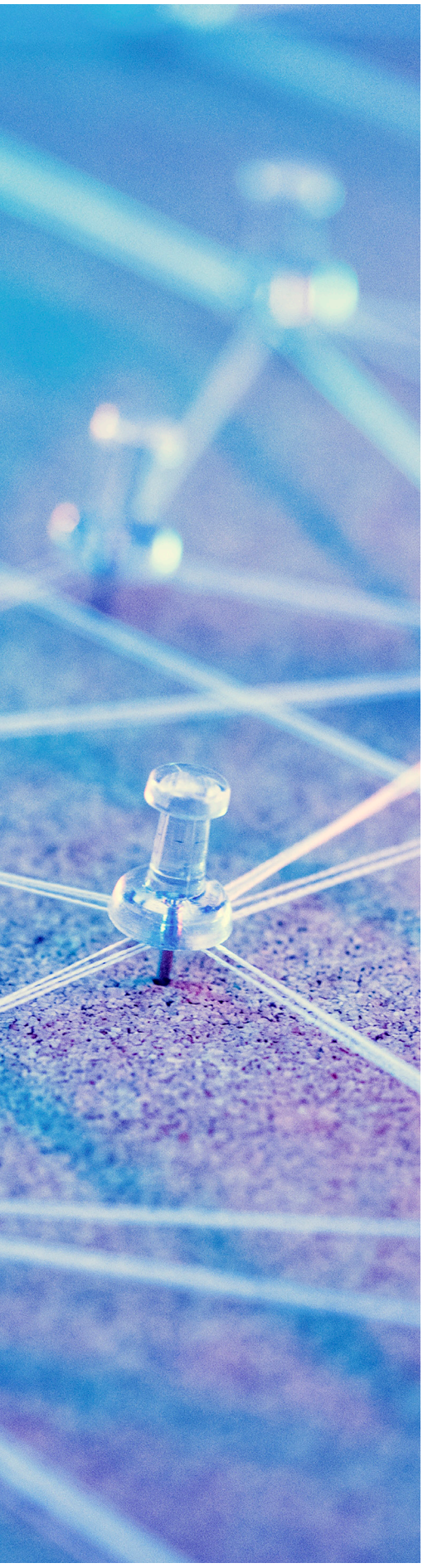
Dutch Cloud Community

Digitale Soevereiniteit

Whitepaper



01. Samenvatting

Met dit whitepaper over digitale soevereiniteit wil Dutch Cloud Community inzicht geven in de brede maatschappelijke discussie rondom dit thema. Hoe definiëren we een soevereine cloud? Welke factoren spelen een rol? En cruciaal: welke scenario's zijn er voor de toekomst? Wat zijn de consequenties van de keuzes die we als samenleving maken en welke kosten zijn hiermee gemoeid?

De Nederlandse cloud- internetsector is in gesprek met de overheid en de politiek om samen te werken aan een gebalanceerd beleid waarin de belangen van de burger, de privacy, maar ook de zelfstandigheid van ons land geborgd kunnen worden. Dit whitepaper brengt de risico's en afhankelijkheden in kaart en legt de basis voor vervolgstappen om de digitalisering van onze samenleving op een verantwoorde en evenwichtige manier voort te zetten.

Na een kort overzicht van de situatie waarin onze overheid zich nu bevindt ten opzichte van niet Europese clouddiensten kijken wij kort naar de voorgeschiedenis en hoe wij als land zo afhankelijk zijn geworden van deze diensten.

We staan vervolgens stil bij de risico's van de huidige situatie, op geopolitiek niveau, op de controle over onze data (en de gegevens van onze overheid en burgers) en de impact van de huidige koers op werkgelegenheid, onderwijs, belastinginkomsten en kosten.

Daarnaast biedt het whitepaper een voorstel voor duidelijke definities van de criteria waaraan een soevereine clouddienst zou moeten voldoen. Momenteel worden verschillende begrippen door elkaar gebruikt, waardoor belanghebbenden vaak niet dezelfde taal spreken. Eenduidigheid in deze discussie is essentieel.

Tenslotte benoemen we verschillende scenario's voor de toekomst:

- Doorgaan op de ingeslagen weg
- Een radicale breuk en een keuze voor 100% soeverein en open-source
- Een middenweg; een gebalanceerd, evenwichtig beleid waarin Nederland zichzelf minder afhankelijk kan maken, zonder al hetgeen dat er al is overboord te gooien.

En niet te vergeten:

- Hoe ziet de weg naar voren er dan uit?
- Welke stappen kunnen genomen worden door de Nederlandse cloud- en internetsector en door de overheid?
- Hoe kunnen wij samen werken aan de toekomst?

Inhoudsopgave

02. Introductie

Een constatering, die niet alleen door ons gemaakt wordt, maar door alle experts en door de overheid zelf: vanaf de dag dat de overheden clouddiensten gingen gebruiken zijn bijna al die diensten systematisch afgenomen bij de 3 grote Amerikaanse aanbieders van publieke clouddiensten: Microsoft, Amazon Web Services en Google.

De overheid heeft overeenkomsten gesloten over licenties en inkoopvoorwaarden met de drie grote Amerikaanse partijen, en voor de inkopers van landelijke, gemeentelijke en provinciale overheden, maar ook die van onderwijs- en zorginstellingen, is ‘de cloud’ eigenlijk synoniem voor Microsoft of AWS.

De afhankelijkheid van de Nederlandse overheid van het Amerikaanse aanbod is bijna totaal geworden.

Dit is een situatie die nooit beleidsmatig als zodanig is besloten.

Er is geen bewuste keuze gemaakt voor dit beleid. Het is organisch ontstaan, mede door het feit dat de overheid niet één opdrachtgever is maar een veelvoud aan CIO’s die min of meer zelfstandig hun inkoopbeleid vormgeven.

Er was tot 2024 ook geen aandacht voor de gevolgen van de keuzes die gemaakt zijn. Er is nooit een risicoanalyse gemaakt. Er is ook niet gesproken of gedebatteerd over de gevaren van de afhankelijkheid die hiermee ontstond. Het was gewoon zoals het was.

Pas in 2024 zijn de eerste vragen gesteld over de wenselijkheid van de ontstane situatie. Een belangrijke trigger hiervoor was het besluit van de beheerder van het .nl domein, SIDN, om hun Domein Registratie Systeem niet meer zelf te beheren maar volledig naar de cloud van Amazon Web Services te brengen. Hierdoor stelde de commissie Digitale Zaken van de Tweede Kamer voor het eerst een aantal scherpe vragen. Is het wel verantwoord om het hart van het Nederlandse internet in een Amerikaanse cloud te hangen? Is er geen Nederlandse partij die dit zou kunnen? Is er een inschatting gemaakt van de impact op de privacy van gebruikers? Is er een plan B voor als er een probleem zou zijn?

Toen begon duidelijk te worden dat SIDN geen uitzondering is. De initiatiefnota “Wolken aan de horizon” van Kamerleden Barbara Kathmann en Jesse Six Dijkstra in april schetste een ontluisterend beeld van een overheid die inmiddels volledig afhankelijk is geworden van een niet-Europese cloud en niet meer in staat is om zelfs haar eigen beleidsregels te volgen.

In 2024 is het debat aangewakkerd. Instituut Clingendael besteedde een Policy Briefing aan het onderwerp, experts zoals Bert Hubert schreven erover en Dutch Cloud Community zelf zocht het gesprek op met beleidsmakers en politici. Vanuit de kant van grote belanghebbenden zoals het bureau van de CIO Rijk (bij het ministerie van Binnenlandse Zaken), de Directie Digitale Economie van het

ministerie van Economische Zaken, maar ook de Vereniging van Nederlandse Gemeenten kwam er steeds meer aandacht voor dit onderwerp.

Op 15 januari 2025 verscheen het rapport “Het Rijk in de cloud. Donkere wolken pakken samen” van de Algemene Rekenkamer. De Rekenkamer keek naar het cloudgebruik van het Rijk en kwam tot conclusies die volledig overeenkomen met het bovenstaande:

Wij citeren:
“In dit onderzoek trekken we de volgende belangrijkste conclusies:

1. *Het Rijk heeft beperkt zicht op clouddiensten.*
2. *Het Rijk maakt onvoldoende strategische risicoafwegingen.*
3. *Het Rijk waarborgt onvoldoende de principes (digitale) soevereiniteit, continuïteit van de dienstverlening en de gegevensbescherming in 3 onderzochte public cloud-contracten.”*

Bij twee derde van de afgenomen diensten heeft nooit een risico-analyse plaatsgevonden, zelfs niet voor cruciale diensten zoals die van de Belastingdienst of paspoortuitgaven. In een kwart van de gevallen “weet men niet” welke clouddiensten gebruikt worden.

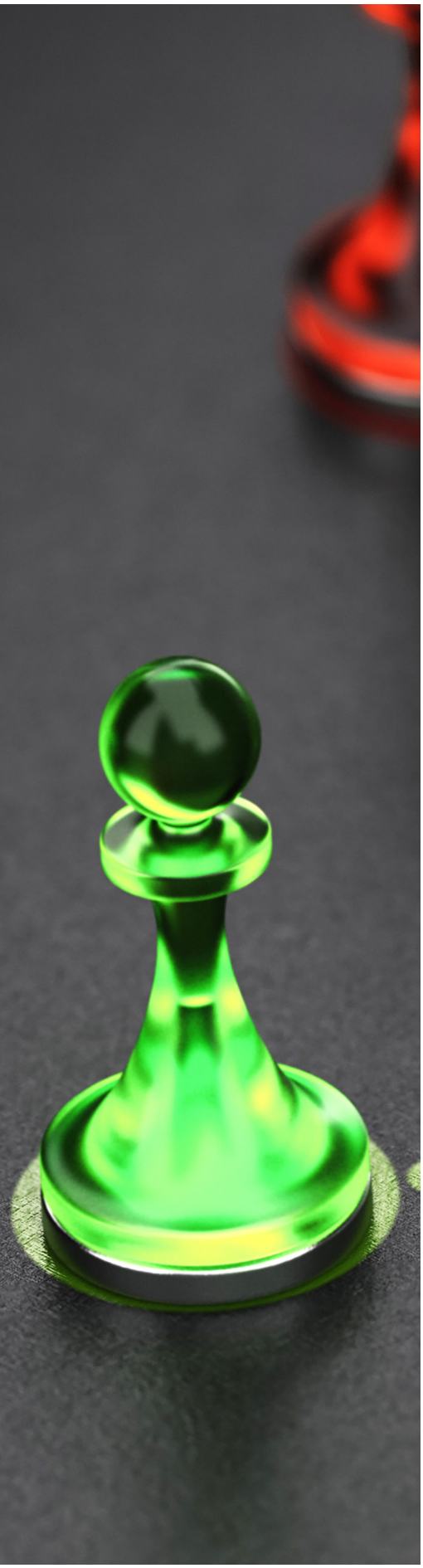
“We concluderen”, aldus het rapport, “dat de betreffende ministeries onvoldoende maatregelen nemen om de soevereiniteit, continuïteit van dienstverlening en gegevensbescherming te waarborgen in public cloud-contracten. Dit betekent dat het Rijk risico’s loopt, bijvoorbeeld als een cloudprovider failliet gaat. Het risico bestaat dat het Rijk producten of diensten voor burgers en bedrijven niet kan blijven leveren. Ook bestaat het risico dat gegevens van burgers en bedrijven onvoldoende beschermd zijn en kunnen worden misbruikt door kwaadwillenden en statelijke actoren.”

Het moge duidelijk zijn dat dit zo niet heel lang door kan gaan.

Met dit whitepaper wil Dutch Cloud Community, als brancheverenigingen van de Nederlandse hosting- en cloudsector, het perspectief van de Nederlandse industrie op het thema van Digitale Soevereiniteit toelichten.

Op 17 januari 2025, twee dagen na het rapport van de Algemene Rekenkamer, verscheen een brief van de Ministerraad aan de Tweede Kamer (waarin het kabinet overigens afwijkt van de gehanteerde soevereiniteit-definities zoals die worden gebruikt door de Algemene Rekenkamer). Dit geeft extra aanleiding om met dit whitepaper deze discussie te vervolgen.

Dit whitepaper wil de verschillende invalshoeken belichten die relevant zijn om te begrijpen waar de discussie over gaat en waarom het zo’n belangrijk onderwerp is geworden.



03. Digitale soevereiniteit, digitale autonomie, digitale onafhankelijkheid

Als branchevereniging van de Nederlandse cloud- en internetsector zijn wij diep betrokken bij de discussie rond digitale soevereiniteit. Wij proberen in dit debat op een constructieve manier de verschillende partijen te helpen om stappen te maken die de overheid kunnen helpen om, zonder afbreuk te doen aan wat er al gebouwd is, een balans te vinden waarin meer ruimte gevonden kan worden voor samenwerking met de eigen industrie.

Het doel van dit whitepaper is om te duiden waar de discussie om gaat: over welke definities kunnen alle stakeholders het eens worden? Wat zijn de verschillende aspecten die komen kijken bij dit thema? En belangrijk: welke scenario's zijn er voor de toekomst, wat zijn de gevolgen van de keuzes die wij als samenleving moeten maken en welke kosten horen daarbij?

Digitale soevereiniteit, digitale onafhankelijkheid, digitale autonomie: allemaal termen om een thema te benoemen dat heel lang ondergeschoven bleef en dat opeens center stage is geworden. Opeens is controle over onze digitalisering een onderwerp dat de politiek, de overheid en de media belangrijk vinden.

Er zijn meerdere reden waarom het thema opeens naar de voorgrond komt: De geopolitieke ontwikkelingen zorgen ervoor dat de hele EU zich opeens bewust is geworden van het belang van onafhankelijk blijven of worden van buitenlandse mogendheden.

Daaraan gelieerd is de bezorgdheid over de afhankelijkheid van een klein groepje hele grote techreuzen die we in Nederland en in de EU

hebben laten ontstaan en het gebrek aan een ‘Plan B’ voor het geval dat wij later van die afhankelijkheid af zouden willen.

Een derde reden mag gezocht worden in de alsmaar toenemende cyberdreigingen die bedrijf en burger steeds meer bezighouden.

Tot slot is er nog een vierde reden: het gunnen van grote projecten en investeringen aan Nederlandse en Europese partijen die daar klaar voor staan. Investeren in je eigen mensen en je eigen economie. Investeren in werkgelegenheid en het uitbouwen van de infrastructuur en het mogelijk maken voor de eigen industrie om zich verder te ontwikkelen.

Wij moeten in Nederland en Europa beginnen om de implementatie van deze technologieën aan onze eigen bedrijven te durven gunnen om daarmee de ontwikkeling en opschaling ervan mogelijk te maken.

Overheden en politici erkennen het belang van het waarborgen van data-soevereiniteit en het behouden van onafhankelijkheid van derde mogendheden. Het bevorderen van sterke Europese tech-bedrijven is een thema dat zowel door de Europese Commissie als door nationale overheden voortdurend wordt benadrukt. Desondanks lijkt het, wanneer er keuzes moeten worden gemaakt, alsof de Nederlandse (en Europese) industrie vaak onzichtbaar is.

Dutch Cloud Community heeft de waarheid niet in pacht en wij zijn ook niet een 100% neutrale partij. Wij zien dit whitepaper dan ook als een levend document, waarop wij de inbreng en de toevoegingen van anderen verwelkomen om het verder te laten groeien.

