Kernbevindingen | Multistakeholderbijeenkomst Digitale Soevereiniteit

Huys Clingendael, 8 juli 2024

Op 8 juli 2024 hostten Instituut Clingendael en Internet Society Nederland (ISOC NL) een multistakeholderbijeenkomst over digitale soevereiniteit. De bijeenkomst beoogde concrete stappen te identificeren voor overheden, bedrijven en andere belanghebbenden die invulling geven aan de ambitie van digitale open strategische autonomie op het gebied van clouddiensten.

De paneldiscussie bracht zo'n 35 deelnemers van de overheid, bedrijfsleven en maatschappelijke organisaties bijeen op Huys Clingendael, plus ongeveer 100 deelnemers online. In de twee workshops die volgden bespraken de in-Huys deelnemers de thema's: (1) Data Soevereiniteit: Wat willen we beschermen?; en (2) Naar een Europese Bijenkorf Cloud Megascaler.

Dit beknopte verslag presenteert de belangrijkste bevindingen, vragen en vervolgstappen.
Omdat discussie plaats vond onder de Chatham House Rule zijn namen weggelaten.

<u>Data Soevereiniteit: Wat willen we beschermen?</u>

- **Beschikbaarheid**: Wat gebeurt er als je een dag, een week, of zelfs nooit meer toegang hebt tot je data?
    - Het risico van verlies van toegang tot essentiële data benadrukt de noodzaak van digitale soevereiniteit, vooral in de cloud.
    - Dominante, niet-Europese cloud-aanbieders zoals Microsoft Azure, Amazon AWS of Google Cloud Platform bieden mogelijk niet de gewenste volledige controle over Europese, kritische data.
    - Maak een risico-analyse van langdurig verlies van toegang tot data op basis van de afhankelijkheid van niet-Europese cloud-aanbieders zoals Microsoft Azure, Amazon AWS of Google Cloud Platform dat kan leiden tot verlies van controle over kritieke data. Overweeg hierbij het voorbeeld van Amazon, dat onlangs heeft aangekondigd €10 miljard te investeren in datacenters en logistieke infrastructuur in Duitsland, al blijft ieder Amerikaans bedrijf altijd onder Amerikaanse wetgeving vallen.

- **Bescherming**: Welke informatie willen we binnen Nederland houden en wat moeten we actief beschermen?
    - Er is geen eenduidig antwoord op de vraag welke sectoren, activiteiten en datatypes bescherming verdienen. Sommige sectoren, waaronder de militaire, delen van het openbaar bestuur, energie, en gezondheidszorg werden genoemd. Maar in hoeverre is er data binnen deze sectoren die wel naar (niet-Europese) cloud mag? Welke criteria kunnen helpen bij het definiëren van de grenzen van wat aanvaardbaar is? Bij welke dimensies (d.w.z. sectoren, of datatypes, of applicatie) moeten we beginnen om te analyseren?
    - Grote technologiebedrijven en geavanceerde toepassingen zoals "large language models" zijn afhankelijk van enorme hoeveelheden data om te functioneren en te verbeteren. Aangezien het voorkomt dat werknemers onbewust bedrijfsdata delen met systemen en AI-tools zoals ChatGPT, moeten we "onbetrouwbare" diensten niet verbieden in bepaalde contexten om onze data te beschermen?

  - Het is belangrijk om op metaniveau naar data te kijken: de waarde van inzichten uit persoonsgegevens op nationaal niveau moet niet worden onderschat. Zo kunnen regionale of nationale dynamieken worden afgeleid uit de massale gegevensverzameling en metadata-analyse. In hoeverre zijn dit zaken die de overheden zou moeten willen beschermen?
  - De overheid en bedrijven in kritieke sectoren zouden baat hebben bij het maken van risicobeoordelingen over het onbewust delen van bedrijfsdata met AI-tools. Er zijn tools die automatisch bescherming bieden tegen ongewenst datadelen en die in bedrijfsprocessen geïntegreerd kunnen worden om data-integriteit te waarborgen.

