebruik van gegevens (d.w.z. enkel ten behoeve van de uitvoering van de (cloud)dienst)? |
| Beveiliging & certificering | |
| J20 | Staat de provider het toe om de geografische locatie te kiezen waar de gegevens worden opgeslagen om te voldoen aan lokale IE- en gegevensbeschermingswetten? |
| <i>Zijn de volgende certificaten/verklaringen beschikbaar?</i> | |
| J21 | ISO 9001 |
| J22 | ISO 27001 |
| J23 | ISO 27017 |
| J24 | ISO 27701 |
| J25 | SOC1 (evt. ISAE3402) |
| J26 | SOC2 |
| J27 | SOC3 |
| J28 | SWIPO IaaS Code |
| J29 | NEN7510 |
| J30 | Baseline Informatiebeveiliging Overheid (BIO) |

Onderzoekskader – Juridische en organisatorische aspecten (vervolg)

| Juridische en organisatorische aspecten | |
|--|--|
| ID | Criterium |
| J31 | BIO Thema-uitwerking Clouddiensten |
| J32 | CSA STAR |
| Kunstmatige Intelligentie (AI) | |
| J33 | Biedt de provider duidelijke documentatie van AI-systeemfunctionaliteiten? |
| J34 | Heeft de provider een gedocumenteerd beleid omtrent het verantwoordelijk gebruik van AI? |
| Environmental, Social & Governance (ESG) | |
| J35 | Heeft de leverancier een gedocumenteerd beleid omtrent ESG? |
| <i>Zijn de volgende certificaten/verklaringen beschikbaar?</i> | |
| J36 | Climate Neutral Data Centre Pact (CNDCP) |

B3

Gehanteerde definities

Gehanteerde definities – Cloudservicemodellen

Gebruikte definities voor cloudservicemodellen, gebaseerd op The NIST Definition of Cloud Computing (2011)

| Servicemodel | Definitie |
|--------------|---|
| IaaS | Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). |
| PaaS | Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| SaaS | Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. |

Gehanteerde definities – Cloud-deploymentmodellen

Gebruikte definities cloud-deploymentmodellen, gebaseerd op The NIST Definition of Cloud Computing (2011)

| Deploymentmodel | Definitie |
|-----------------|--|
| Private cloud | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. |
| Community cloud | The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. |
| Public cloud | The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. |
| Hybrid cloud | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). |

B4

SIDN-casus

In deze casus zijn specifieke technische en functionele criteria in overweging genomen die reeds onderdeel waren van het onderzoekskader

Achtergrond en huidige situatie applicaties en infrastructuur

SIDN is een Nederlandse beheerder van domeinnamen. Op dit moment beheert SIDN ongeveer 6,3 miljoen geregistreerde domeinnamen. SIDN maakt gebruik van twee belangrijke applicaties voor het aanbieden van zijn diensten: het Domein Registratie Systeem (DRS) en het Domain Name System (DNS). Daarnaast biedt SIDN diensten aan zoals WHOIS, Merkbewaking en de RegCheck. Verder maakt SIDN intern gebruik van ondersteunende applicaties voor zijn bedrijfsvoering, zoals Finance en HR.

DRS 5, dat in 2010 door SIDN is gelanceerd, is op dit moment het meest gebruikte systeem voor domeinregistratie. Momenteel wordt DRS 5 door ongeveer 1075 registrars gebruikt. Er wordt samen met het Canadese CIRA gewerkt aan een opvolger van DRS 5: Fury.

Op dit moment beheert SIDN zijn eigen servers en een groot deel van de infrastructuur, waaronder hardware, netwerken, storage en besturingssystemen. Op basis van zijn sourcingstrategie, heeft SIDN de keuze gemaakt om het nieuwe systeem voor domeinregistratie te implementeren in de public cloud.

Specifieke technische en functionele criteria voor deze casus

Om te komen tot een selectie van een public cloudprovider, heeft SIDN criteria opgesteld die zijn gebaseerd op de sourcingstrategie die samen met een externe partij is opgesteld. Deze criteria zijn tevens gepubliceerd in een blogpost op de website van SIDN en in een memo. SIDN heeft een keuze gemaakt op basis van de destijds publiek beschikbare informatie, aangevuld met informatie die bij cloudproviders is opgevraagd en de marktkennis van een externe partij.