Dutch Cloud Community hoopt hiermee bij te dragen aan een belangrijk debat over de toekomst van digitalisering in ons land en onze maatschappij.

04. Aanleiding van de discussie – een stukje historie, wat eraan vooraf ging

Outsourcing als trend in de markt
[Algemene marktontwikkeling]

Rond 2015 was toepassing van clouddiensten sterk in opkomst. Het uitbesteden van IT was al zeer gebruikelijk. Maar wanneer we kijken naar twee elementen die in de kern van IT liggen dan blijkt de uitbestedingsgolf richting cloudgebaseerde diensten in 2015 nog maar net op gang te zijn gekomen. Verwerkingscapaciteit (servers) en gegevensopslag (storage) staan in zakelijk Nederland dan aan de vooravond van een groeiperiode. Op dat moment gaat cloud snel, maar het is toch vooral SaaS dat daar voorloper en beeldbepaler in is. De infrastructuur als zodanig doen we niet snel de deur uit en dat kan ook niet zomaar. Dat blijkt duidelijk uit de storage-situatie en in wat mindere mate uit hoe onze servers qua locatie geregeld zijn. Natuurlijk is het zo dat niet iedereen servers heeft of gebruikt. Maar als ze er zijn, staan ze per definitie niet alleen in huis. Vooral hosting is in 2015 aan de orde. Cloud-gebaseerde verwerkingscapaciteit (IaaS) is nog niet mainstream. Langzaam maar zeker zette de trend naar het buitenshuis regelen van basale infrastructuur services zich door. Datacenters, hosters en aanbieders van cloud infrastructuur speelden hier vroegtijdig op in. Toch was de beweging langzaam.

Het gebruik van clouddiensten is in de afgelopen 20 jaar sterk gestegen. Los van de details is met name de overall ontwikkeling opvallend. Vrijwel elke organisatie (groot of klein) wordt vroeg of laat geconfronteerd met het gebruik of de overweging van clouddiensten. Een belangrijke fase in de ontwikkeling is de verschijning van clouddiensten voor meer bedrijfskritische toepassingen, waarmee het 'hart' van menig IT-organisatie wordt geraakt door deze ontwikkeling. De algemene grondhouding ten aanzien van cloud ontwikkelt zich op dat moment van 'relatief terughoudend' naar 'breed geaccepteerd'.

Cloud is inmiddels niet meer weg te denken uit het aanbod van oplossingen en diensten door IT-bedrijven. Het groeit snel, zowel voor minder kritische als essentiële applicaties. Lokale IT-bedrijven verwerken ook steeds vaker cloud-gebaseerde oplossingen in hun aanbod. SaaS-gebaseerde applicaties lopen hierbij voorop. Zo verweven steeds meer lokale aanbieders in hun aanbod de oplossingen van public cloud platforms als vervanging van of aanvulling op private cloud-oplossingen, waarbij hun lokale aanwezigheid en vertrouwensrelatie een belangrijke extra is. In de mix van bedrijven zien we dat bedrijven die cloud-diensten aanbieden, vaak jonger en kleiner (in aantal fte's) zijn dan andere bedrijven. We bevinden ons in deze jaren op een kantelpunt van het aanbod in de IT-markt. Cloud begint meer en meer de standaard of het uitgangspunt te zijn in de ontwikkeling van applicaties en diensten. Die leveranciers die cloud-gerelateerd aanbod naast zich laten liggen, lopen op termijn het risico om langs de zijlijn te staan. Waar cloud-gebaseerd aanbod in eerste instantie voldoende was voor aanbieders om relevant te blijven, is nu het moment aangebroken dat specialisatie een vereiste is. Wanneer we kijken naar bedrijven met als primaire rol IT-dienstverlener (MSP, reseller, VAR), Internet Service Provider of consultant met in haar dienstenpakket

beheersdiensten op IT-infrastructuur, dan valt een aantal zaken op. Meer dan de helft van de deze bedrijven heeft het beheer van IT-infrastructuur in hun dienstenportfolio. In de onderkant van het segment (zzp'ers en zeer kleine bedrijven) en bij bedrijven met 10 tot 50 fte ligt meer focus op deze diensten dan bij grote bedrijven. Dit bevestigt het beeld dat veel kleinere MKB-bedrijven hun infrastructuur uitbesteden aan een bekende, vertrouwde ICT-professional. Als deze bedrijven elkaar ontgroeien, wordt vaak de stap gezet naar een wat grotere, professionelere ICT-dienstverlener. Dit is

de reden dat het segment tussen 2 en 10 werknemers iets achterblijft. Middelgrote ICT-dienstverleners bedienen vaak meerdere verticale segmenten. De zorg en de overheid worden het meest genoemd in zowel het MKB (in dit geval lokale zorg en overheid) als het grootzakelijk segment (provinciale en centrale overheid en grotere zorginstellingen). In het MKB worden ook de segmenten onderwijs, zakelijke dienstverlening en de financiële sector genoemd. In de grootzakelijke markt is meer aandacht voor de zakelijke dienstverlening en de industrie, gevolgd door de financiële markt en retail. In zowel het MKB als de grootzakelijke markt blijven de sectoren agro, leisure en non-profit achter als aandachtsgebied voor de aanbieders.

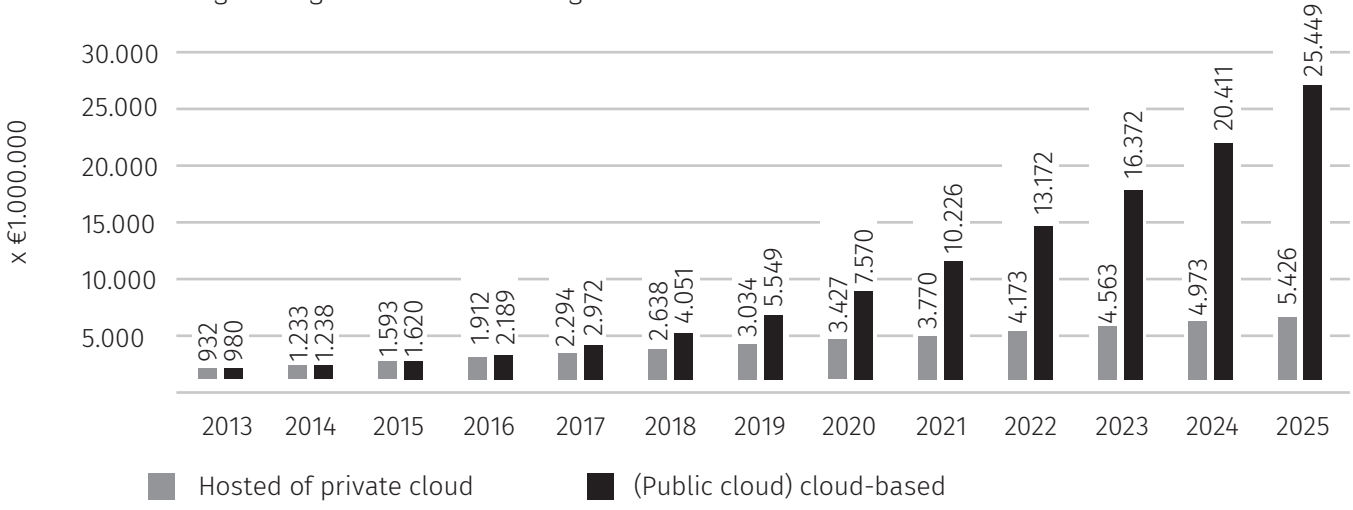
Overheid en IT

Heel lang was het beleid van de overheid om IT in eigen hand te houden en geen commerciële clouddiensten te gebruiken. Geleidelijk aan veranderde dit beleid. Diensten van commerciële cloud-aanbieders boden flexibiliteit en ze waren ook goedkoper dan alles zelf laten ontwikkelen en telkens weer een wiel uit moeten vinden dat elders al lang bestond. Althans, dat was de verwachting. In 2022 koos de overheid voor een nieuwe cloudstrategie, die het voor hen mogelijk maakt om diensten af te nemen bij commerciële aanbieders. Wel met een aantal restricties, zo blijkt uit de brief van de staatssecretaris aan de Kamer: *"Om veiligheidsrisico's te minimaliseren zijn overheidsinstellingen verplicht vooraf een risico-analyse te maken. Het gebruik van commerciële clouddiensten is bovendien niet toegestaan voor het opslaan of verwerken van staatsgeheime informatie en er mogen geen diensten worden afgenomen van leveranciers uit landen met een actief cyberprogramma dat gericht is tegen Nederlandse belangen. Het ministerie van Defensie valt buiten de reikwijdte van dit nieuwe beleid. Voor gegevens uit de basisregistratiepersoonsgegevens en bijzondere persoonsgegevens geldt het principe nee tenzij. De nieuwe cloudstrategie vervangt het huidige beleid, dat dateert uit 2011. Daarbij werd nog geen gebruik gemaakt van commerciële clouddiensten. In de nieuwe situatie mogen overheidsorganisaties clouddiensten extern gaan afnemen. Alle opslag en verwerking van persoonsgegevens vindt plaats op een verantwoorde manier, die aansluit bij geldende privacyvereisten. Dit is het principe. In de praktijk weten wij dat de GDPR (de Nederlandse AVG) en de Amerikaanse wetgeving met elkaar botsen.*

Voor die risicoafweging wordt door de chief information officer van het Rijk samen met de CIO's van de betrokken ministeries voor het einde van 2022 een richtlijn opgesteld. CIO Rijk monitort de toepassing van dit beleid en wordt betrokken bij besluitvorming over uitzonderingen. Toezicht op naleving van de regels valt onder de bestaande wettelijke taken van Algemene Rekenkamer, Auditdienst Rijk en Autoriteit Persoonsgegevens."

In de praktijk is de overheid echter niet één enkele centrale inkoper: het zijn tientallen CIO's van tientallen departementen die met vrij grote autonomie beslissen over hun ICT-bestedingen. Dit is overigens wel een punt waar de huidige staatssecretaris voor Digitale Zaken verandering in wil aanbrengen door de overheid meer als één organisatie te laten werken op het gebied van ICT-bestedingen.

Ontwikkeling cloud-gerelateerde bestedingen



05. Wie is Dutch Cloud Community en wat is de cloud?

Dutch Cloud Community is de brancheverenigingvoor de Nederlandse cloud- en internetsector. Bedrijven in onze sector werken voor duizenden klanten in de gezondheidszorg, financiën, logistiek en vele andere branches. Deze klanten stellen de hoogste eisen aan de dienstverlening die door bedrijven uit onze sector wordt geboden. Het is een sector waar professioneel gewerkt wordt met veel kennis, expertise en certificeringen. Samen met onze leden, partners, overheidsinstanties, politieke organen en andere belanghebbenden staan wij in het hart van deze sector.

Onze leden zijn dus (voornamelijk) hostingbedrijven en cloudbedrijven, zo is de korte uitleg. Maar eigenlijk zijn er nauwelijks bedrijven in de sector te vinden die precies hetzelfde doen. Achter die twee termen hosting en cloud schuilen verschillende activiteiten die wel met elkaar verbonden zijn, maar waar heel andere businessmodellen bij horen. De bedrijven leveren andere diensten aan andere groepen gebruikers. De begrippen hosting en cloud zijn een beetje de catch-all namen voor een verscheidenheid aan activiteiten.

Hosting, simpel gezegd, is het beschikbaar maken van ruimte op je servers voor derde partijen. Hierdoor hoeft de eigenaar/gebruiker niet zelf hardware te kopen om zijn bestanden op te zetten en hoeft hij niet zelf te zorgen voor de connectiviteit naar het internet.

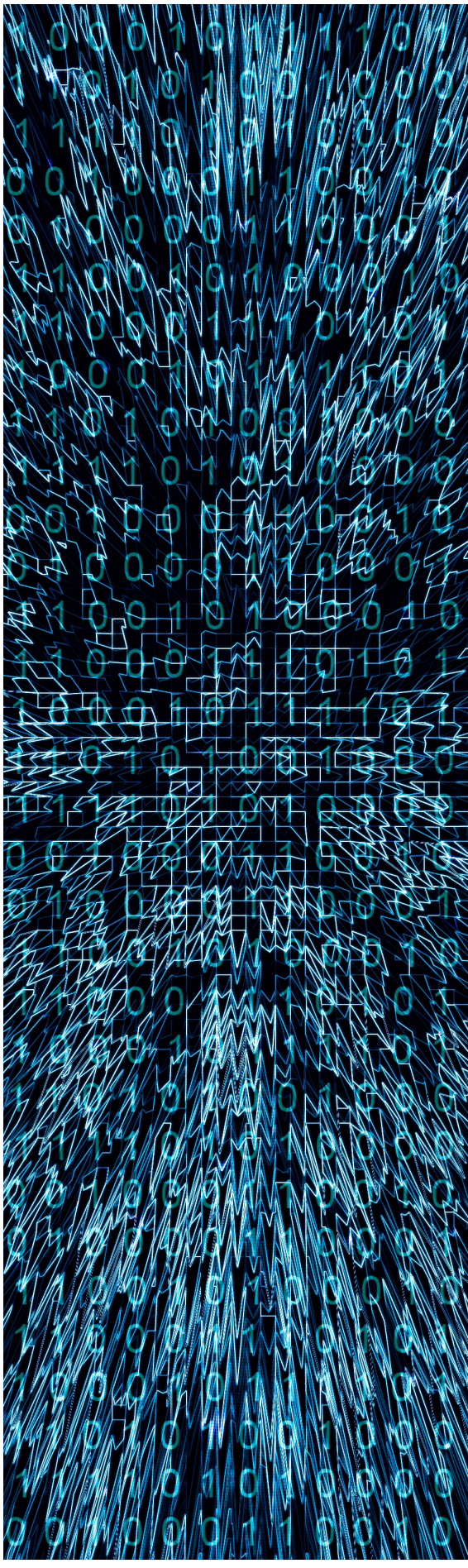
Een goed voorbeeld daarvan is webhosting. De klant huurt ruimte op de server van de hoster, mag daarop de bestanden van zijn website installeren (meestal in combinatie met een eigen domeinnaam en eventueel andere diensten zoals e-mail of een webshop) en de provider zorgt ervoor dat de website blijft draaien, beveiligd is, vindbaar is en altijd bereikbaar is. Als dat een kleine site is, gaat dat normaal gesproken via zogeheten shared hosting, wat betekent dat meerdere (soms honderden) klanten hun website op dezelfde fysieke server hebben draaien. Voor grotere, zwaardere sites is het nodig om een eigen al dan niet virtuele server in te richten.

Wat is dan het verschil met een **cloud**? In beginsel is het principe hetzelfde: de eigenaar van de bestanden die in de cloud komen te staan kiest ervoor om deze op de server van een provider te zetten, die dan onder andere zorgt voor het altijd beschikbaar maken van de bestanden, voor de connectiviteit en een deel van de beveiliging.

Het grote verschil is dat een cloudomgeving niet alleen min of meer statische bestanden omvat, maar een werkomgeving is waarin intensief computing plaatsvindt: berekeningen, mutaties en andere activiteiten waardoor de bestanden continu veranderen. De cloudomgeving heeft daarom behoefte aan rekenkracht (CPU's), aan werkgeheugen, aan storage en aan allerlei verbindingen met andere systemen en andere clouds van waaruit data, identificatie, processen en security gehaald en gebracht moeten worden.