- **Kijken naar oplossingen**
  - Een gebalanceerde aanpak die zowel bescherming als efficiënte verwerking van data combineert, is noodzakelijk. Dit biedt niet alleen zekerheid en controle, maar stimuleert ook innovatie en efficiëntie door Europese spelers.
  - Als alternatief voor het gebruik van Microsoft door de overheid als cloud systeem, kunnen we overwegen om een Europese “Bijenkorf” Cloud Megascaler te ontwikkelen in plaats van te vertrouwen op de big tech hyperscalers. Dit zou een strategische stap zijn om de controle en soevereiniteit over onze data te waarborgen, vooral voor cruciale sectoren zoals de overheid, gemeentes en ziekenhuizen.

Naar een Europese Bijenkorf Cloud Megascaler

- **Scope-definitie**
  - Een alles-in-een pakket zou minstens vijf essentiële diensten moeten bevatten, met name: S3 object storage; Infrastructure as Code (IaC); Kubernetes; Identity and Access Management (IAM); and Database Management System (DMS).[i] Mogelijk aangevuld met AI-systemen.
  - Dit pakket moet voldoen aan de hoogste standaarden van veiligheid en interoperabiliteit. Overweeg aanvullingen met minder essentiële clouddiensten om aan de toekomstige eisen van de markt te voldoen.
  - Het is nog onduidelijk welke Nederlandse en andere Europese bedrijven interesse hebben om dit voorstel te ontwikkelen.
  - De overheid kan de creatie van een Bijenkorf Cloud Megascaler aanmoedigen door proto-typing aan de hand van heldere criteria te stimuleren, en afname te garanderen als een succesvol prototype gecreëerd is.
  - Als de Bijenkorf Cloud Megascaler afnemers werkelijk wil ‘ontzorgen’, zou het één juridische entiteit moeten zijn die verantwoordelijk gehouden kan worden
  - Zou er één ‘Bijenkorf megascaler’ moeten zijn of meerdere?

- **Criteria en Uitdagingen voor een Duurzame Europese Bijenkorf Cloud**
  De ontwikkeling van een cloudoptie die Europese soevereiniteit centraal stelt, vereist meer duidelijkheid over de volgende criteria en uitdagingen:
  - Probleemstelling: Wie is de klant? Wat is de behoefte?
  - Kernprincipes: Vrij en open.
  - Interoperabiliteit: Gebruik van open standaarden en compatibel zijn met bestaande platformen.
  - Portabiliteit: Data en diensten moeten eenvoudig verplaatst kunnen worden
  - Voorkeursaanbesteding: open source.
  - Schaal: Hoe te garanderen dat zo een project een Europese schaal bereikt?

- Kennis: Controle op kennisbasis ook in combinatie met opleidingen.
- Voldoen aan Europese wet- en regelgeving.
- Transparantie in governance en eigenaarschap.
- Kapitaal/Investeerders: gezien het gebrek van groot 'venture capital' in Europa, hoe wordt zo een onderneming gefinancierd?
- Aanbestedingsregels: flexibiliteit voor overheden om Europese cloudoplossingen te kopen.

- **Rol van de overheid**
  - Het is de vraag of de overheid bovenstaande criteria zou moeten opleggen en handhaven, of dat het wenselijker is dat bedrijven zelf tot afspraken komen.
  - Het is de vraag welke welke mogelijkheden zijn er voor overheden om de Europese cloudmarkten te stimuleren, naast hun rol als toezichthouder en als (grote) klant.

- **Kosten en financiering**
  - Exit strategie voor bedrijven: migratie van huidige (Amerikaanse) cloud providers naar een Europees alternatief kost veel geld, dat vooral maatschappelijke organisaties niet direct voorhanden hebben. Kan de overheid financiering bieden om los te komen een bestaand contract en bijbehorende systemen? Met andere woorden: is er voldoende geld en kennis voor een exit strategie?
  - Amerikaanse hyperscalers zijn in eerste instantie vaak goedkoper dan de alternatieven. Maar als een bedrijf groeit, en nieuwe diensten nodig heeft en het cloudverbruik oploopt, komt de afnemer vaak voor een onaangename verrassing te staan. Hoe kunnen Europese bedrijven en organisaties aangemoedigd worden om direct voor een Europese cloud oplossing te kiezen?