Het onderzoekskader dat voor het quickscan-onderzoek is gebruikt, is breder dan de door SIDN gehanteerde set van criteria om te komen tot een selectie van een cloudprovider.

De voorliggende analyse is uitgevoerd op basis van de relevante technische en functionele criteria voor deze casus, en op basis van dezelfde informatie als voor de generieke analyse uit hoofdstuk 2. De resultaten van de analyse van deze casus zijn opgenomen in de tabel op de volgende pagina.

Voor deze casus beperkt de analyse zich tot de technische en functionele criteria en de juridische aspecten. Daarnaast heeft SIDN nog strategische criteria gedefinieerd die specifiek op SIDN van toepassing zijn. Deze zijn niet meegenomen in de analyse van deze casus, omdat deze organisatiespecifiek zijn en in dit quickscan-onderzoek niet gewogen kunnen worden op basis van de informatie uit het onderzoekskader.

De analyse voor deze casus laat gaps zien tussen het aanbod van Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers

Analyse van een specifieke set aan criteria gerelateerd aan deze casus ter overweging bij de keuze voor een publieke cloudprovider

| ID | Criterium | Microsoft Azure | Amazon Web Services | Google Cloud Platform | T-Systems Open Telekom Cloud | Orange Flexible Engine | OVHcloud | IONOS | Scaleway | KPN CloudNL | Leaseweb | ODC-Noord |
|-----|---|-----------------|---------------------|-----------------------|------------------------------|------------------------|----------|-------|----------|-------------|----------|-----------|
| T2 | Biedt de provider wereldwijd diensten aan? | | | | | | | | | | | |
| T4 | Zijn er datacenters in Europa beschikbaar? | | | | | | | | | | | |
| T7 | Heeft de provider concrete doelstellingen en maatregelen m.b.t. duurzaamheid? | | | | | | | | | | | |
| T11 | Hoeveel nieuwe clouddiensten heeft de provider afgelopen jaar (2023) uitgebracht? | | | | | | | | | | | |
| T12 | Is DDOS-beveiliging beschikbaar? | | | | | | | | | | | |
| T14 | Is Disaster Recovery beschikbaar? | | | | | | | | | | | |
| T15 | Is ransomwarebeveiliging beschikbaar? | | | | | | | | | | | |
| T16 | Biedt de provider monitoring tools om wijzigingen van resources overzichtelijk te maken voor klanten? | | | | | | | | | | | |
| T17 | Is sleutelbeheer beschikbaar? | | | | | | | | | | | |
| T18 | Wordt data-encryptie toegepast? | | | | | | | | | | | |
| T19 | Is authenticatie-integratie beschikbaar? | | | | | | | | | | | |

De analyse voor deze casus laat gaps zien tussen het aanbod van Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers

| Analyse van een specifieke set aan criteria gerelateerd aan deze casus ter overweging bij de keuze voor een publieke cloudprovider | | | | | | | | | | | | |
|--|---|-----------------|---------------------|-----------------------|------------------------------|------------------------|----------|-------|----------|-------------|----------|-----------|
| ID | Criterium | Microsoft Azure | Amazon Web Services | Google Cloud Platform | T-Systems Open Telekom Cloud | Orange Flexible Engine | OVHcloud | IONOS | Scaleway | KPN CloudNL | Leaseweb | ODC-Noord |
| T22 | Zorgt de provider voor geïntegreerde beveiliging en compliance? | | | | | | | | | | | |
| T24 | Zijn er mogelijkheden voor geautomatiseerde provisioning en configuratie van de infrastructuur? | | | | | | | | | | | |
| T26 | Is Infrastructure as Code beschikbaar? | | | | | | | | | | | |
| T27 | Is Everything as Code beschikbaar? | | | | | | | | | | | |
| T28 | Zijn er tools voor geautomatiseerde deployment beschikbaar? (CI/CD) | | | | | | | | | | | |
| T29 | Is de Serverless-functionaliteit beschikbaar? | | | | | | | | | | | |
| T30 | Is Managed Database beschikbaar? | | | | | | | | | | | |
| T32 | Is Managed Container Platform beschikbaar? | | | | | | | | | | | |
| T39 | Is SaaS Load Balancer beschikbaar? | | | | | | | | | | | |
| J1 | Nederlands recht (of ander passend EU-recht) van toepassing? | | | | | | | | | | | |
| J9 | Is er een (eventueel naar Nederlands recht aangepaste) privacyverklaring beschikbaar? | | | | | | | | | | | |