Ook hier hebben we het over 'de cloud', maar er schuilt een heel scala aan definities achter die term. De belangrijkste drie daarvan op een rijtje:

IaaS: Infrastructure as a Service. In IaaS wordt de fysieke infrastructuur van de cloudomgeving door de provider geleverd en beheerd. De gebruiker neemt rekencapaciteit, opslag, virtualisatie, werkgeheugen en connectiviteit af van de provider en kan zijn opdrachten op de infrastructuur van de cloud laten draaien. Dat is een hele flexibele aanpak. De gebruiker/klant bespaart zich de uitgaven van de aanschaf en de rompslomp en het beheer van eigen infrastructuur. Bovendien is het heel makkelijk voor



de gebruiker om snel op te schalen op het moment dat dit nodig is. Het beheer van de omgeving zelf is nog wel in handen van de gebruiker. Voorbeelden van hosting providers die dit soort diensten leveren zijn Leaseweb en Hetzner.

De infrastructuur wordt hier door de IAAS-provider beheerd, doorontwikkeld en hoog beschikbaar gehouden. Het beheer van de toepassingen bovenop deze IAAS van de omgeving zelf is nog wel in handen is van de gebruiker.

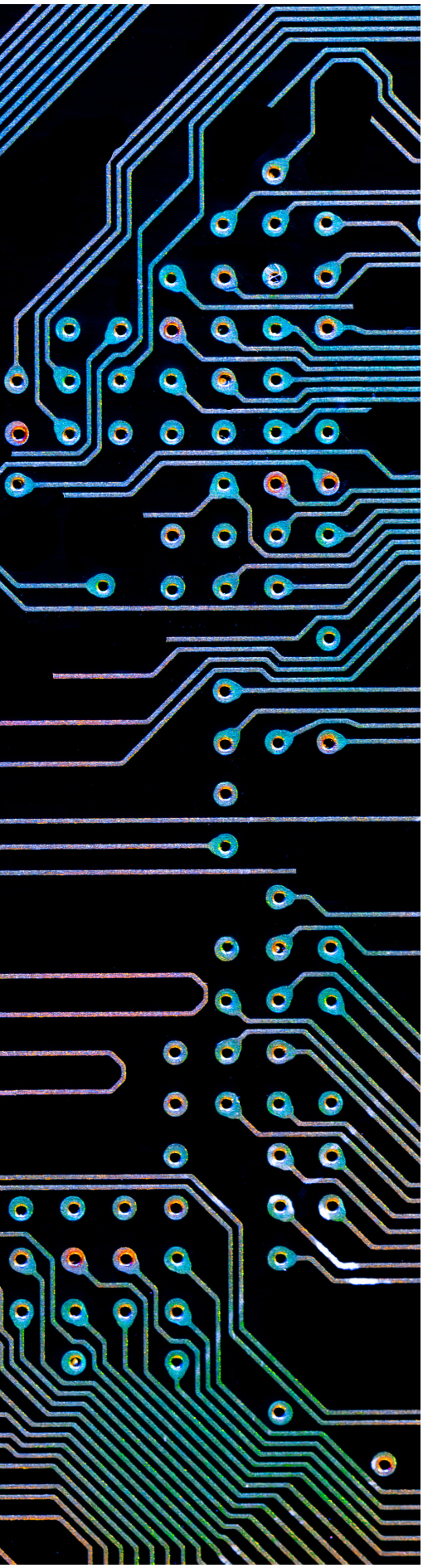
PaaS: Platform as a Service. In een PaaS-omgeving neemt de provider wat meer taken over van de gebruiker. Meestal is de cloudaanbieder degene die bijvoorbeeld het Operating System op de servers en de middleware beheert. De gebruiker kan zijn applicatie op het platform van de provider laten draaien, of daar een eigen ontwikkelomgeving in bouwen.

SaaS: Software as a Service. In een SaaS-omgeving is de gebruiker niet meer eigenaar van de omgeving of zelfs van de applicatie, maar neemt hij op abonnementsbasis een dienst af van de provider. Denk aan Office 365 of Salesforce. De klant krijgt een login op een software applicatie die verder volledig in beheer is bij de provider. Vaak kan de toepassing gewoon via een webbrowser benaderd worden. Updates van de software gebeuren transparant, zonder dat de gebruiker er iets voor hoeft te doen. Ook backups, onderhoud en beveiliging vallen helemaal onder de verantwoordelijkheid van de dienstaanbieder. SaaS ontzorgt de klant volledig en maakt het heel flexibel om bijvoorbeeld een gebruiker toe te voegen. Dit is, op dit moment, de snelst groeiende tak van clouddiensten.

De voordelen van IT in de cloud laten draaien zijn legio. Het is geen verrassing dat de ‘gang naar de cloud’ steeds verder doorzet. Er komen steeds minder toepassingen die nog echt eisen dat ze op de locatie van de gebruiker in een eigen omgeving draaien.

In deze drie belangrijkste vormen zitten sterke nuances. Maar samengevat geeft dit wel een beeld van wat cloud computing is.

In de bijlages kunt u een uitgebreid woordenboek van cloud-termen vinden.



06. Publieke cloud vs private cloud en hybride cloud (multicloud)

Een private cloud is een omgeving die door een provider specifiek voor een organisatie is ingericht. De infrastructuur staat bij de provider, maar wordt niet gedeeld met andere gebruikers.

Een private cloud is het soort omgeving dat een Nederlandse cloudprovider aan klanten zal aanbieden. Een beveiligde omgeving, op de schaalbare infrastructuur van de provider, in een eigen of gedeeld datacenter, waar de provider de IT van de klant zal beheren.
Hierin bestaan verschillende nuances, zoals:

- Volledig airgapped private cloud (waarbij niets fysiek wordt gedeeld)
- Deels fysiek gedeeld (networking en storage) en deels fysiek dedicated (compute)
- Volledig fysiek gedeeld en logisch gescheiden

Een publieke cloud is een meer generieke omgeving waarin vele gebruikers (soms miljoenen), gebruik maken van dezelfde infrastructuur en diensten. Dit is typisch het aanbod van de grote ‘hyperscalers’, Amerikaanse partijen als Microsoft, Amazon Web Services en Google, of grote Chinese aanbieders zoals Ali Baba.

In Europa zijn voornamelijk het Franse OVH, het Duitse Hetzner, het Nederlandse Leaseweb en het eveneens Duitse LIDL aanbieders van dit soort publieke clouddiensten.

07. De multicloud

Multicloud is de naam voor een hybride propositie, waarin bepaalde onderdelen in een private cloud zitten (bijvoorbeeld de dataopslag en bepaalde toepassingen) en andere diensten afgenomen worden vanuit een publieke cloud. Alle providers bieden tegenwoordig de mogelijkheid om diensten uit verschillende clouds te bundelen en naast elkaar of met elkaar te gebruiken.

08. Onderkennen van de risico's

De redenen voor de systematische keuze voor niet-Europese providers zijn als volgt samen te vatten:

Gemak: Overheden werken al veel samen met bepaalde Amerikaanse partijen. De producten en diensten zijn goed bekend en er liggen al raamovereenkomsten. De inkoper kan met een paar muisklikken zijn diensten aanschaffen. Als je met een Nederlandse partij wilt werken zou je een volledige onderhandeling aan moeten gaan over de voorwaarden, zo is de perceptie. In werkelijkheid valt dat wel mee.

Bekendheid: Ook al is de wens er om met Nederlandse partijen te werken: wie zijn ze? Wat hebben ze te bieden? Met wie moet je praten? Er is geen duidelijk overzicht beschikbaar (in de vorm van een portal bijvoorbeeld) van wie wat tegen welke voorwaarden kan bieden.

Technisch: Het is onder andere lastig om jouw clouddiensten te spreiden onder meerdere partijen. De interoperabiliteit tussen de verschillende Nederlandse en Europese partijen is nog niet goed ontwikkeld. Overigens is het delen van data tussen bijvoorbeeld AWS en de cloud van Microsoft ook heel erg lastig.

Prijs: De perceptie bij veel overheidsdiensten is dat de public cloud goedkoper is. Dat is, onderaan de streep, meestal niet het geval. Maar die perceptie is er wel. In het hoofdstuk over kosten gaan wij dieper in op de opbouw van de kosten van een clouddienst.

Risico: Vragen die wij vaak tegenkomen bij de overheid hebben betrekking op redundantie en risicomanagement. AWS, Google en Microsoft worden gezien als laag-risico-opties, met een kleine kans dat er iets fout zal gaan. De keuze voor de publieke cloud van de grote Amerikaanse aanbieders is er één die voor de opdrachtgever veilig is. Vroeger zei men: "No one ever got fired for choosing IBM". Dat principe is nu leidend voor veel inkopers bij de keuze voor Microsoft of AWS. Je kunt er nooit van beschuldigd worden onverstandige risico's te hebben genomen. De inkopers worden gestuurd door de CTO en niet door de CEO. Daarmee wordt het voornamelijk een kostenafweging en niet een front-office-, efficiency- en kwaliteits-besluit.

One stop shop: De cloud van een grote Amerikaanse provider biedt alle functionaliteiten die de gebruiker nu nodig heeft, maar ook in de toekomst nodig verwacht te hebben. Alles zit onder één dak. Het werkt en integreert met elkaar. Bovendien wordt heel veel software van derden ontwikkelt om te kunnen werken met de diensten van (met name) Microsoft.

Er is minder oog voor de risico's die deze keuze op termijn met zich meebrengt. Hoe sterker de band wordt die de overheid opbouwt met de publieke cloud, hoe moeilijker het wordt om ooit terug te keren. De keuze voor gemak brengt verborgen kosten met zich mee.

09. Geopolitiek belang

Internet expert Bert Hubert vatte het in een recent artikel mooi samen: *“Als je al je spullen uit één land haalt, dan zullen die mensen uiteindelijk toch wel gaan bepalen wat voor ICT-dingen je nog kan doen.”*

Je hoeft niemand uit te leggen waarom het onvoorzichtig is om alle clouddiensten die de overheid van een Europees land gebruikt bij een Chinese provider onder te brengen. Dat spreekt voor zich. Maar is 100% afhankelijk worden van een provider uit de Verenigde Staten zo veel veiliger?

Toen de VS in 2003 de invasie van Afghanistan aan het voorbereiden was wilde Nederland (net als Duitsland, Frankrijk en zelfs het Verenigd Koninkrijk) in eerste instantie geen deel uitmaken van de coalitie die Donald Rumsfeld aan het vormen was. Toen liet Rumsfeld de hamer vallen: “Je bent voor ons of tegen ons”. Wie niet meedoet kon handelssancties verwachten. Nederland draaide om en stuurde troepen.

In november dit jaar hebben de Amerikaanse kiezers opnieuw Donald Trump als president gekozen. Een president die heel duidelijk kiest voor “America First”. Het zou van naïviteit getuigen om te denken dat bij een volgende crisis de regering van de VS zou aarzelen om gebruik te maken van de totale afhankelijkheid van haar Europese partners om druk op ons uit te oefenen.

10. Controle over onze data 1/2

Amerikaanse wetgeving is ondubbelzinnig. Data die onder de controle valt van Amerikaanse entiteiten valt onder de Amerikaanse wetgeving van de CLOUD Act, FISA en de Defense Production Act en kan worden opgevraagd door de Amerikaanse autoriteiten, ongeacht het land waar die data zich bevindt.

Dus ook data die door een Amerikaanse provider in een Europees datacenter staat, valt onder Amerikaanse wetten.

Dit is wat instituut Clingendael schrijft in hun Policy Brief Cloud Sovereignty van 2024

Box 2. The CLOUD Act, FISA and the Defense Production Act The CLOUD Act, adopted by the US Congress in 2018, obliges 'US service providers to preserve and produce data they control regardless of where it is stored'. The FISA is a US federal law that governs the surveillance and collection of foreign intelligence information. It defines foreign intelligence information as 'information relating to a foreign power or that generally concerns the ability of the United States to protect against international terrorism or a potential attack by a foreign power or agent of a foreign power'. A legal expert analysis made for the Dutch Cybersecurity Centrum (NCSC) concludes that only in two conditions can EU entities avoid falling under the CLOUD Act, even if located outside the US: (1) If there is no 'corporate relation to any company with a presence in the US (such as a US subsidiary)' and if there are 'no sufficient contacts with the US such that it is reasonable for the US to assert jurisdiction over the EU Entity/non-US entity'; (2) When there is a 'corporate relationship with a company based in the US, the US company must not have possession, custody, or control over the data that is stored in the EU. In no case can the EU Entity have a US parent company, as the parent would be considered to have possession of or control over the data of its subsidiary'. The analysis goes as far as to recommend CSPs that wish to be completely out of the CLOUD Act's scope 'not to employ US nationals who have access to relevant data'. The Defense Production Act, which was first enacted in 1950 during the Korean War, gives the US President authority to expand and speed up the supply of materials and services from the US industrial base as needed to promote the national defence. Although not specifically mentioning cloud services, the Act is broad in scope and flexible enough to accommodate it, should an attack on American CSPs occur. Theoretically, such an event could have negative consequences in the availability of cloud services to European customers and governments, as American needs would be prioritised. See: Eurojust, The CLOUD Act, 22 December 2022; US Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): an overview, 10 March 2020; US Federal Bureau of Investigation, Foreign Intelligence Surveillance Act (FISA) and Section 702: news and updates; Dutch Ministry of Justice and Security – National Cyber Security Centre, Memo Cloud Act, 16 August 2022.

Hierover bestaan aardig wat misverstanden, die de verschillende vendoren van niet-Europese publieke clouddiensten in hun communicatie ook liever onbelicht laten. Zo biedt een aantal Amerikaanse leveranciers 'soevereine clouddiensten' aan, waarmee ze bedoelen dat de data in een Europees datacenter staat en soms op zo'n manier is ingeregeld dat er geen rechtstreeks koppeling naar de Amerikaanse infrastructuur aanwezig is.

Echter, zolang het bedrijf gecontroleerd is door een Amerikaanse UBO blijft de Amerikaanse wetgeving van toepassing. En als er geen rechtstreekse koppeling is kan de rechter in Washington het bedrijf opdracht geven om er een aan te leggen. Soeverein ben je alleen als de overheid van een niet-EU-land de data onmogelijk kan opvragen. Het wel of niet aanleggen van een fysieke link heeft hier geen invloed op.

10. Controle over onze data 2/2

Bert Hubert schreef hier het volgende over:

Dat het niet uitmaakt op welke servers je data staat komt door een specifieke wet. Microsoft wilde ooit niet meewerken aan een overheidsverzoek voor in Ierland gehoste data en die rechtszaak liep al een hele tijd. Toen heeft de Amerikaanse overheid via de "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act) verduidelijkt dat hun afluisterwetgeving universeel geldig is. Microsoft gaf het verzet toen op en overhandigde de data.

Dat de Amerikaanse overheid bij alle data op servers van Amerikaanse bedrijven kan, ongeacht de locatie, staat op de volgende drie plekken beschreven:

1. De Cloud Act Memo opgesteld op verzoek van het Nederlandse NCSC. Hier staat zelfs de aanbeveling dat Europese bedrijven geen Amerikanen in dienst moeten nemen als ze buiten de reikwijdte van de Amerikaanse CLOUD Act willen blijven.

