

Autonomie uitbesteden? *Tegenstrijdig en noodzakelijk voor cloud*

ICT-Infrastructuur is chefsache. Onze minister-president wordt bevraagd als een overheidsnetwerk na 25 jaar onzichtbaar onder de grond zitten een technische storing heeft die net even te lang duurt. Hoe zit dat in uw organisatie? Hoeveel aandacht verdient uw soevereiniteit? En kunt u verantwoord mee in de beweging naar 'cloud'?

'Ik heb geen verstand van ICT'. Dat is wat ik vaak hoor in gesprekken met opdrachtgevers, bestuurders en producteigenaren; in ieder geval binnen de overheid. Ook in cloudvraagstukken wordt dit vaak gezegd. Te vaak, wat mij betreft. Externe factoren, de Oekraïne oorlog, economische wedloop tussen VS en China waar we letterlijk middenin zitten en de voortdurende cyber-wedloop maken dat 'soevereiniteit' een thema is. Het is zaak dat we 'genoeg verstand van ICT' in de bestuurskamer en bij opdrachtgevers opbouwen om verantwoord mee te bewegen met de tech-ontwikkeling naar meer cloud. Waar staan we?

Weet waar je staat in de cloud!

Soeverein ben je als je als middeleeuws heerser gewoon 'de baas bent' in je eigen gebied en onafhankelijk. Een soeverein weet waar zij of hij staat en heeft overzicht over het gebied. Echter, alleenheersers bestaan vooral op Netflix. Afgezien van Lodewijk de Veertiende (later dan de middeleeuwen) waren er weinig mensen echt soeverein. Iedereen is van allerlei anderen afhankelijk voor zijn bestaan. In onze hoogtechnologische samenleving is dat nog veel sterker het geval dan in de spreekwoordelijke tijd van ridders en koningen. Zij waren 80% soeverein en 20% afhankelijk. Wij zijn 80% enorm afhankelijk. Dat gaat niet veranderen. Soevereine Chefsache is dan dat je echt weet waar je afhankelijk van bent en daar richting aan kunt geven. Kunt u dat voor uw ict-infrastructuur? En maakt het daarbij uit of dit een cloud-infrastructuur is? De buitenwereld verwacht dat!

Cloud maakt ons minder soeverein; dus daar moeten we wat mee

Los van de details van wat we onder cloud, publieke cloud, cloud native technologie, hyperscaler en dergelijke verstaan; het is een ontwikkeling die ons afhankelijker maakt. Iedere technologische ontwikkeling maakt ons afhankelijker. Er komt een 'laag' bij. Zo proberen we de details en complexiteit van de nieuwe technologie te beheersen. Als de laag goed genoeg gestandaardiseerd is, als er externe experts zijn en controle mechanismes, dan kunnen we de laag uitbesteden. We nemen een abonnement, doen een verantwoorde aankoop of stappen in een partnership. Zelf doen, terug naar de middeleeuwse 80% zelf en 20% afhankelijk, is een illusie. Niemand maakt zijn eigen chips, niemand is eigenaar van alle glasvezelkabels die hij benut, niemand wekt zijn eigen elektriciteit op. Er zijn uitzonderingen, maar u bent vrijwel zeker niet zo'n uitzondering. De vraag is dus niet of we uitbesteden. De vraag is niet of we iets in de cloud doen. De vraag is hoe je dat verantwoord richting geeft. Opdrachtgevers ontkomen er niet aan te investeren in de basiskennis die daarvoor nodig is. Wie de benodigde soevereiniteit wil bereiken, zal dat moeten organiseren. Inzicht in de marktontwikkeling is daar een aspect van. Voor de opdrachtgever is het meer een kwestie van organisatie, dan een kwestie van technologie.