De analyse voor deze casus laat gaps zien tussen het aanbod van Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers

Analyse van een specifieke set aan criteria gerelateerd aan deze casus ter overweging bij de keuze voor een publieke cloudprovider

| ID | Criterium | Microsoft Azure | Amazon Web Services | Google Cloud Platform | T-Systems Open Telekom Cloud | Orange Flexible Engine | OVHcloud | IONOS | Scaleway | KPN CloudNL | Leaseweb | ODC-Noord |
|-----|--|-----------------|---------------------|-----------------------|------------------------------|------------------------|----------|-------|----------|-------------|----------|-----------|
| J10 | Is er een verwerkersovereenkomst incl. dienstspecifieke informatie beschikbaar?. | | | | | | | | | | | |
| J11 | Is er beleid omtrent cookies beschikbaar? | | | | | | | | | | | |
| J12 | Is er een DPIA beschikbaar? | | | | | | | | | | | |
| J13 | Is er een Data Transfer Agreement (DTA) beschikbaar? | | | | | | | | | | | |
| J14 | Indien van toepassing, is er sprake van een geldig doorgiftemechanisme (in het bijzonder met de VS), bijvoorbeeld op grond van modelclausules? | | | | | | | | | | | |
| J15 | EU Cloud Code of Conduct | | | | | | | | | | | |
| J16 | ISO 27018 | | | | | | | | | | | |
| J22 | ISO 27001 | | | | | | | | | | | |
| J23 | ISO 27017 | | | | | | | | | | | |
| J24 | ISO 27701 | | | | | | | | | | | |

B5

**Scenario's voor het
kiezen van een
Europese/Nederlandse
cloudprovider**

Naar aanleiding van de gapanalyse zijn vier scenario's opgesteld voor het afnemen van clouddiensten bij een Europese/Nederlandse cloudprovider

Scenario's voor het afnemen van diensten bij Europese/Nederlandse cloudproviders

Naar aanleiding van de SIDN-casus is onderzocht welke generieke scenario's voor organisaties bestaan voor het afnemen van diensten bij Europese/Nederlandse cloudproviders.