2. Een set WOO-documenten van het Shared Service Centre-ICT van de overheid. Op pagina 6 staat: *"Niet uit te sluiten valt dat inzage gevraagd wordt door de Amerikaanse overheid, zoals ook bevestigd door SLM-Rijk in de CTO-raad"*.

3. Promises unkept: The EU-US Data Privacy Framework under fire analyse US afluisterwetgeving. Daarin staat: *"Particularly under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 … The crux of the issue lies in the fact that these laws allow broad data collection by US intelligence agencies, leaving EU data vulnerable to indiscriminate surveillance."*

Over dat laatste, er bestaan zogeheten 'standard contractual clauses', maar die voorkomen niet dat je afgeluisterd wordt. Ze maken het wel deels legaal, maar daar heb je in de praktijk niets aan.

Overigens geldt de Nederlandse AIVD/MIVD afluisterwetgeving ook internationaal. Als de Amerikaanse overheid z'n e-mail via een Nederlands bedrijf zou stallen op servers in Amerika, dan zou de AIVD die gegevens ook op kunnen vragen. Ook voor onze wet maakt het niet uit waar je server staat. Daarom zet de Amerikaanse overheid zijn e-mail ook niet op servers onder buitenlands beheer. Alleen wij zijn zo onverstandig.

Het is een niet onderbouwde gedachte dat 'de servers staan in de EU' iets uitmaakt voor de Amerikaanse wet. Iedereen die dit meldt moet dat vooral nog eens op schrift herhalen. Ik heb een paar weken geleden rondgevraagd of iemand deze toezegging ooit op schrift had gekregen van Microsoft, maar niemand bleek hier iets van te kunnen vinden. Vraag er vooral om!

Er is overigens nog een extra ironisch iets. Amerikanen hebben zelf al niet al te veel privacy onder hun eigen recht, maar nog wel een beetje. Als er in bulk is afgeluisterd moeten de Amerikaanse inlichtingendiensten een beetje hun best doen om het verkeer van Amerikanen te '"masken'. Dit soort regels gelden niet voor verkeer van Europeanen. Het is fascinerend dat we, door onze data op aparte EU-servers te zetten, juridisch gezien onder Amerikaans recht veel makkelijker afluisterbaar worden!

11. Autonomie

Met wie worden je bestanden gedeeld? Wie mag inzicht krijgen in jouw data? Voor de vakantiefoto's van een privé persoon is dit meestal niet de meest prangende vraag.

Het wordt wel een belangrijke vraag op het moment dat je bedrijfsgeheimen ergens op moet slaan. Dat je onderzoeksresultaten met andere onderzoekers wilt delen. Of dat het gaat over de e-mailwisseling tussen een minister en zijn ambtenaren.

Privacy is dan niet meer een luxe. Het is absoluut noodzakelijk. En door de dominante positie van de grote Amerikaanse spelers wordt het steeds lastiger om partijen te vinden die nog wel bereid zijn om respectvol om te gaan met de privacy van de gebruikers.

In een artikel in het NRC van 31 december 2024 vertellen onderzoekers naar hun zoektocht naar een privacy-vriendelijk platform om data tussen verschillende universiteiten te delen:
"Want de afgelopen tien tot vijftien jaar verhuisde vrijwel iedere instelling 'naar de cloud' en doekte zijn eigen rekencentrum op, vertelt Wladimir Mufty van SURF. De belofte was dat dit goedkoper zou zijn ('niet waar') en dat het werk van ict-ers leuker werd omdat ze meer zouden gaan aansturen dan zelf opslaan en beheren. Het resultaat is dat Amazon, Microsoft en Google nu ook de wetenschappelijke opslagmarkt domineren.

"We hebben twintig soorten chocolade en maar drie smaken als het gaat om het opslaan van onze data", zegt Van Dijck in een vergaderzaal van SURF in Utrecht. Mufty vult aan: "Door die cloudbeweging zijn we afhankelijk geworden van techbedrijven die mede bepalen hoe wij kunnen samenwerken. Maar IT moet helpen, niet dwingen."

12. Technische afhankelijkheid

De keuze om onze cloud van buiten Europa te halen leidt tot een almaar groeiende afhankelijkheid van de technische kennis van buiten Europa. Naarmate wij onze eigen kennis afbouwen en blind gaan varen op die van de grote tech-reuzen worden wij afhankelijker van hun platform en hun expertise.

Wij hebben zelf geen technische kennis meer in huis en omdat wij de Nederlandse sector links laten liggen bouwen wij ook in de private industrie geen nieuwe kennis op. Uiteindelijk gaat het ten koste van de Nederlandse knowhow, van investeringen in onze eigen infrastructuur en daarmee ook van de aantrekkingskracht van bedrijven, investeerders en innovatie.

Waarom heeft de overheid nog kennis in huis nodig als wij alleen nog maar contractmanagement doen met een paar hele grote partijen? En waarom zouden de hbo's en de universiteiten nog opleiden als er in ons land en in Europa nauwelijks nog bedrijven zijn die overleven wanneer alle IT in de cloud van de hyperscalers staat?

Dit is geen denkbeeldig doemscenario. De landelijke, provinciale en gemeentelijke overheden zijn gecombineerd de grootste afnemer van clouddiensten in de markt. De systematische keuze om diensten niet bij Nederlandse providers af te nemen leidt onherroepelijk tot een verarming van de kennis in ons eigen land en het wegkwijnen van het onderwijs, omdat de banen voor de afgestudeerden er niet zijn.

13. Kosten

De perceptie van veel CIO's is nog steeds dat de keuze voor een publieke cloud de meest kost-effectieve is. In de praktijk is het plaatje veel genuanceerder. De totale kosten, als alles eenmaal is opgeteld, zijn meestal veel hoger dan de raming vooraf.

Bij een Infrastructure as a Service (IaaS)-product wordt de facturering meestal gebaseerd op de middelen die door de gebruiker worden toegewezen en verbruikt. De prijsstructuur kan per aanbieder verschillen, maar enkele veelvoorkomende factuurelementen zijn:

Computing: Kosten voor rekenmiddelen zijn meestal gebaseerd op het type en de grootte van de virtuele machines (VM's) of instanties. De prijs kan afhangen van het aantal CPU-kernen, de hoeveelheid RAM en het type instantie (bijvoorbeeld: algemeen gebruik, rekenkracht geoptimaliseerd of geheugen geoptimaliseerd).

Opslag: Facturering voor opslag betreft de hoeveelheid gebruikte gegevensopslag over een bepaalde periode, meestal gemeten in gigabytes of terabytes per maand. Dit omvat zowel de primaire opslag voor draaiende instanties als aanvullende opslag, zoals objectopslag of blokopslag.

Dataverkeer: De meeste IaaS-aanbieders rekenen kosten voor dataverkeer of bandbreedtegebruik. Dat geldt voor gegevens die in en uit de IaaS-omgeving worden overgedragen. Inkomend dataverkeer is vaak gratis, terwijl uitgaand dataverkeer wordt gefactureerd na een bepaalde drempel.

Netwerken: Kosten voor geavanceerde netwerkfuncties, zoals load balancers, toegewijde IP-adressen of VPN-toegang. Onder netwerkkosten vallen ook tarieven voor gegevensoverdracht binnen of tussen regio's.

IP-adressen: Sommige aanbieders brengen kosten in rekening voor statische IP-adressen als die niet aan een draaiende instantie zijn gekoppeld of als meer IP-adressen worden gebruikt dan in het basispakket zijn opgenomen.

Besturingssysteem en softwarelicenties: Hoewel veel aanbieders de kosten van het besturingssysteem opnemen in de prijs van de VM, kunnen er extra kosten zijn voor premium besturingssystemen of softwarelicenties die op de VM zijn geïnstalleerd, zoals databases of applicatieservers.

Ondersteuningsplannen: Ondersteuning wordt doorgaans aangeboden in verschillende niveaus, variërend van basisondersteuning, die mogelijk bij de service is inbegrepen, tot premiumondersteuning met snellere responstijden en toegang tot meer ervaren technici.

Snapshots en back-ups: Kosten voor het maken van snapshots en back-ups van je gegevens, wat essentieel is voor herstel na een ramp en continuïteitsplanning voor bedrijven.

Naleving en beveiligingsfuncties: Extra kosten kunnen van toepassing zijn voor verbeterde beveiligingsmaatregelen, nalevingscertificeringen en auditmogelijkheden.

Een offerte kan er leuk uitzien, maar de werkelijke prijs per maand kan schommelen tussen het twee- en vijfvoudige. Een ding is zeker: het zal nooit goedkoper uitkomen dan verwacht.

Er is een sterke trend gaande van "cloud repatriation": organisaties die in hun eerste, snelle groeifase de keuze voor het gemak van de publieke cloud hebben gemaakt maken inmiddels een omgekeerde beweging, naar meer controle over hun eigen infrastructuur.

Een bekend voorbeeld is 37Signals, het bedrijf van David Heinemeier Hansson, dat 7 miljoen dollar aan besparingen bereikte door uit de cloud van AWS te stappen.

Ook in Nederland zien wij partijen als The Sharing Group (Mijndomein) de weg terugzoeken vanuit de publieke cloud naar meer controle over de kosten.

14. Exit-strategie

Een lastig vraagstuk, waar niemand een eenvoudig antwoord op heeft is de exit-strategie vanuit de publieke cloud. Met andere woorden: als ik al mijn data en mijn applicaties in de cloud van Microsoft of AWS heb gezet en ik wil geen gebruik meer maken van die provider, hoe kom ik er weer van af?

Een clouddienst stopzetten is niet zo eenvoudig als de krant opzeggen. Je hele bedrijfsvoering is er omheen gebouwd. Je security is erop ingericht. Je data zit in een proprietary formaat dat niet heel makkelijk omgezet kan worden naar iets anders (met de Data Act komt hier wel verandering in, hoe daar vorm aan gegeven zal worden is nog onduidelijk). Je applicatie is cloud-native ontwikkeld voor de clouddienst van die specifieke provider.

Dat alles maakt het verlaten van het ecosysteem waar je in bent gestapt een behoorlijke uitdaging. De publieke cloudaanbieders ontwikkelen hun diensten uiteraard op een manier die erop gericht is om de klant voor eeuwig in hun omgeving te behouden.

En toch is het niet alleen belangrijk, maar in principe zelfs een verplichting voor een overheidsdienst om een duidelijke exit-strategie te hebben. Maar op dit moment constateren wij helaas dat er nauwelijks overheidsdiensten zijn die een antwoord hebben op de vraag: ‘Wat is je plan B?’ En dat is een ernstig punt van zorg.

In 2022 is een kleine Amsterdamse bank, de Amsterdam Trade Bank, failliet gegaan. Deze bank deed zaken met Rusland toen de Amerikaanse sancties van kracht werden. “After being sanctioned by the US in early April over its Russian ownership, Microsoft yanked the company’s and staff’s access to their email accounts.”Van de ene dag op de andere kon niemand meer ergens bij. Toen was het snel klaar.

15. Securityrisico's

Een argument dat vaak genoemd wordt om de keuze naar de publieke cloud te rechtvaardigen is die van de beveiliging. Een grote provider als Microsoft, zo luidt het, heeft de middelen en resources om ervoor te zorgen dat de beveiliging altijd goed op orde is.
In 2024 zijn er echter verschillende grote security problemen geweest in de cloud van Microsoft.

In juli publiceerde security bedrijf Crowdstrike een update op hun Falcon-software waardoor miljoenen Windows-systemen wereldwijd opeens niet meer konden functioneren. Bedrijven, overheden, ziekenhuizen en vliegvelden waren van het ene moment op het andere verlamd. Niets werkte meer. Toen pas werd bekend dat de software van Falcon niet een API was op het Windows-systeem, maar in de kernel van het besturingssysteem zat, waardoor er geen ontkomen aan was.

De Cyber Security Review Board zei in 2024:
"Microsoft's security culture was inadequate and requires an overhaul."

The Verge schrijft:
These are just the latest in a long line of security breaches, though. Chinese government hackers targeted Microsoft Exchange servers with zero-day exploits in early 2021, enabling them to access email accounts and install malware on servers hosted by businesses. Last year, Chinese hackers breached US government emails thanks to a Microsoft Cloud exploit. The incident allowed the hackers to access online email inboxes of 22 organizations, affecting more than 500 people including US government employees working on national security.

Described as a "cascade of security failures" by the US Cyber Safety Review Board, last year's US government email attack was "preventable," according to the board. It also found that a number of decisions inside Microsoft contributed to "a corporate culture that deprioritized enterprise security investments and rigorous risk management." Microsoft still isn't 100 percent sure how a key was stolen to enable the Chinese hackers to forge tokens and access highly sensitive email inboxes.

Hiermee zeggen wij niet dat een publieke clouddienst per definitie onveilig is. Over het algemeen hebben de grote providers hun zaakjes best wel op orde. Maar als je denkt dat je een beveiligingsprobleem kunt outsourcen, dan sla je een verleidelijk maar gevaarlijk pad in.

Het is niet zo eenvoudig. Publieke clouds zijn per definitie zeer aantrekkelijke targets voor criminelen en spionagediensten van bevriende en minder bevriende landen. En hierbij weten we dat de vraag nooit is óf er wordt ingebroken maar wanneer...

Centralisatie bij de hyperscalers zal de aantrekkelijkheid voor inbrekers alleen maar vergroten.

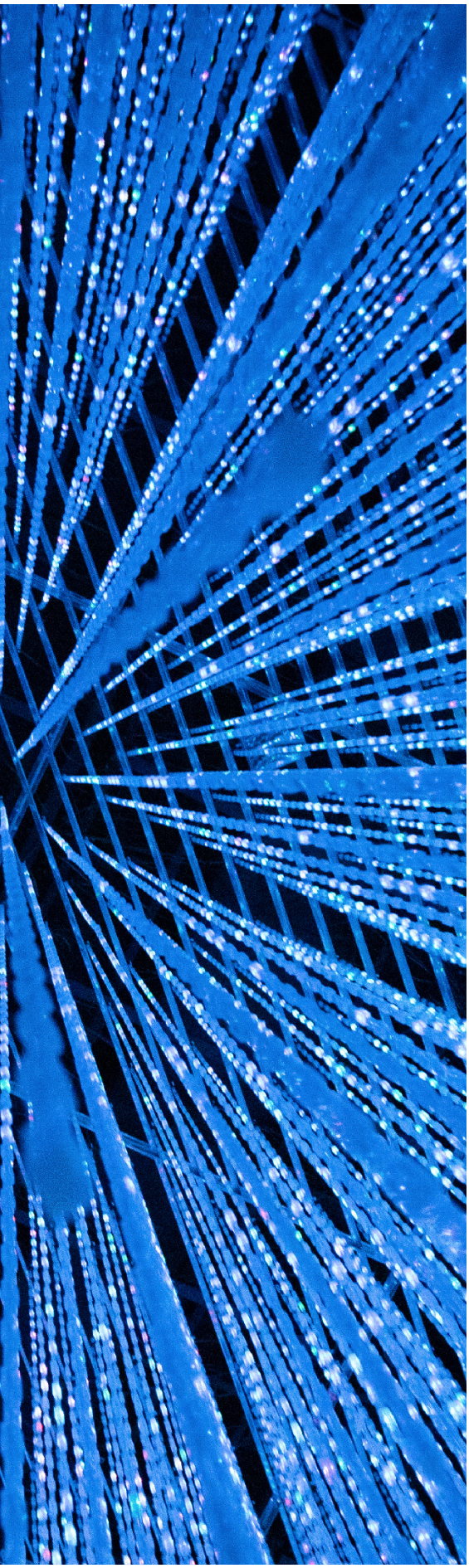
Daarnaast is het ook niet zo dat andere providers, die nu ook al heel veel werk leveren voor hoge securityklanten in de financiële sector, de zorg en allerlei andere veeleisende sectoren, hun security niet op orde hebben.