- **Lessen uit het verleden**
  - We kunnen leren van eerdere Europese initiatieven, zoals de Europese zoekmachine (Qwant), FIWARE, en de EU DNS. Analyseer deze eerdere Europese initiatieven en ook Gaia-X, en bespreek waarom Gaia-X, ondanks de intentie om een Europees cloud-ecosysteem te creëren, als mislukt wordt beschouwd vanwege gebrekkige governance, onduidelijke doelen, complexiteit, en onvoldoende marktsteun. Deze initiatieven kunnen waardevolle lessen bieden, zowel in termen van wat werkt als wat niet werkt.
    - FIWARE: Ondanks technische innovaties, werd FIWARE gehinderd door gebrek aan commerciële adoptie.
    - EU DNS: Slaagde erin een robuuste infrastructuur te bieden, maar faalt vooralsnog in brede acceptatie vanwege de dominantie van bestaande spelers.
    - Gaia-X: De complexiteit, gebrekkige governance en onduidelijke doelstellingen leidden tot onvoldoende steun en vertragingen.
  - Waardevolle lessen voor het creëren van een nieuwe kampioen kunnen ook in andere sectoren gezocht worden. Waarom is Airbus bijvoorbeeld wel gelukt? Hoe vergaat het Rapidus, de Japanse inzet op een nieuwe kampioen voor de halfgeleiderindustrie van de toekomst?

- **Cloud en Klimaat**
  - De klimaatcrisis kan een impuls geven aan een Europese cloudoplossing. Een klimaatvriendelijkere Europese cloud Megascaler, zoals CODUS (Cloud Optimized

Data Use Strategies), kan een Unique Selling Point (USP) geven aan de Europese propositie
  - Het hergebruiken van warmte uit datacenters voor het verwarmen van woningen, scholen en andere gebouwen kan bijdragen aan duurzame energieoplossingen en het verminderen van de ecologische voetafdruk.

- **Stack Loskoppelen**
  - Hyperscalers zoals Microsoft, Google en Amazon houden de lagen van de (Cloud) stack graag bij elkaar: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). Het is ook mogelijk om de lagen van de stack los te koppelen. Het loskoppelen van deze lagen kan zorgen voor meer flexibiliteit en controle over de infrastructuur. Wanneer de lagen van de cloud stack losgekoppeld zijn, kunnen organisaties kiezen voor de beste oplossing per laag, in plaats van gebonden te zijn aan een enkel ecosysteem. Dit bevordert interoperabiliteit, vermindert vendor lock-in, en kan de veiligheid en efficiëntie verhogen. Het stelt organisaties ook in staat om sneller te reageren op veranderingen in de markt en technologische innovaties.

- **Bijenkorf Model(len)**
  - Een Bijenkorf Cloud Megascaler heeft als risico dat keuzevrijheid verloren gaat als er voor de 'winner-takes-all' model aanneemt. Zou de Megascaler beter als secundaire optie voor cloud fungeren in plaats van als primaire optie?
  - Suggesties voor alternatieve oplossingen zijn: (1) dat iedereen dezelfde APIs gebruikt; (2) een federatief model met een broker/agent.
  - Of moeten we juist van het verleden leren waarbij de afgelopen jaren het duidelijk is geworden dat het federatief model niet meer van toepassing is gezien de huidige geopolitieke stand van zaken met de opkomst van Big Tech en de invloed op het internationale speelveld?

---

[i] Toelichting bij de vijf essentiële diensten in een Alles-in-1 basispakket:

- S3 Object Storage: schaalbare en kostenefficiënte oplossing voor het opslaan en ophalen van grote hoeveelheden data. Het is ideaal voor back-up en archivering en biedt robuuste redundantie en hoge beschikbaarheid.
- Infrastructure as Code (IaC): Hiermee kunnen infrastructuren automatisch worden beheerd en voorzien via code. Dit verbetert de consistentie en efficiëntie en vermindert menselijke fouten door infrastructuur en configuratie als code te behandelen.
- Kubernetes: Dit open-source systeem automatiseert de deployment, scaling, en het beheer van "containerized" applicaties. Het biedt flexibiliteit en schaalbaarheid voor het draaien van applicaties in de cloud, wat essentieel is voor moderne microservices-architecturen.
- Identity and Access Management (IAM): Dit systeem beheert en controleert de toegang tot middelen en data in de cloud. Het is cruciaal voor het waarborgen van veiligheid en compliance door gebruikers en hun toegangsrechten te beheren.
- Database Management System (DMS): Een systeem dat gegevens efficiënt opslaat, ophaalt, beheert en organiseert en de gegevensintegriteit, veiligheid en toegankelijkheid garandeert.