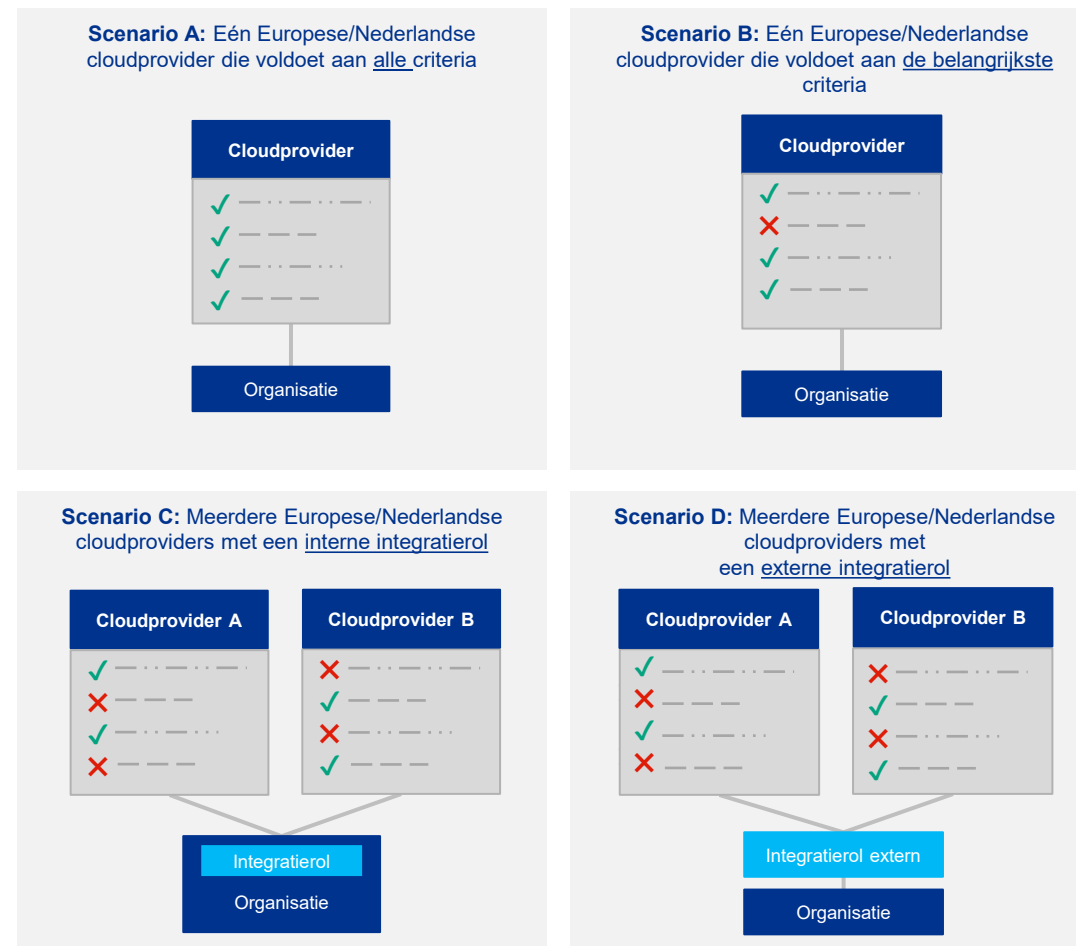
Uit de gapanalyse blijkt dat op dit moment gaps bestaan tussen het aanbod van Europese/Nederlandse cloudproviders en het aanbod van de Amerikaanse hyperscalers. Zo worden Everything-as-a-Code en geïntegreerde compliance tools niet door alle Europese/Nederlandse providers aangeboden. Individuele organisaties moeten zelf vaststellen of de geïdentificeerde gaps invloed hebben op de organisatiespecifieke criteria en of daarmee een keuze mogelijk is voor een Europese/Nederlandse cloudprovider.

Er zijn vier scenario's opgesteld om nader vast te stellen welke gevolgen de keuze voor een Europese/Nederlandse cloudprovider kan hebben voor een organisatie. Voor ieder scenario zijn voordelen, nadelen en inpassingsmaatregelen geïdentificeerd.

Voor het afnemen van clouddiensten bij Europese/Nederlandse cloudproviders zijn de volgende scenario's opgesteld:

- Eén Europese/Nederlandse cloudprovider die voldoet aan alle specifieke criteria.
- Eén Europese/Nederlandse cloudprovider die voldoet aan de belangrijkste criteria.
- Meerdere Europese/Nederlandse cloudproviders met een interne integratierol.
- Meerdere Europese/Nederlandse cloudproviders met een externe integratierol.

De uitwerking van deze scenario's is op de volgende pagina's te vinden. De keuze voor een van deze scenario's zal impact hebben op de organisatie die de clouddiensten afneemt. Het is niet ondenkbaar dat de uitvoering hiervan een kosten-opdrijvend effect heeft.



De twee scenario's waarbij diensten worden afgenomen van één Europese/Nederlandse cloudprovider vragen om inpassingsmaatregelen

Scenario A: Eén Europese/Nederlandse cloudprovider die voldoet aan alle criteria

Beschrijving van dit scenario

De criteria voor de selectie van een cloudprovider verschillen per organisatie. Dit scenario is van toepassing op organisaties waarbij één Europese/Nederlandse cloudprovider voldoet aan alle criteria die een organisatie stelt.

Voor organisaties waarbij op dit moment nog geen cloudprovider aan alle criteria voldoet, is dit scenario (nog) niet van toepassing. Daarnaast hebben meerdere Europese/Nederlandse providers criteria die nu nog niet worden ingevuld, wel op hun roadmap staan. In de toekomst zou het dus mogelijk kunnen zijn dat een Europese/Nederlandse cloudprovider ook voor organisaties waarvan de criteria nu nog niet gedekt worden, zal voldoen en dit scenario alsnog van toepassing wordt.