16. Licentievoorwaarden

We hebben het hier voornamelijk, als het gaat om de overheid, over de licenties van Microsoft.

Dominante softwarebedrijven gebruiken nog steeds verschillende manieren om de keuze van Europese bedrijven bij de migratie naar de cloud te beperken, zoals mededinging verstorende praktijken, inclusief ongerechtvaardigde en discriminerende bundeling, koppelverkoop, prijsstelling op basis van een voorkeursbehandeling voor eigen producten en technische en economische lock-in. Dat zegt de Europese brancheorganisatie voor cloudinfrastructuur service-providers, CISPE.

Deze organisatie benoemt vooral Microsoft als de partij die gebruik maakt van haar dominante positie in productiviteitssoftware om zo Europese klanten naar haar eigen Azure-cloudinfrastructuur te leiden. Dit ten nadele van Europese aanbieders van cloudinfrastructuur en gebruikers van IT-diensten. Het marktaandeel van Europese aanbieders van cloudinfrastructuur is de afgelopen jaren om die reden fors afgenomen.



17. Voorbeeldfunctie van de overheid

Bovendien hebben overheden een voorbeeldfunctie. Je kunt niet alleen met woorden het belang van een Europese cloudindustrie benadrukken en verwachten dat deze industrie zonder klanten kan draaien. Als we een gezonde sector willen die zich kan blijven ontwikkelen en die in staat is om in de toekomst een alternatief te bieden voor de Chinese en Amerikaanse clouds, dan moet deze sector op zijn minst een eerlijke kans krijgen om mee te dingen wanneer overheidswerk wordt uitbesteed. Op dit moment is dat niet het geval.

Bedrijven door alle sectoren van de economie, klein en groot, kijken naar wat de overheid doet en spiegelen zich aan dat gedrag. Als de overheid het doet geeft het een stempel van kwaliteit en betrouwbaarheid. Als de overheid ervoor kiest om niet met een bepaalde sector te werken geeft dat de omgekeerde boodschap aan de private sector.

Omgekeerd werkt het ook zo. Als de overheid het signaal geeft dat het vertrouwen heeft in de eigen industrie en dat het bereid is om daar waar mogelijk met deze industrie te werken, dan heeft dat een stimulerend effect. Het wekt vertrouwen bij het bedrijfsleven, het maakt het voor de eigen providers mogelijk om de investeringen te maken die het aanbod aan diensten versterken. Uiteindelijk wordt zo het gat tussen Europese en Amerikaanse clouddiensten steeds kleiner.

Gezien onze uitgebreide Europese wetgeving hebben wij een mogelijkheid om Europa te positioneren als ‘Europe as the Digital Safe Haven’.

Als we dan zelf onze data bij de hyperscalers plaatsen, laten we deze kans lopen. Wat zijn onze woorden nog waard als de daden niet volgen?

18. Werkgelegenheid en belastinginkomsten

Geld dat we naar Amerika sturen blijft niet in Nederland. Geld dat de Nederlandse overheid overdraagt aan Microsoft of een AWS is geld dat niet in onze eigen economie gestopt wordt.

Iedere cent die de overheid uitgeeft aan Nederlandse partijen, wordt weer gebruikt om in Nederland mensen aan het werk te zetten, om leveranciers te betalen en een keten in leven te houden. Over iedere cent wordt weer belasting afgedragen aan de overheid. Dit gebeurt niet met bestedingen die onze overheid in het buitenland doet. Het geld belandt niet in de economie van ons land, of die van Europa, maar eindigt in de Verenigde Staten.

De Europese hoofdkantoren van Microsoft en Google zijn in Ierland, waar het belastingstelsel voordeliger is dan in Nederland. AWS zit in Luxemburg, waar de 'corporate tax rate' een zachte 16% is.

Het betekent ook dat er met het geld van de overheid geen werkgelegenheid in Nederland komt. De ontwerpers, de developers en de beheerders van de clouddiensten bevinden zich in de VS of in Azië. Er komen geen banen bij in onze eigen techsector met de honderden miljoenen die de overheid naar de cloud van Microsoft of AWS stuurt.

Een studie van een aantal samenwerkende brancheorganisaties naar de impact van digitalisering benoemde hoe belangrijk die digitalisering voor de hele Nederlandse economie is. Samen met de omvang en groei van de faciliterende sectoren (onder andere: IT, telecommunicatie, digitale infrastructuur, IT-dienstverlening, hosting, web, datacenter en e-commerce) vormen zij de digitaal toegevoegde waarde. De intensiteit waarmee gebruik wordt gemaakt van digitale technologieën door de werkzame beroepsbevolking is hierbij bepalend. Eerder onderzoek (The METISFiles 2017) liet zien dat de werkzame beroepsbevolking voor meer dan 50% van hun tijd gebruik maakt van ICT voor het uitoefenen van hun taak. Dit deel vormt de zogenaamde 'digitale beroepsbevolking'. De omvang hiervan bedroeg in 2019 al 25% van de werkzame beroepsbevolking. Op basis van de structuur van de economie werd berekend dat de omvang van de digitale beroepsbevolking zou doorgroeien naar 2,9 miljoen in 2025, circa 36% van de totale beroepsbevolking. De groei van de digitale beroepsbevolking kan daarbij nog worden versterkt bij een snelle adoptie van nieuwe technologieën zoals AI, machine-learning, 3D-printing en sensor-technologie.

Uiteindelijk betekent geen werkgelegenheid ook geen reden voor mbo, hbo en universiteiten om op te leiden naar functies die nooit ingevuld zullen worden. Minder onderwijs betekent minder kennis in onze economie, dus ook minder competitiviteit voor de Nederlandse bedrijven die nog wel overblijven, waardoor wij uiteindelijk helemaal niet meer in staat zijn om diensten te leveren die zich nog kunnen vergelijken met het aanbod uit Amerika. Dit klinkt zwartgallig, maar het is helaas een realistische kijk op de toekomst.

19. Een sterke Europese techsector

Nederland is er trots op dat ons land een koploper is in digitalisering en de thuishaven van een aantal toonaangevende techbedrijven. Wij bewonderen onze toppers, zoals ASML en Adyen. Zowel de EU als de Nederlandse overheid vinden het essentieel dat Europa zich staande kan houden ten opzichte van de concurrentie uit China en de Verenigde Staten.

Het is ook essentieel dat Europa in staat is om zijn eigen boontjes op het digitale vlak te doppen. De digitalisering van de samenleving versnelt alleen maar in hoog tempo. AI en quantum computing zijn game changers die invloed gaan hebben op alle aspecten van onze economie en op de manier waarop wij als burgers leven, leren, consumeren en cultuur en entertainment tot ons nemen.

Kunnen wij ons veroorloven om dit allemaal aan partijen van buiten de EU toe te vertrouwen zonder dat Europa en Nederland hier een rol in spelen?

Dit is een belangrijke vraag. Wellicht is het antwoord van de regering uiteindelijk: ja. Maar dat moet dan een weloverwogen besluit zijn. Niet een standaardkeuze, zonder nadenken, omdat wij, Nederland en de EU, zaten te slapen terwijl anderen voor ons besloten.
Vanuit Dutch Cloud Community denken wij dat het antwoord gewoon ‘nee’ is. Dit is niet verstandig. Niet voor onze sector en ook niet voor de welvaart en gezondheid van onze totale economie.

En als wij inderdaad van mening zijn dat het wél belangrijk is dat Nederland een koploper moet blijven en dat Europa een serieuze tech-sector nodig heeft, dan moeten wij accepteren dat die keuze consequenties heeft en dat de eerste daarvan is dat de belangrijkste en grootste klant zijn boodschappen waar mogelijk bij de eigen sector doet.

Het is een illusie om te denken dat de Nederlandse en Europese industrie de investeringen kunnen opbrengen om een aanbod te creëren dat zich kan meten met dat van de Amerikaanse providers, zonder dat de overheden dit als klant ook steunen. Dat gaat simpelweg niet gebeuren. Maar we moeten wel alternatieven gaan bouwen. Europa en Nederland moeten een plan B gaan creëren.

20. Digitale Soevereiniteit – definities

Inleiding
Digitale soevereiniteit kent vele facetten. In dit hoofdstuk onderzoeken wij de diverse aspecten ervan en bieden wij een basis voor verdere discussie.

Op dit moment gebruikt iedereen de termen soevereiniteit, autonomie en onafhankelijkheid, meestal door elkaar en zonder dat er eenduidige definities zijn.

Er is behoefte aan een terminologie die door iedereen gebruikt kan worden, met begrippen die een breed draagvlak hebben.

Wij willen hiermee een voorzet geven. Nogmaals, Dutch Cloud Community heeft de waarheid niet in pacht. Wij nodigen iedereen daarom uit om deze definities zelf aan te vullen, om er kritiek op te hebben en commentaar op te leveren. Het is belangrijk dat wij allemaal (industrie, beleidsmakers, wetgevers en klanten) meedenken en het uiteindelijk eens worden over definities die we breed kunnen dragen

Doelstelling
De verkenning die wij hiermee inzetten moet uiteindelijk resulteren in een definitie van digitale soevereiniteit die:

- herkenbaar en relevant is voor alle stakeholders (andere cloudproviders, cloudgebruikers, beleidsmakers op zowel nationaal als internationaal niveau, maatschappelijke organisaties),
- (grotendeels) door deze stakeholders wordt onderschreven,
- het mogelijk maakt de mate van digitale soevereiniteit van een product, dienst, proces of organisatie vast te stellen,
- wordt ingezet in het publieke debat over digitale soevereiniteit.

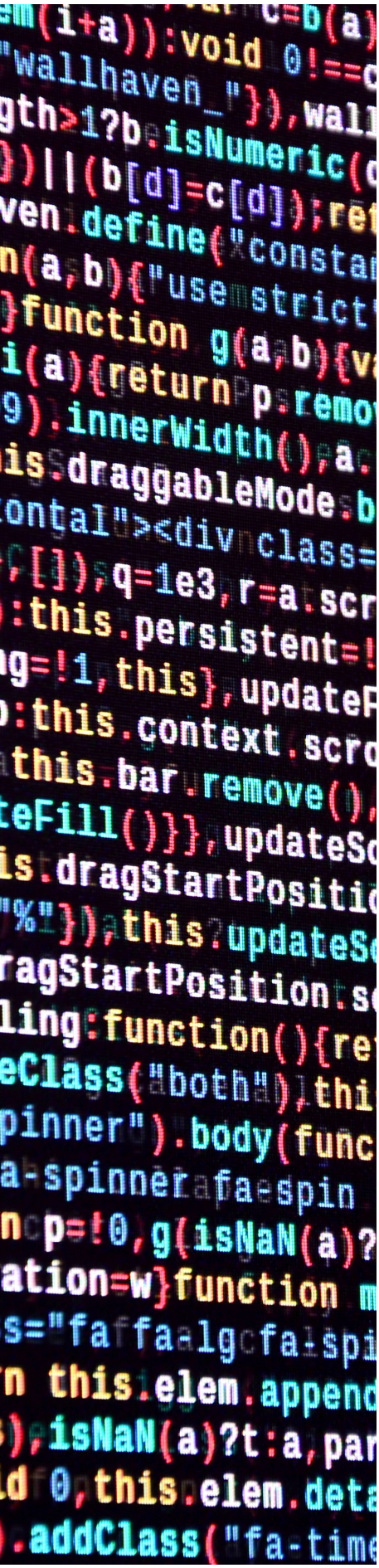
Doelgroep
Het is belangrijk om vast te stellen op wiens digitale soevereiniteit deze verkenning zich richt. We concentreren ons op de digitale soevereiniteit van de clouddienst en diens leverancier. Meer specifiek richt deze verkenning zich op de Europese digitale soevereiniteit, waarbij nationale of niet-Europese soevereiniteit buiten beschouwing blijven. De soevereiniteit van de cloudgebruiker is mede afhankelijk van de soevereiniteit van de leverancier en diens diensten.

Aspecten
Digitale soevereiniteit kan worden bepaald aan de hand van de onderstaande, niet-uitputtende lijst van aspecten:

a. Compliance aan Europese en nationale regelgeving.
b. Toepasselijke jurisdictie voor de clouddienst/ dataverwerking en cloudleverancier.
c. Organisatorische eigenschappen van de cloudleverancier.
d. Mate van controle door de data-eigenaar over de data(verwerking) en de perceptie van die controle.
e. Interoperabiliteit tussen clouddiensten van dezelfde en andere cloudleveranciers en transparantie daarover.
f. Portabiliteit tussen clouddiensten van andere cloudleveranciers. Eenvoudig in te richten en transparant.
g. Mate van afhankelijkheid van voor de clouddienst essentiële technologie.

Ad a) Over dit aspect is waarschijnlijk weinig discussie nodig. Cloudleveranciers en hun diensten moeten voldoen aan Europese en nationale regelgeving.

Ad b) Als naleving van niet-Europese regelgeving vereist is, mag dat niet in strijd zijn met Europese regelgeving. Als er wel een conflict is, diskwalificeert deze leverancier of dienst zich als Europese



soevereine partij. Het is wenselijk dat er een strengere eis komt, waarbij naleving van niet-Europese regelgeving geheel wordt verboden.

Ad c) Dit aspect gaat over de toegang tot en controle over de leverancier, dienst en dataverwerking. Als een niet-Europese entiteit de uiteindelijke belanghebbende (UBO) en/of beslisser is over deze elementen, diskwalificeert de leverancier of dienst zich als Europees soeverein.

Ad d) In hoeverre heeft de eigenaar van de data zelf zeggenschap over en controle op het proces van dataverwerking? Als die er in te beperkte mate (wat is dat dan precies?) is, is het proces van dataverwerking niet digitaal soeverein.

Ad e) Dataverwerking tussen verschillende clouddiensten van dezelfde en van verschillende cloudleveranciers is mogelijk. Het is daardoor niet noodzakelijk om alle clouddiensten bij één en dezelfde leverancier af te nemen. Er is verdere discussie nodig om dit aspect beter te definiëren. Is het bijvoorbeeld vereist om een single-sign-on dienst over verschillende cloudleveranciers te laten werken?

Ad f) Het is mogelijk om een clouddienst bij de ene leverancier in te ruilen voor een soortgelijke dienst van een andere leverancier. Het is noodzakelijk om hiervoor standaardproducttypes te definiëren voor zover die (nog) niet aanwezig zijn. De leverancier moet transparant zijn over eventuele afwijkingen van de standaard en de inspanning die nodig is voor migratie naar een andere, volledig compatibele leverancier.