Marktpartijen staan te trappelen om u soeverein te maken

Aanbieders van cloud begrijpen de behoefte aan soevereiniteit. Het verbaast dus niet dat we bij de drie dominante Amerikaanse hyperscalers aanbiedingen voor 'soevereine cloud diensten' aantreffen. Hetzelfde geldt voor opkomende concurrenten die zich positioneren door hun klanten 'meer soevereiniteit' te bieden. Uiteraard is dat voor een deel marketing. Dat is gezond, want het leidt tot het juiste gesprek. Een deel van de oplossing zal van de aanbieders komen. Als opdrachtgever is het cruciaal om uw deel van het gesprek te voeren. Richting geven vereist kennis van het aanbod. Daarnaast is standaardisatie, certificering en weten op welke expert-oordelen u kunt bouwen, noodzaak. Nieuwe wet- en regelgeving wijst in dezelfde richting. Niemand koopt een auto die niet door de RDW gekeurd is. Helaas doen we dat voor ict-infrastructuur nog steeds te vaak en maar al te vaak laten we ons door de automobielfanaten in onze eigen organisaties verleiden tot onverstandige keuzes.

Het soevereine cloud-aanbod van marktpartijen is maximaal een derde van de oplossing. De eigen basiskennis en het goed benutten van externe oordelen moeten de andere twee derde zijn die daar een gezond tegenwicht aan bieden. Zo organiseer je soevereiniteit in een wereld vol met afhankelijkheden.



Sovereign cloud proposities,
hyperscalers en andere
(commerciele) dienstverleners



Eigen basiskennis en het zelf
kunnen richten en organiseren
van cloud



Weten welke certificeringen,
standaarden en externe oordelen
bevestiging bieden

Wet- en regelgeving komt ons langzaam te hulp en kun je niet afschuiven

Op deze drieslag van aanbod, eigen kennis en extern oordeel volgt wet- en regelgeving. Bestaande wetgeving voor (vitale) infrastructuur en regelgeving rond cybersecurity geldt uiteraard ook bij gebruik van cloudinfrastructuur. Specifieke wet- en regelgeving voor cloud komt daarbovenop. Wetgeving waaraan de aanbieders moeten voldoen, maar vooral ook wetgeving waar u als organisatie zelf aan moet voldoen en waarvoor u de verantwoordelijkheid niet kunt afschuiven. Dat vergroot de behoefte aan certificeringen en een governance die u zicht geeft op het in control zijn en blijven.

Belangrijke EU wetten op dit gebied die doorwerken in Nederland zijn: EU Data Act, GDPR (Avg), NIS2, CER en EU Cybersecurity Act. Onder die laatste ontwikkelt de EU certificeringsschema's waaronder het EUCS voor cloud computing. We mogen aannemen dat deze in het Nederlandse rijkscloudbeleid worden overgenomen en in ieder geval voor de (semi-)overheid essentieel worden. Deze wetten hebben invloed op de aanbieders, maar leggen ook allerlei verantwoordelijkheden bij u als opdrachtgever. Aanbieders moeten het bijvoorbeeld makkelijker maken om van leverancier te switchen (aldus EU Data Act). De lijst met belangrijke en kritieke organisaties die aan strengere cybersecurity maatregelen moeten voldoen wordt met NIS2 en CER sterk uitgebreid. Het betreft zowel groter private bedrijven als overheid. Tijdens het 'Securing Sovereignty' event van Capgemini wordt u bijgepraat over deze ontwikkelingen en krijgt u een doorkijkje in de soevereine cloud oplossingen die in de markt voorhanden zijn.

Waaruit bestaat het 'soevereine cloud' aanbod?

Naast marketing bestaan het soevereine cloud aanbod op het eerste gezicht uit veel technische termen. Zolang dat zo blijft, is het moeilijk om goed opdrachtgeverschap in te richten. Laten we proberen het aanbod met een niet-tech bril te bekijken.