Implicaties voor de bedrijfsvoering en organisatie

Op basis van dit scenario worden geen specifieke wijzigingen in bedrijfsvoering en benodigde rollen in de organisatie voorzien, los van de rollen die in algemene zin noodzakelijk zijn in een organisatie voor het afnemen van clouddiensten.

Analyse scenario

Het productaanbod van Europese/Nederlandse cloudproviders is over het algemeen minder uitgebreid dan dat van de Amerikaanse hyperscalers. Toch is het voor organisaties waarvan de specifieke criteria overeenkomen met het geleverde productaanbod mogelijk om te kiezen voor een Europese/Nederlandse cloudprovider. Daarnaast blijven de Europese/Nederlandse cloudproviders nieuwe functionaliteiten ontwikkelen zoals vermeld op de roadmaps van deze partijen.

Scenario B: Eén Europese/Nederlandse cloudprovider die voldoet aan de belangrijkste criteria

Beschrijving van dit scenario

In dit scenario kiest een organisatie voor één Europese/Nederlandse cloudprovider die kan voldoen aan de belangrijkste technische en functionele criteria, maar niet aan alle criteria.

Implicaties voor de bedrijfsvoering en organisatie

De organisatie zal een keuze moeten maken met betrekking tot de criteria die niet ingevuld kunnen worden door de gekozen cloudprovider. Een organisatie heeft hiervoor de volgende mogelijkheden:

1. Een organisatie kan de missende criteria zelf in te vullen, wat betekent dat hiervoor additionele kennis in huis moet worden gehaald of dat bestaande rollen hiervoor vrijgemaakt en eventueel getraind moeten worden.
2. Ook is het mogelijk om de missende criteria door een externe partij te laten uitvoeren, waarbij integratie van deze partij in de organisatie en de cloudprovider noodzakelijk is.
3. Ten slotte kan de organisatie overwegen om de missende criteria te schrappen.

Analyse scenario

Op basis van de analyse lijkt het erop dat Europese/Nederlandse cloudproviders op dit moment op hoofdlijnen kunnen voldoen aan een groot aantal criteria. Bij Europese/Nederlandse providers ontbreken momenteel functionaliteiten zoals Everything-as-a-Code of geïntegreerde beveiligings- en compliance tooling. Dit betekent bijvoorbeeld dat de organisatie zelf meer deploymentactiviteiten voor applicaties moet uitvoeren, en ook meer werkzaamheden moet uitvoeren om tot een geïntegreerd beeld van de compliance in de cloudomgeving te komen.

De twee scenario's met waarbij diensten worden afgenomen van meerdere Europese/Nederlandse cloudproviders vragen om integratiemaatregelen

Scenario C: Meerdere Europese/Nederlandse cloudproviders met een interne integratierol

Beschrijving van dit scenario

In dit scenario kiest een organisatie voor een combinatie van twee of meerdere Europese/Nederlandse cloudproviders, die gezamenlijk alle technische en functionele criteria afdekken. Een belangrijk kenmerk van dit scenario is dat de afnemer een deel van de clouddiensten van de ene provider afneemt, en een ander deel van de clouddiensten van een andere provider.

Een gevolg van de keuze voor meerdere providers is dat clouddiensten door de afnemer worden geïntegreerd. In dit scenario wordt deze integratie door de organisatie zelf uitgevoerd.

Een keuze voor meerdere cloudproviders kan leiden tot het toevoegen van nieuwe criteria, bijvoorbeeld de mate waarin een cloudprovider ondersteuning biedt bij integratie met diensten van een andere cloudprovider en verdere portabiliteit.

Implicaties voor de bedrijfsvoering en organisatie

Het gebruik van twee of meerdere cloudproviders heeft tot gevolg dat organisaties ook intern kennis van en ervaring met twee (of meer) cloudplatformen moeten opbouwen. Daarom past dit scenario in de praktijk alleen bij relatief grote organisaties of organisaties met zeer specifieke behoeften. Doordat de organisatie de integratierol op zich neemt, dient deze over kennis van en ervaring met cloudintegratie te beschikken (bijvoorbeeld met betrekking tot rollen voor integratiemanagement en extra leveranciersmanagement). Sturing geven aan verschillende cloudproviders voor verschillende functionaliteiten zorgt voor extra complexiteit.