Ad g) De cloudleverancier moet inzicht hebben in de mate van afhankelijkheid van niet-Europese technologie. Bij sterke afhankelijkheid moet duidelijk zijn welke mitigatie- of migratiemogelijkheden er zijn als de toegang tot deze technologie wordt geblokkeerd. Daarover moet transparant worden gecommuniceerd naar (potentiële) gebruikers. Over dit aspect is een uitgebreide discussie nodig. Het gaat niet alleen om hardware (zoals chiptechnologie) maar ook om software (zoals besturingssystemen, applicaties, SDN). In hoeverre is een cloudleverancier soeverein als de ene niet-Europese technologie eenvoudig vervangen kan worden door een andere? Worden alleen eindproducten zoals compute-faciliteiten in beschouwing genomen, of omvat dit ook toegang tot grondstoffen die noodzakelijk zijn voor deze compute-faciliteiten?

21. Wat kan de Nederlandse en Europese industrie vandaag?

Is het nu, in 2025, mogelijk voor overheidsdiensten om vanuit de Nederlandse en Europese industrie aan hun behoefte aan cloud-services te voldoen?

Dit is een hele belangrijke vraag. Als het antwoord nee is, waar hebben wij het dan nog over? Dat overheden clouddiensten nodig hebben in inmiddels wel duidelijk. Dat er risico's zijn aan een volledig niet-Europees beleid ook wel. Maar is er een alternatief?

Het antwoord is genuanceerd. Ja, er zijn op een aantal gebieden prima alternatieven, en nee, de Europese en Nederlandse sectoren kunnen niet alles wat de aanbieders uit de VS kunnen.

Het publieke cloudaanbod van Microsoft of Amazon Web Services is uiteraard zeer uitgebreid. Van simpele rekenkracht en opslag tot AI en daarnaast ook bijzondere dingen zoals een kant-en-klaar 5G-netwerk of (bij AWS) een as-a-service grondstation om een netwerk van satellieten te beheren.
De grootste aanbieders van publieke clouddiensten in Europa, zoals het Duitse Lidl, komen niet in de buurt van de Amerikanen als het gaat om de diversiteit van het aanbod.

Het is te verwachten dat Europese en Nederlandse providers een periode nodig zullen hebben om dit aanbod te kunnen evenaren. Er zit een gat dat niet in een hele korte periode overbrugd gaat worden. Wellicht gebeurt dat ook nooit als er geen wil is om het voor elkaar te krijgen.

Het grote verschil tussen Europa (inclusief Nederland) en de Verenigde Staten is niet public versus private. Ook veel Nederlandse en Europese providers zijn namelijk public in plaats van private. Het verschil zit in het aanbod van platformdiensten in deze clouds. Als we kijken naar het dienstenaanbod van Microsoft en AWS, dan loopt dat uiteen van development en data science tot AI, IoT en nog veel meer. Deze clouds hebben zich dankzij de wereldwijde adoptie kunnen ontwikkelen tot marktplaatsen met een enorm dienstenassortiment. Nieuwe diensten worden nu dus eerst voor Microsoft en AWS ontwikkeld om vervolgens een versie te ontwikkelen die door een CSP, MSP of enterprise kan worden gebruikt in een public of private cloud. Die laatste stap wordt steeds vaker zelfs al helemaal niet meer gezet.

Dit is de reden dat we moeten stoppen met vergelijken, maar moeten beginnen met ontwikkelen en soms moeten accepteren dat (nog) niet alles beschikbaar is. Als we niet gaan beginnen, komt het nooit van de grond.

Een belangrijke nuancering is dat 90% van de gebruikers van de clouds van AWS en Microsoft Azure gebruik maakt van minder dan 20 diensten, uit de honderden die worden aangeboden. De meeste diensten worden slechts voor specialistische doelen door een kleine groep klanten gebruikt. Wanneer is bijvoorbeeld de laatste keer dat u een satellietnetwerk heeft hoeven installeren?

De kerndiensten die het meest gebruikt worden zijn meestal redelijk algemene, gestandaardiseerde clouddiensten die onder andere zijn gebaseerd op rekenkracht, opslag en hosting. Die zijn ook prima te vinden bij Nederlandse en Europese partijen.

Als wij kijken naar onze eigen Nederlandse industrie, dan is het een sector die nu al werkt met veeleisende

klanten uit de wereld van de zorg, de financiële wereld, de logistiek en lokale overheden. Bij deze leveranciers zijn alle relevante certificeringen gewoon aanwezig, is continuïteit van de dienstverlening gewaarborgd en zijn backups en redundantie vanzelfsprekend. Het is een professionele sector met hoog opgeleide mensen en stevige bedrijven die al geruime tijd actief zijn, met mooie klantportfolio's.

Er zijn diensten die in de nabije toekomst alleen door de grote Amerikaanse publieke cloudaanbieders geleverd kunnen worden. Het is niet meer dan logisch dat overheden en bedrijven daar zaken mee doen en er zijn een veel Nederlandse bedrijven (MSP's) die dit soort dienstverlening ook faciliteren en beheren voor gebruikers.

Maar als je daarnaast gaat kijken naar wat er daadwerkelijk gebruikt wordt, dan zie je al snel dat ook bij de overheid het gros van de IT-uitbestedingen draait rond overzichtelijke, gestandaardiseerde diensten. Die zijn gewoon beschikbaar bij de Nederlandse en Europese aanbieders.

We kijken vaak te makkelijk naar de uitgebreide snoepwinkels van AWS of Azure, zonder stil te staan bij de vraag: heb ik dit allemaal wel nodig?

22. Hoe kan de toekomst eruit zien?

Er zijn meerdere scenario's voor de manier waarop Nederland de komende 5 à 10 jaar om kan gaan met clouddiensten. De keuzes die we vandaag maken zullen gevolgen voor de lange termijn hebben, niet alleen voor onze economie, maar voor de hele maatschappij.

Hieronder de drie meest voor de hand liggende opties, met een toelichting op wat ze inhouden en welke impact ze kunnen hebben op de samenleving.

Optie 1: doorgaan op de huidige weg

De Initiatiefnota 'Wolken aan de Horizon' vat de situatie als volgt samen: "De markt van cloudleveranciers wordt namelijk volledig gedomineerd door slechts drie Amerikaanse megabedrijven – de 'hyperscalers'. Hun dominantie neemt toe. Zo heeft Microsoft 40-45% van de cloudmarkt in handen; Amazon heeft 30-35% veroverd; Google komt daar achteraan met 5-10%. Het aandeel van Europese en Nederlandse leveranciers is zeer mager. Een keuze voor de cloud betekent vrijwel standaard de keuze voor Microsoft, Amazon of Google."

Wat betekent het om door te gaan met werken op dezelfde manier?

Door de goede compatibiliteit tussen de clouddiensten van Azure en Office 365 hebben de inkopers het gemak van een one-stop-shop waarin ongeveer alle diensten die ze willen afnemen bij één loket gehaald kunnen worden. De twee andere hyperscalers, AWS en Google, spelen een kleinere rol dan Microsoft. De Nederlandse Cloudsector doet niet of nauwelijks mee. Licenties en contractuele voorwaarden zijn via het Strategisch Leveranciers Management van de overheid (SLM)geregeld. De voorwaarden vanuit het Rijksbrede cloudbeleid 2022 blijven geldig, maar zijn, zoals nu het geval is, voornamelijk een papieren exercitie door gebrek aan audit en handhaving.

De afhankelijkheid van de leverancier is maximaal. Er is geen exit-strategie en security wordt voornamelijk uitbesteed aan de leverancier. Ook op (geo)politiek niveau is er totale afhankelijk van de VS. De regie van het cloudbeleid komt in de praktijk in handen van de leveranciers.

De overheid zelf heeft in dit scenario minder technische kennis in eigen huis en focust zich op contractmanagement en het aansturen van de contractanten.

Het gat tussen het aanbod van Europese leveranciers en de Amerikaanse hyperscalers wordt groter doordat de overheid als belangrijke opdrachtgever geen impuls kan geven aan de eigen sector. Hierdoor wordt de industrie geleidelijk aan kleiner, minder goed ontwikkeld en dus ook minder aantrekkelijk voor de afnemers vanuit het bedrijfsleven.
Op termijn verdwijnt de Nederlandse/Europese cloudsector en loont het ook niet meer voor de hbo's en universiteiten om op te leiden voor niet bestaande banen. Als we accepteren dat clouddiensten uit Amerika komen, dan moeten we ook accepteren dat de investeringen erin naar de VS gaan.

Dit is een strategie van hoog gemak, maar ook hoog risico. En op termijn ook een redelijk dure optie.

Een gevolg van deze keuze is het geleidelijk aan afsterven van de eigen sector, van de eigen kennis

en van onze onafhankelijkheid. Nogmaals, het is heel goed mogelijk dat de overheid besluit dat dit wenselijk is. Maar dan is het wel belangrijk dat de beleidskeuze gemaakt wordt op een bewuste manier, met begrip van de gevolgen. En niet 'by default' omdat een situatie organisch ontstaan is en we pas merkten dat er een probleem was toen het te laat was om er nog iets aan te veranderen.

Optie 2: de keuze voor soeverein en open source

Door Europa heen hebben een aantal pilotprojecten plaatsgevonden, bij landelijke, regionale en lokale overheden, om alles naar soevereine open source platformen te migreren.

De projecten waren meestal kleinschalig en in bijna alle gevallen zo opgezet (geen opleiding van de gebruikers, nauwelijks support, weinig budget, geen meetbare targets) dat ze ongeveer allemaal een stille dood zijn gestorven.

Als we kijken naar wat er nodig is om 90% van de vraag te kunnen beantwoorden dan kan dit voor een groot deel ook al met een open source software (OSS) cloud worden gerealiseerd. Het vraagt wellicht wat meer inzet in de fase om deployments te automatiseren, maar de gevraagde schaal is overzichtelijk. De vraag is niet of we het kunnen. De vraag is: blijven we voor gemak op de korte termijn kiezen of durven we nu een koerswijziging te starten, wetende dat het ons (overheid en aanbieder) in de beginfase wat meer energie gaat kosten.

In alle eerlijkheid lijkt het op dit moment niet realistisch om een grootschalig beleid in te voeren dat zich 100% richt op soevereine en open source

aanbieders. Het aanbod is er niet, want leveranciers die zo'n schaal aan zouden kunnen bestaan niet. De diensten en producten kunnen slechts op specifieke domeinen de vergelijking aan met het aanbod van de hyperscalers.

De keuze voor dit beleid zou inhouden dat de overheid zelf de regie neemt en een hoge mate van technische expertise ontwikkelt, om zelf in staat te zijn om een veelvoud aan nauwgedefinieerde open-source oplossingen aan elkaar te breien en de regie over de beveiliging ervan volledig in eigen handen te houden. Dit is een proces van jaren, met grote investeringen. Bovendien vraagt het om een strakke, gecentraliseerde regie en toezicht, wat het tegenovergestelde is van het decentrale model dat de overheid nu hanteert.

Ook de compatibiliteit met bestaande systemen zou problematisch zijn.

In alle eerlijkheid lijkt deze optie eerder een nobel streven dan een realistisch scenario op de horizon van 2030.

Wel is het raadzaam om meer kennis over open source op te bouwen door te experimenteren, maar deze experimenten op een gestructureerde manier aan te pakken; met voldoende funding, voldoende tijd, de juiste ondersteuning en heldere, meetbare doelen.

Optie 3: de multicloud, beleid met balans

Er worden door de overheid al veel clouddiensten afgenomen. Organisaties zijn ervan afhankelijk, processen zijn erop ingesteld en systemen zijn er op ingericht. Voor elke overheid is continuïteit essentieel.

Zorgen dat de diensten blijven opereren, zonder te tornen aan de kwaliteit en de continuïteit moet altijd een belangrijke overweging zijn.

De kunst is het vinden van een balans waarmee geen schade ontstaat aan wat al opgebouwd is, maar wel de omstandigheden ontstaan om geleidelijk aan ruimte te geven aan de Nederlandse en Europese industrie om een eerlijke kans te krijgen om voor de overheid te werken. Zo ontstaat een situatie waarin de sector kan groeien, verder kan innoveren, onderwijs en onderzoek kan aantrekken en uiteindelijk op steeds meer fronten een aantrekkelijk alternatief voor de Amerikaanse hyperscalers kan bieden.

Het eindplaatje in dit scenario is een inkoopbeleid waarin de overheid nog steeds zaken blijft doen met de huidige partners, maar actief kijkt naar welke diensten ook vanuit Nederlandse en Europese aanbieders beschikbaar zijn en de keuze maakt om, daar waar er alternatieven voorhanden zijn, ook met deze partners te werken.

Het beleid kan dan worden samengevat als: 'Europees, tenzij'. De overheden kiezen ervoor om hun IT-aanbestedingen met Europese partijen te doen, tenzij er een goede reden is om dat niet te doen (er is behoefte aan een product of dienst die niemand in Europa kan leveren).

Dit is een optie die vraagt om het maken van beleidskeuzes: er moet vanuit de overheid een wil zijn om een gebalanceerd beleid vorm te geven en dat moet gebeuren in overleg met de sector.

De overheid moet duidelijk zicht hebben op wat de eigen industrie wel en niet kan bieden en onder welke voorwaarden. Via raamovereenkomsten moet het voor CIO's eenvoudig worden om de keuze te maken voor Nederlandse of Europese aanbieders.

Offertetrajecten moeten op de schop: zij zijn vandaag in veel gevallen zo geschreven dat er maar één partij gekozen kan worden. De offerte vraagt bijvoorbeeld expliciet naar een product van Microsoft en niet naar een functionaliteit die wellicht ook op andere manieren ingevuld kan worden.

23. Wat kunnen we nu al samen doen? Concrete stappen

De Nederlandse en Europese industrie zijn nu al in staat om te voldoen aan een groot deel van de vraag van de overheidsdiensten. Het is belangrijk dat de overheid als opdrachtgever ten eerste weet wat de eigen sector kan leveren. Daarnaast moet het op een soepele manier, zonder additionele obstakels, zaken kunnen doen met die sector.

Met concrete acties kan in samenwerking tussen overheid en industrie gewerkt worden aan het weghalen van de obstakels die de overheden als opdrachtgever ervaren om zaken te doen met de eigen sector. Die obstakels zitten op verschillende niveaus: technisch, juridisch en commercieel. Als collectief kunnen wij aan de slag gaan om op verschillende punten stappen te maken die de weg vrij maken voor een nauwere samenwerking.

Een belangrijke eerste stap is **het ontwikkelen van een keurmerk voor Nederlandse en Europese leveranciers,** als een gezamenlijk project tussen de vragers (de overheden) en de aanbieders (de sector)

Dat keurmerk gaat over compliance met de ARBIT inkoopvoorwaarden van de overheid en technische oplossingen om naadloos op het HAVEN platform van de VNG te kunnen draaien. Ook aspecten als continuïteit, benodigde certificeringen, redundantie en noodplannen (in geval van het faillissement van een leverancier bijvoorbeeld), kunnen onderdeel zijn van dit keurmerk.

Raamovereenkomsten

Op basis van het keurmerk kunnen de vragende en aanbiedende partijen ook samen werken aan juridische aspecten zoals een raamovereenkomst waar Nederlandse (en eventueel Europese) bedrijven op in kunnen tekenen, zodat overheidsinstanties niet telkens nieuwe onderhandelingen hoeven aan te gaan om diensten af te nemen bij de eigen industrie.