- Soevereine cloud proposities zijn een contract; net als iedere andere uitbesteding.
- Een soevereine cloud propositie helpt u om steeds te weten waar u staat.
- Een soevereine cloud propositie kan uw data niet bekijken; u hebt de sleutels zelf.
- Een soevereine cloud propositie maakt het makkelijk om te wisselen van aanbieder.

Ten eerste: soevereine cloud is een contract

Juist om een eenzijdige tech-focus te voorkomen helpt het om te constateren dat soevereine cloud in de eerste plaats een contract is. Dat maakt meteen duidelijk dat we 80% afhankelijk zijn van anderen. Bij sterk gestandaardiseerde meer op public cloud gebaseerde vormen is het één contract; wel een ingewikkelde. Doet u meer zelf dan zijn het vaak veel contracten voor ieder deel een ander. Goed contractmanagement is dus essentieel. Weten welk contract voor welk aspect, weten welke partij welke verantwoordelijkheid heeft en weten welke verantwoordelijkheden u zelf behoudt.

Ten tweede: een soevereine cloud voorziening laat contine zien 'waar u staat'

Goede operationele soevereiniteit vereist dat u goede dashboards heeft die continu aangeven hoe de infrastructuur vandaag functioneert, inclusief de afhankelijkheden van anderen (zoals de netwerkaanbieder). Ten tweede wilt u na iedere verandering zien of het geheel nog aan de eisen en cybersecuritynormen voldoet. Een kwartaalrapportage op basis van globale service niveau KPI's is dan onvoldoende. Een goede soevereine cloud voorziening lost dit op met ingebouwde dashboards die steeds de actuele stand geven.

Ten derde: een soevereine cloud maakt uw data onzichtbaar voor pottenkijkers

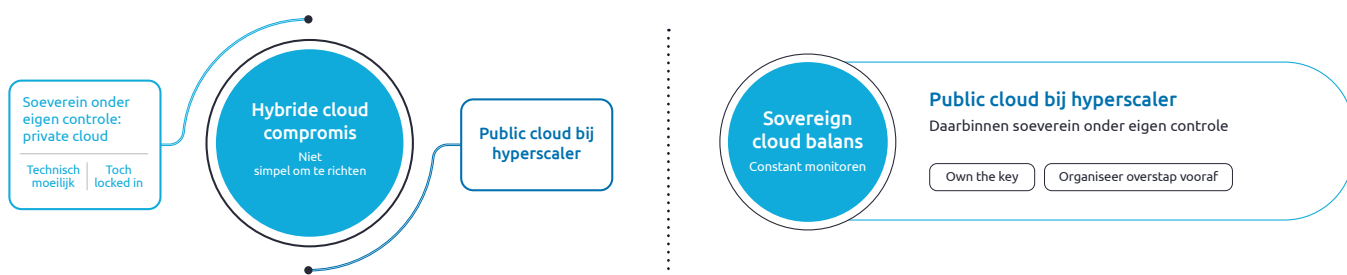
Data soevereiniteit betekent dat u er op kunt vertrouwen dat onbevoegden niet in uw informatie kunnen kijken en deze ook niet kunnen stelen. Grondige encryptie is daarvoor essentieel, evenals goede diensten voor het beheer van sleutels en wachtwoorden. Voor netwerkverkeer accepteren we dit inmiddels algemeen



(het slotje in de browser, met de achterliggende standaarden die regelmatig worden bijgewerkt). Voor verwerking in datacenters gaan de ontwikkelingen snel. De nieuwste soevereine cloudvoorzieningen werken met CPU's (chips) die intern veilige verwerking mogelijk maken. Het zogeheten confidential compute. In ons 'Securing Sovereignty' wordt u bijgepraat over dat soort ontwikkelingen. Binnen een aantal jaren zal dit gemeengoed zijn. Noodzakelijk, want het beschermt ons tegen de meer hardnekkige hardware gerichte aanvallen.