Analyse scenario

Het scenario waarbij de organisatie zelf de integratierol vervult wanneer er voor meerdere Europese cloudproviders wordt gekozen, zorgt voor extra benodigde resources en controlemechanismen, en daarmee hogere kosten.

Scenario D: Meerdere Europese/Nederlandse cloudproviders met een externe integratierol

Beschrijving van dit scenario

De beschrijving van dit scenario is in feite gelijk aan die van scenario C, met dien verstande dat in scenario D de integratierol niet wordt uitgevoerd door de organisatie zelf, maar door een externe partij.

De externe integratiepartner is hierbij verantwoordelijk voor het vertalen van behoeften van de organisatie naar de cloudproviders en voor het uitvoeren van de functionele en technische integratie van de clouddiensten. Ook kan de externe integratiepartner (deels) het contract- en leveranciersmanagement uitvoeren.

Implicaties voor de bedrijfsvoering en organisatie

Ook in dit scenario wordt gebruikgemaakt van meerdere cloudproviders, waarbij de organisatie kennis van en ervaring met deze cloudplatformen intern moet opbouwen.

Het aansturen van een integratiepartner vraagt van de organisatie zowel een duidelijke behoeftestelling als een heldere governance hiervoor.

Analyse scenario

Het scenario waarbij de organisatie kiest voor twee of meerdere Europese/Nederlandse cloudproviders met een externe integratierol, zorgt ervoor dat de organisatie zich kan blijven focussen op haar kerntaken terwijl de integratiepartner ervoor zorgt dat de gestelde criteria worden ingevuld. Een nadeel van dit scenario kan zijn dat het gebruik van verschillende cloudproviders en het inhuren van een integratiepartner extra kosten met zich meebrengen.



kpmg.com/socialmedia

Dit rapport (het 'Rapport') is opgesteld voor het ministerie Economische Zaken ('EZ') door KPMG Advisory N.V. in verband met een onderzoek naar het dienstenaanbod tussen Europese en Nederlandse en de Amerikaanse hyperscale cloudproviders. Dit Rapport is het resultaat van een zogeheten quickscan en bevat geen definitieve conclusies.

De informatie in dit Rapport weerspiegelt informatie en de analyse daarvan per de datum van dit Rapport. Deze informatie is aan verandering onderhevig. Bij het opstellen van dit Rapport hebben wij vertrouwd op de juistheid en volledigheid van de informatie afkomstig uit openbare bronnen of van derden, informatie verstrekt door of namens EZ of informatie welke anderszins door ons is geanalyseerd, zonder deze onafhankelijk te hebben geverifieerd. Wij aanvaarden geen aansprakelijkheid en/of verantwoordelijkheid voor dergelijke informatie en, voor zover betrekking hebbend op door EZ verstrekte informatie, is EZ hiervoor verantwoordelijk.

De door KPMG Advisory N.V. uitgevoerde werkzaamheden behelzen geen audit of review van de in het Rapport opgenomen informatie. Wij benadrukken dan ook dat wij geen opinie geven, noch enigerlei vorm van zekerheid verstrekken ten aanzien van de informatie in dit Rapport.

KPMG Advisory N.V. aanvaardt geen enkele aansprakelijkheid voor haar werkzaamheden, voor het Rapport of voor oordelen, bevindingen, aanbevelingen of opinies die wij gevormd hebben, anders dan jegens EZ. KPMG Advisory N.V. aanvaardt geen aansprakelijkheid jegens enige andere partij als gevolg van verstrekking van het Rapport aan een dergelijke partij.

Dit Rapport mag alleen in zijn geheel worden gelezen en mag uitsluitend worden gebruikt of openbaar worden gemaakt in overeenstemming met de overeengekomen doeleinden en voorwaarden. De bijlagen vormen een onlosmakelijk onderdeel van het Rapport en moeten in samenhang met de hoofdtekst worden gelezen.

© 2024 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Document Classification: KPMG Confidential