Eén duidelijk loket voor de overheid

Uiteindelijk ontwikkelen wij een interface tussen de overheid en de sector. Het zogenaamde Bijenkorf model, waarmee de overheid via één loket toegang heeft tot bedrijven waarvan het de garantie heeft dat ze voldoen aan een aantal van tevoren gedefinieerde eisen. Dat betekent dat de overheden kunnen aankloppen bij één loket en daarachter een aantal contractante partijen kunnen vinden die een aanbod hebben dat past bij hun behoefte. Dit loket zorgt er ook voor dat het keurmerk meegroeit met de tijd, dat de overeenkomsten aangepast worden, dat contracten nageleefd worden enz..

Overheden helpen exit-strategieën te ontwikkelen

De Nederlandse cloudsector kan de overheid ondersteunen in de ontwikkeling van exit-strategieën. Wij weten, ook uit het rapport van de rekenkamer, dat voor een groot deel van de clouddiensten die de overheid gebruikt geen duidelijk plan bestaat voor het geval de dienst, om welke reden dan ook, niet meer beschikbaar is, niet meer gebruikt mag worden, of het niet meer wenselijk is om te gebruiken.

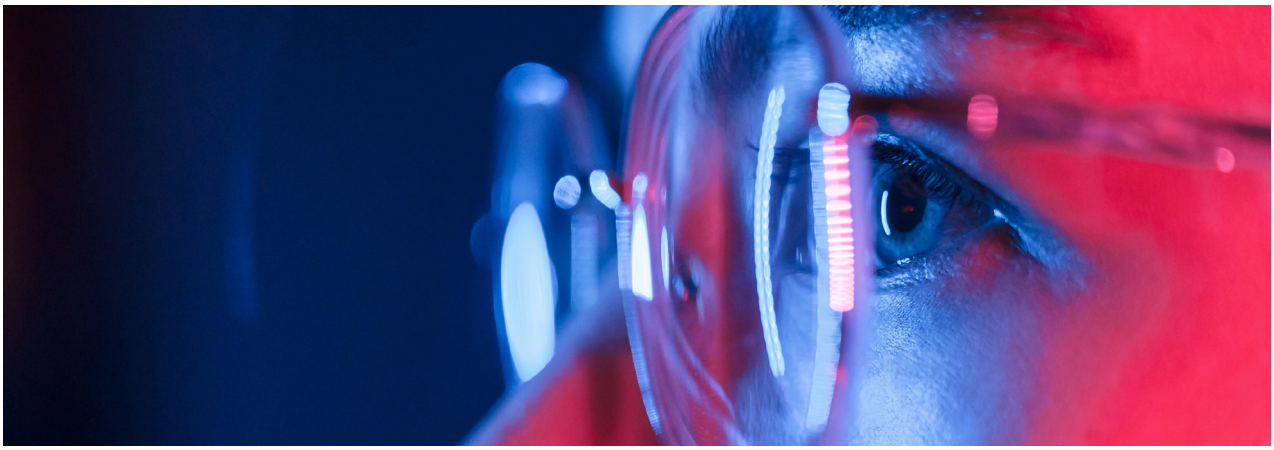
In samenwerking tussen de overheid en de Nederlandse cloudbedrijven kunnen wij helpen met een inventarisatie van de behoeften en op basis daarvan omgevingen creëren waarin de continuiteit van de dienstverlening geborgd kan worden. De branche zet zich hier ook graag voor in.

Aanbestedingen neutraal maken

Aanbestedingen van de overheid zijn vandaag in veel gevallen zo geschreven dat er maar één partij gekozen kan worden. In de aanbesteding zelf staat niet de omschrijving van de dienst die gezocht wordt, maar de merknaam van het product dat de inkoper eigenlijk al heeft gekozen voor de aanbesteding plaatsvond.

Uiteraard hebben wij het hier met name over de diensten en producten van Microsoft. Door in de aanbesteding expliciet te vragen naar het product van Microsoft is er geen reden meer voor andere leveranciers om zelfs de moeite te nemen om te reageren op de aanbesteding.

Dit kan anders en slimmer. Door de eisen en de gewenste functionaliteiten in plaats van het product te omschrijven, kunnen meerdere leveranciers een voorstel doen en kunnen die voorstellen op hun verdiensten beoordeeld worden. Op objectieve criteria, dus. Iets wat voor het bedrijfsleven heel normaal is.



24. Conclusie

Met dit whitepaper wil Dutch Cloud Community de verschillende aspecten van de discussie rondom digitale soevereiniteit samenbrengen in één document.

Waarom voeren we deze discussie? Wat ging eraan vooraf? Wat wordt precies bedoeld met concepten als een soevereine cloud? Welke definities kunnen we hanteren? En vooral: wat zijn de risico's van het huidige (gebrek aan) beleid en welke opties hebben we voor de toekomst?

De wereld verandert razendsnel. Binnen één jaar is digitale soevereiniteit verschoven van een onderbelicht thema naar een urgent onderwerp dat op vele agenda's staat. De sector, politiek en overheid zien het belang en de noodzakelijkheid om snel en doordacht stappen te zetten.

Dit whitepaper presenteert ook een mogelijke roadmap voor deze stappen. De oplossing ligt niet in het stilleggen van de overheid of het afbreken van vitale digitale infrastructuren die de afgelopen jaren zijn opgebouwd. De sleutel is een gefaseerde aanpak waarin overheid en sector samenwerken aan een gebalanceerd cloudbeleid. Zo kan de digitalisering van onze samenleving en overheidsdiensten doorgaan op een manier die Nederland minder afhankelijk maakt van buitenlandse partijen, zonder in te boeten op innovatie en efficiëntie en binnen de kaders van de wetgeving en het huidige cloudbeleid. De tijd om te handelen is nu. De Nederlandse cloud- en internetsector is zich bewust van haar verantwoordelijkheid en is bereid deze op zich te nemen. Digitale soevereiniteit vraagt om optimale samenwerking tussen alle betrokken partijen.

Het moet uiteindelijk makkelijker worden voor de overheid en andere organisaties om zaken te doen met de Nederlandse cloud- en internetsector. Dit kan met een keurmerk, raamovereenkomsten en een centraal platform waar vraag en aanbod effectiever worden samengebracht. Dit vraagt om investeringen van het bedrijfsleven en onze sector is bereid die te doen. Er staat namelijk veel op het spel!

We moeten een nieuwe manier van samenwerken ontwikkelen, zonder afbreuk te doen aan bestaande structuren en zonder partijen bij voorbaat uit te sluiten.

De weg naar digitale soevereiniteit is lang en complex. De ontwikkelingen van het afgelopen jaar hebben laten zien hoe cruciaal onafhankelijkheid is in een tijdperk waarin bijna alles digitaal aan het worden is. Laten we deze uitdaging gezamenlijk aangaan: het bedrijfsleven en de overheid kunnen niet zonder elkaar.

25. Terminologie

Cloud Computing:

1. Cloud: Een netwerk van servers die via het internet worden gebruikt om gegevens en toepassingen op te slaan en te verwerken.

2. Public cloud: Een cloudinfrastructuur die door meerdere klanten wordt gedeeld en eigendom is van een externe cloudprovider (bijvoorbeeld: Amazon Web Services, Microsoft Azure, Google Cloud).

3. Private cloud: Een cloudinfrastructuur die alleen door één organisatie wordt gebruikt en doorgaans op locatie wordt beheerd.

4. Hybrid cloud: Een combinatie van private en public clouds die samenwerken, vaak om data en applicaties te delen.

5. IaaS (Infrastructure as a Service): Een cloud-service waarbij gebruikers hardware- en netwerk-resources huren (bijvoorbeeld: virtuele machines, opslag, netwerken).

6. PaaS (Platform as a Service): Een cloudservice die een platform biedt waarop gebruikers applicaties kunnen ontwikkelen, uitvoeren en beheren zonder zelf de onderliggende infrastructuur te beheren.

7. SaaS (Software as a Service): Een cloudservice waarbij gebruikers toegang krijgen tot software-toepassingen via het internet, zonder dat ze deze zelf hoeven te installeren of te beheren.

8. Serverless Computing: Een model waarbij de cloudprovider automatisch de infrastructuur beheert en schaling verzorgt terwijl gebruikers alleen betalen voor de werkelijke uitvoering van code.

9. Virtualization (Virtualisatie): Het proces waarbij fysieke hardware wordt gesimuleerd om meerdere virtuele machines op één server te laten draaien.

10. VM (Virtual Machine): Een softwarematige computer die in een fysieke computer draait en fungeert als een aparte machine met een eigen besturingssysteem en toepassingen.

11. Containerization: Een technologie waarbij toepassingen en hun afhankelijkheden in digitale containers worden verpakt om consistente en draagbare omgevingen te bieden.

12. Kubernetes: Een opensource-platform voor het automatiseren van het beheer van containerized applicaties, inclusief schaalvergroting en -verkleining.

13. Cloud storage: Online opslagdiensten waarmee gebruikers gegevens op afstand kunnen opslaan en ophalen.

14. Multi-tenant: Een architectuur waarbij meerdere gebruikers of organisaties dezelfde fysieke infrastructuur delen, maar logisch gescheiden omgevingen hebben.

15. Elasticity (Elasticiteit): Het vermogen van een cloudservice om automatisch middelen (zoals rekenkracht of opslag) te schalen naar behoefte.

16. Scalability (Schaalbaarheid): Het vermogen om het aantal resources in een cloudomgeving uit te breiden of te verkleinen om te voldoen aan de veranderende vraag.

17. Load balancing: Een techniek om verkeer of werklast gelijkmatig over meerdere servers of resources te verdelen.

18. Cloud native: Het ontwikkelen van applicaties die volledig gebruikmaken van de schaalbaarheid en flexibiliteit van cloudplatforms.

19. API (Application Programming Interface): Een set van regels en tools waarmee verschillende softwarecomponenten met elkaar kunnen communiceren, vaak gebruikt in cloudomgevingen.

20. Edge computing: Verwerking van data dichter bij de bron (bijv. sensoren of IoT-apparaten) in plaats van in een gecentraliseerde cloud.

21. Latency (Latentie): De vertraging tussen het verzenden van gegevens en de ontvangst ervan, vaak een belangrijk aspect in cloud computing.

22. Disaster recovery (DR): Strategieën en diensten voor het herstellen van gegevens en diensten na een ramp, vaak onderdeel van cloudoplossingen.

23. DevOps: Een cultuur en set van werkwijzen die softwareontwikkeling (Dev) en IT-beheer (Ops) combineren, vaak in de context van cloud computing.

24. Data migration: Het proces van het overzetten van gegevens van een on-premise omgeving naar de cloud, of tussen verschillende cloudomgevingen.

25. Identity and Access Management (IAM): Een systeem voor het beheren van gebruikersidentiteiten en hun toegang tot resources in een cloudomgeving.

26. Cloud Security: Beveiligingsmaatregelen en -protocollen die worden toegepast om gegevens en applicaties in de cloud te beschermen.

27. Service Level Agreement (SLA): Een contract dat de verwachte prestaties en beschikbaarheid van een cloudserviceprovider specificeert.

28. Pay-as-you-go: Een prijsmodel waarbij klanten alleen betalen voor de resources die ze daadwerkelijk gebruiken.

29. Cloud Orchestration: Het proces van het beheren van de interacties en connecties tussen verschillende cloudgebaseerde systemen en diensten.

30. VDI (Virtual Desktop Infrastructure): Een technologie waarbij desktopomgevingen op afstand worden gehost op een server, toegankelijk via de cloud.

Cybersecurity:

1. Malware: Schadelijke software die is ontworpen om systemen te beschadigen, te verstoren of ongeautoriseerde toegang te verkrijgen (bijv. virussen, wormen, Trojaanse paarden).

2. Phishing: Een vorm van social engineering waarbij aanvallers proberen gevoelige informatie te verkrijgen door zich voor te doen als een betrouwbare bron via e-mails, websites of sms.

3. Ransomware: Een type malware dat bestanden of systemen versleutelt en losgeld eist om toegang te herstellen.

4. Firewall: Een beveiligingssysteem dat inkomend en uitgaand netwerkverkeer controleert en blokkeert op basis van vooraf ingestelde beveiligingsregels.

5. Antivirus: Software die is ontworpen om malware op te sporen, te voorkomen en te verwijderen.

6. Zero-Day: Een kwetsbaarheid in software die onbekend is bij de ontwikkelaar en door aanvallers kan worden misbruikt voordat er een patch beschikbaar is.

7. DDoS (Distributed Denial of Service): Een aanval waarbij meerdere systemen worden gebruikt om een doelwit te overbelasten met verkeer, waardoor deze niet meer bereikbaar is.

8. Encryption (Versleuteling): Het proces van het omzetten van gegevens in een code om ervoor te zorgen dat alleen geautoriseerde partijen deze kunnen lezen of ontcijferen.

9. Decryption (Ontsleuteling): Het proces van het omzetten van versleutelde gegevens terug naar hun oorspronkelijke vorm zodat ze leesbaar zijn.

10. Authentication (Authenticatie): Het proces waarbij een systeem controleert of een gebruiker is wie hij of zij beweert te zijn, vaak door middel van wachtwoorden of biometrische gegevens.

11. Authorization (Autorisatie): Het proces waarbij wordt bepaald welke acties een gebruiker mag uitvoeren nadat deze is geauthentiseerd.

12. Multi-Factor Authentication (MFA): Een beveiligingsmethode waarbij meerdere verificatie-stappen nodig zijn om toegang te krijgen, zoals een wachtwoord én een sms-code.

13. Vulnerability (Kwetsbaarheid): Een zwakte in software, hardware of een netwerk die door een aanvaller kan worden misbruikt om toegang te krijgen of schade aan te richten.

14. Patch: Een update die wordt uitgebracht om een kwetsbaarheid of fout in software te verhelpen.

15. Penetration testing (Pentesting): Een ge-simuleerde cyberaanval die wordt uitgevoerd door beveiligingsexperts om zwakke punten in een systeem te identificeren.

16. Brute-force attack: Een aanval waarbij een aanvaller probeert een wachtwoord of encryptie-sleutel te kraken door alle mogelijke combinaties te proberen.

17. Botnet: Een netwerk van geïnfecteerde com-puters (bots) die door een aanvaller op afstand worden bestuurd, vaak voor aanvallen zoals DDoS.

18. Social engineering: Het manipuleren van mensen om vertrouwelijke informatie te onthullen of ongeautoriseerde acties uit te voeren.

19. Insider threat: Een beveiligingsrisico dat komt van een persoon binnen de organisatie, zoals een medewerker die opzettelijk of per ongeluk vertrouwelijke gegevens lekt.

20. Keylogger: Een type malware of hardware dat toetsaanslagen registreert om vertrouwelijke informatie, zoals wachtwoorden, te stelen.

21. Hashing: Het proces van het omzetten van gegevens in een vaste, onomkeerbare code (hash) die wordt gebruikt om gegevensintegriteit te controleren.

22. SSL/TLS (Secure Sockets Layer/Transport Layer Security): Protocollen die worden gebruikt om gegevens te versleutelen tijdens de overdracht via netwerken, zoals internet.