Tenslotte: soevereine cloud implementeert technologie 'inwisselbaar'

Technische soevereiniteit vereist tenslotte expertise. De aanbieders benutten technologie en standaarden. Veel daarvan is zelfs open source. Echter, als dit verkeerd geconfigureerd staat, dan levert het niet de beloofde voordelen. Het belang om lock-in te beperken ligt bij u als afnemer. Het is dus logisch dat het eigen expertise vraagt (aangevuld met externe ogen die dwingen) om cloudvoorzieningen zo standaard mogelijk te gebruiken. Overstappen naar een andere aanbieder zal nooit een 'druk op de knop' zijn, tenzij u twee verschillende operationele systemen naast elkaar in de lucht wilt houden. De technische kennis en goede werkprocessen, bijvoorbeeld rond geautomatiseerd testen, maken wel veel verschil om overstap naar andere aanbieders mogelijk te maken. Organisatie en techniek moeten er op ingericht zijn dat je voortdurend onderdelen aan het vervangen bent. Dat is de realiteit van de snelle technologie ontwikkeling en de voortdurende security wapenwedloop. Een opdrachtgever moet hiervoor zijn mensen en partners kunnen vertrouwen; maar het helpt als u er zelf ook op door kunt vragen!



Soevereine cloud als 'beter compromis'

In de eerste golf van het naar de cloud brengen van voorzieningen waren wendbaarheid, innovatie en schaalbaarheid belangrijker dan soevereiniteit. Dit verklaart ook waarom commerciële organisaties voor meer dan 50% gebruik maken van de publieke cloud bij de grote hyperscalers, terwijl overheidsorganisaties terughoudend blijven. Soevereiniteit is niet onbelangrijk voor een commercieel bedrijf, maar afgewogen tegen andere overwegingen minder dominant. Bij een echte onverwachte gebeurtenis zoals Covid, kijken we immers allemaal naar de overheid.

De logische volgende stap is om 'hybride' te gaan. Alles naar de publieke cloud wat kan. Voor wat over blijft op cloud gelijkende interne ict-infrastructuur gebruiken. Het besturen van zo'n best-of-both worlds is complex. Zonder expliciete aandacht is de soevereiniteit vaak minder goed dan we denken. Er zijn toch afhankelijkheden en de interne ict-infrastructuur voor de gevoelige voorzieningen blijkt ook niet veilig, vol met vendor lock-in en andere minder prettige kwesties.

De ervaring van de hyperscalers met het specifiek voor overheden of grote bedrijven inrichten van 'afgeschermd private cloud omgevingen' is daarbij op z'n best wisselend. Hybride combinaties en private clouds zijn compromissen met forse nadelen.

Het nu snelgroeiende soevereine cloud aanbod is een andere invulling van de balans. De basisgedachte is dat uw stukje cloud binnen een hyperscale cloud zodanig georganiseerd, beveiligd, dichtgetimmerd en gemonitord wordt dat u voldoende soevereiniteit terugkrijgt om in de nieuwe wereld uw eigen richting te bepalen.

Ook de middeleeuwse koning moest balanceren om te overleven; weet welke balans u kiest en hoe u er als overwinnaar uitkomt! Van harte welkom op ons 'Securing Sovereignty' event. U hoort er over ervaringen van anderen en wordt bijgepraat over recente ontwikkelingen.

OVER DE AUTEUR



Michael Stoelinga

Michael Stoelinga is Chief Architect Public Sector bij Capgemini. In deze rol combineert hij brede ervaring met digitalisering in de publieke sector, met een netwerk van klanten en collega's in en buiten Nederland. Omdat het effectief toepassen van cloud technologie voorwaardelijk is voor betere dienstverlening en vertrouwen in het functioneren van de overheid, is Michael intensief met dit onderwerp bezig.

✉ michael.stoelinga@capgemini.com

[in linkedin.com/in/mstoelinga](https://www.linkedin.com/in/mstoelinga)

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

www.capgemini.com



Get the future you want