23. Man-in-the-Middle Attack (MitM): Een aanval waarbij een aanvaller zich tussen twee communicerende partijen plaatst en hun communicatie onderschept of manipuleert zonder dat ze het weten.

24. Spyware: Software die zonder medeweten van de gebruiker informatie verzamelt en doorstuurt naar een externe partij.

25. Adware: Software die ongewenste advertenties weergeeft en mogelijk persoonlijke gegevens verzamelt.

26. Privilege escalation: Een aanval waarbij een aanvaller toegang verkrijgt tot hogere rechten of bevoegdheden dan oorspronkelijk is toegestaan.

27. Zero trust: Een beveiligingsmodel waarbij niemand, zelfs niet gebruikers binnen een netwerk, automatisch wordt vertrouwd. Verificatie is altijd nodig.

28. Data breach (Datalek): Een incident waarbij vertrouwelijke gegevens ongeautoriseerd worden ingezien, gestolen of openbaar gemaakt.

29. Security Information and Event Management (SIEM): Software die realtime beveiligings-waarschuwingen en loggegevens verzamelt en analyseert om verdachte activiteiten op te sporen.

30. Cyber Threat Intelligence: Het verzamelen en analyseren van gegevens over mogelijke cyberdreigingen, zodat organisaties zich beter kunnen verdedigen.

31. Incident Response (IR): De strategieën en procedures die een organisatie volgt om te reageren op een cyberaanval of datalek.

32. Red team/Blue team: Beveiligingsoefeningen waarbij het ‘Red Team’ probeert een systeem aan te vallen, terwijl het ‘Blue Team’ het probeert te verdedigen.

33. Whitelisting: Een beveiligingsmaatregel waarbij alleen goedgekeurde toepassingen of processen toegang krijgen tot een systeem of netwerk.

34. Blacklisting: Een beveiligingsmaatregel waarbij specifieke applicaties, websites of gebruikers worden geblokkeerd of beperkt.

35. Rootkit: Een type malware dat aanvallers volledige controle geeft over een systeem, vaak zonder dat de gebruiker dit opmerkt.

36. Cryptojacking: Het gebruik van een apparaat van een slachtoffer om cryptovaluta te minen zonder toestemming.

37. Backdoor: Een verborgen methode om ongeautoriseerde toegang te krijgen tot een systeem of applicatie.

38. Advanced Persistent Threat (APT): Een langdurige en gerichte cyberaanval waarbij aanvallers onopgemerkt blijven terwijl ze toegang houden tot een systeem.

39. Sandboxing: Het uitvoeren van software in een geïsoleerde omgeving om te voorkomen dat schade zich verspreidt naar de rest van het systeem.

40. Data Encryption Standard (DES): Een verouderd encryptie-algoritme dat is vervangen door krachtigere methoden zoals AES (Advanced Encryption Standard).

41. VPN (Virtual Private Network): Een technologie die een versleutelde verbinding creëert tussen een apparaat en een netwerk, waardoor de communicatie veilig en privé blijft.

42. Wi-Fi Protected Access (WPA): Een beveiligings-protocol voor draadloze netwerken dat gegevens versleutelt om toegang door ongeautoriseerde gebruikers te voorkomen.

Hosting:

Domein-gerelateerde begrippen

1. Domeinnaam: Het unieke adres van een website, zoals voorbeeld.nl.

2. TLD (Top-Level Domain): Het laatste deel van een domeinnaam, zoals .com, .org, of .nl.

3. ccTLD (Country Code TLD): Landenspecifieke domeinen, zoals .nl (Nederland) of .de (Duitsland).

4. Subdomein: Een toevoeging aan een domeinnaam, bijvoorbeeld blog.voorbeeld.nl.

5. DNS (Domain Name System): Een systeem dat domeinnamen vertaalt naar IP-adressen.

6. Name Server: Een server die verantwoordelijk is voor het beheren van DNS-records.

7. WHOIS: Een protocol waarmee je informatie kunt opvragen over de eigenaar van een domein.

Hosting-soorten

8. Webhosting: Een dienst waarmee websites beschikbaar worden gemaakt op het internet.

9. Shared hosting: Hosting waarbij meerdere websites dezelfde server delen.

10. VPS (Virtual Private Server): Een virtuele server met meer controle en resources dan shared hosting.

11. Dedicated server: Een server die volledig door één klant wordt gebruikt.

12. Cloud hosting: Hosting waarbij de website draait op een cluster van servers in plaats van op één fysieke server.

13. Managed hosting: Een hostingservice waarbij de provider de server volledig beheert.

14. Reseller hosting: Hosting waarmee gebruikers hostingpakketten kunnen doorverkopen.

Server-gerelateerde begrippen

15. Server: Een computer die diensten en resources levert aan andere computers (clients).

16. Load balancing: Het verdelen van verkeer over meerdere servers om de belasting te spreiden.

17. Uptime: De tijd dat een server operationeel is.

18. Bandwidth: De hoeveelheid data die een website kan versturen en ontvangen.

19. Caching: Het opslaan van data om de laadtijd van een website te versnellen.

Beveiliging en protocollen:

20. SSL/TLS (Secure Sockets Layer / Transport Layer Security): Encryptieprotocollen die zorgen voor veilige communicatie tussen een website en bezoekers.

21. HTTPS (HyperText Transfer Protocol Secure): Een veilige versie van HTTP met SSL/TLS.

22. Firewall: Software of hardware die ongeautoriseerd verkeer blokkeert.

23. DDoS (Distributed Denial of Service): Een aanval waarbij servers worden overspoeld met verkeer om ze offline te halen.

24. Backups: Kopieën van gegevens om verlies te voorkomen.

Website- en softwarebegrippen

25. CMS (Content Management System): Software zoals WordPress of Joomla om websites te beheren.

26. FTP (File Transfer Protocol): Een protocol om bestanden te uploaden naar een server.

27. cPanel/Plesk: Veelgebruikte beheerpaneel-software voor hostingaccounts.

28. MySQL/PostgreSQL: Databasesystemen die vaak worden gebruikt voor websites.

Technische begrippen

29. IP-adres: Een uniek nummer dat een apparaat op het internet identificeert.

30. IPv4/IPv6: Twee versies van IP-adressen, waarbij IPv6 meer adressen kan bieden.

31. PHP: Een programmeertaal die vaak wordt gebruikt voor dynamische websites.

32. Cron job: Een taak die op een server automatisch wordt uitgevoerd op een bepaald tijdstip.

33. Apache/Nginx: Veelgebruikte webserversoftware.

Managed Hosting:

Managed hosting is een type hostingdienst waarbij de hostingprovider verantwoordelijk is voor het beheer, onderhoud en technische ondersteuning van de server. Dit betekent dat je als gebruiker niet zelf voor het technische beheer van de server hoeft te zorgen. De provider neemt veel van de complexe en tijdrovende taken uit handen.

Kenmerken van managed hosting

1. Volledig beheer:
De provider zorgt voor de installatie, configuratie, monitoring en updates van de server en de software.

2. Beveiliging:
Beveiligingsupdates, firewallbeheer, malware-scans en bescherming tegen aanvallen zoals DDoS worden vaak inbegrepen.

3. Back-ups:
Regelmatige back-ups van de server om gegevens-verlies te voorkomen.

4. Monitoring:
Continu toezicht op de prestaties van de server om problemen vroegtijdig te detecteren.

5. Technische ondersteuning:
24/7 toegang tot experts die kunnen helpen bij technische problemen of vragen.

6. Schaalbaarheid:
Managed hosting biedt vaak de mogelijkheid om eenvoudig serverresources (zoals opslag of rekenkracht) uit te breiden naarmate je website groeit.

Voor- en nadelen

Voordelen
- Tijdsbesparing: Je hoeft zelf geen technische kennis te hebben of tijd te investeren in serverbeheer.
- Betere prestaties: Optimalisaties worden door experts uitgevoerd, wat resulteert in een snellere en betrouwbaardere website.
- Focus op je kernactiviteiten: Je kunt je richten op je website of bedrijf zonder zorgen over technische zaken.

Nadelen
- Kosten: Managed hosting is vaak duurder dan unmanaged hosting.
- Minder controle: Je hebt minder directe toegang tot de configuratie van de server, omdat de provider dit beheert.

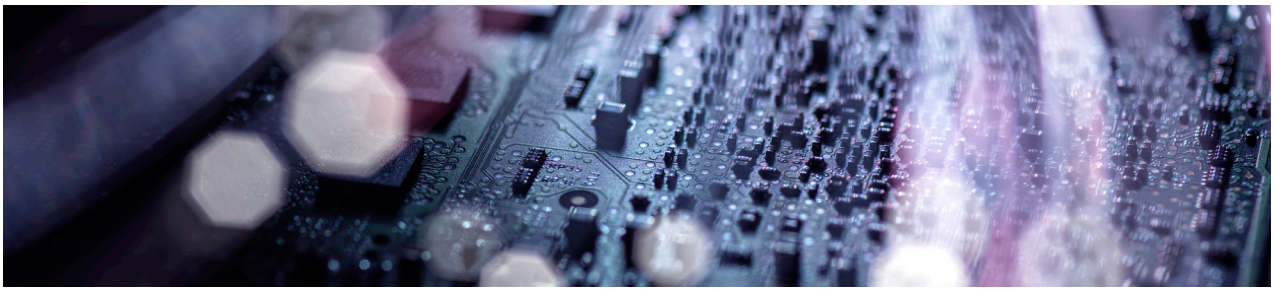
Wanneer kiezen voor managed hosting?

Managed hosting is ideaal als:
- Je weinig technische kennis hebt of geen tijd wilt besteden aan serverbeheer.
- Je een zakelijke website, webshop of applicatie hebt die altijd online moet zijn.
- Je waarde hecht aan optimale beveiliging en prestaties.

Voorbeelden van managed hosting zijn: Managed WordPress Hosting, Managed VPS en Managed Cloud Hosting.

Unmanaged Hosting

Unmanaged hosting is een hostingoptie waarbij de hostingprovider alleen de basisinfrastructuur van de server aanbiedt, terwijl jij zelf verantwoordelijk bent voor het beheren, configureren en onderhouden van de server. Dit betekent dat je meer controle hebt, maar ook meer technische kennis nodig hebt om alles goed te laten werken.



Kenmerken van unmanaged hosting

1. Basisinfrastructuur:
Je krijgt toegang tot een server (fysiek of virtueel), maar zonder aanvullende diensten zoals software-installaties of beheer.

2. Zelfbeheer:

Je bent verantwoordelijk voor:
- Het installeren en updaten van software (zoals een webserver of databases).
- Beveiligingsmaatregelen zoals firewalls en malwarebescherming.
- Het oplossen van technische problemen en fouten.

3. Geen ondersteuning bij configuratie:
De hostingprovider biedt alleen ondersteuning voor hardware- en netwerkgerelateerde problemen, zoals serveruitval.

4. Flexibiliteit:
Je hebt volledige controle over de serverconfiguratie, inclusief het kiezen van besturingssystemen, software en instellingen.

Voor- en nadelen

Voordelen
- Kosten: Unmanaged hosting is meestal goedkoper dan managed hosting.
- Volledige controle: Je kunt de server precies aanpassen aan jouw behoeften.
- Flexibiliteit: Je hebt de vrijheid om software en configuraties te kiezen die het beste passen bij jouw project.

Nadelen
- Technische kennis vereist: Je moet kennis hebben van serverbeheer, beveiliging en probleemoplossing.
- Tijdsinvestering: Het beheren van een server kan veel tijd en aandacht vergen.
- Geen uitgebreide ondersteuning: Als er problemen zijn, moet je ze zelf oplossen (behalve hardware- of netwerkproblemen).

Wanneer kiezen voor unmanaged hosting?

Unmanaged hosting is geschikt als:
- Je ervaring hebt met serverbeheer of een technisch team hebt dat dit aankan.
- Je volledige controle wilt over de serveromgeving.
- Je een beperkt budget hebt en extra kosten voor beheerdiensten wilt vermijden.
- Je een project hebt met specifieke eisen die niet standaard in managed hosting beschikbaar zijn.

Voorbeelden van unmanaged hosting zijn een onbeheerste VPS, dedicated server, of bepaalde cloudservices zoals AWS, Google Cloud en Microsoft Azure.

Vergelijking managed en unmanaged hosting

Managed Hosting

Voordelen :

1. Tijdsbesparing: De hostingprovider be-heert alle technische aspecten, waardoor je tijd kunt besteden aan je kernactiviteiten.

2. Gebruiksgemak: Geen technische kennis nodig; ideaal voor beginners of bedrijven zonder IT-afdeling.

3. Betere beveiliging: Regelmatige updates, monitoring en beveiligings-maatregelen worden door experts uitgevoerd.

4. 24/7 Ondersteuning: Technische hulp is beschikbaar om problemen snel op te lossen.

5. Back-ups inbegrepen: Automatische back-ups zorgen voor extra gemoedsrust.

6. Schaalbaarheid: Eenvoudig resources uitbreiden zonder zelf tech-nische wijzigingen aan te brengen.

Nadelen:

1. Kosten: Managed hosting is vaak duurder dan unmanaged hosting vanwege de extra diensten.

2. Minder controle: Je hebt beperkt toegang tot de serverinstellingen, omdat de provider alles beheert.

3. Beperkte flexibiliteit: Je bent gebonden aan de software en configuraties die de provider biedt.

Unmanaged Hosting

Voordelen:

1. Lagere kosten: Unmanaged hosting is goedkoper, omdat er geen beheerdiensten bij zitten.

2. Volledige controle: Je kunt de server volledig naar wens configureren, inclusief besturingssysteem en software.

3. Flexibiliteit: Geschikt voor complexe of unieke projecten met specifieke eisen.

4. Technische vrijheid: Je bent niet afhankelijk van de beperkingen van een hostingprovider.

Nadelen:

1. Technische kennis vereist: Je moet zelf ervaring hebben met serverbeheer en troubleshooting.

2. Tijdsintensief: Het beheren, beveiligen en onderhouden van een server kost veel tijd.

3. Geen uitgebreide ondersteuning: De hostingprovider helpt alleen bij hardware- of netwerkproblemen.

4. Risico op fouten: Onjuiste configuraties of verouderde software kunnen leiden tot beveiligingsproblemen of storingen.

Overzicht

Aspect	Managed Hosting	Unmanaged Hosting
Kosten	Duurder	Goedkoper
Controle	Beperkt	Volledig
Technische kennis	Niet nodig	Essentieel
Ondersteuning	24/7 technische ondersteuning	Beperkt tot hardware/network
Beveiliging	Beheerd door experts	Zelf verantwoordelijk
Flexibiliteit	Beperkt tot standaardopties	Volledig configureerbaar

Colofon

Eindredactie: Simon Besteman
Vormgeving: Argila marketingcommunicatie

Met dank aan:
Wido den Hollander
Wido Potters
Matthieu van Amerongen
Jacco Brouwer
Instituut Clingendael
Bert Hubert
Arnold Juffer
Ruud Alaerds
Dion Goudkuil
Marin Heideman
Jacqueline van de Werken
Mark Schouten
Hans Hendrikx
Rob Verbeek
Alle leden en partners van Dutch Cloud Community

www.dutchcloudcommunity.nl


De leden van Dutch Cloud Community
De partners van Dutch Cloud Community


Dutch Cloud
Community