Schriftelijke inbreng NLdigital

T.b.v. rondetafelgesprek inzake 'De consequenties van de (beoogde) overname van Solvinity voor DigiD'

Wij danken de Commissie Digitale Zaken voor deze gelegenheid om onze visie op het gebruik van cloud en digitale autonomie te geven. Zoals vooraf aangegeven is het bedrijf dat beoogt Solvinity over te nemen lid van NLdigital. Namens de branche spreken en schrijven wij nooit namens één individueel lid. Om deze reden geven wij in beginsel geen reacties op specifieke casussen.

Op 16 januari jongstleden hebben wij een explainer gepubliceerd die onze visie weergeeft op autonomie en cloudgebruik met de titel "Cloudgebruik en autonomie: risico's begrijpen, beoordelen en beheersen". Deze hebben we t.b.v. het rondtafelgesprek herschreven naar een versie die zoveel mogelijk ontdaan is van technisch jargon.

Specifiek voor deze casus

Wij hebben geen kennis over deze casus anders dan hetgeen openbaar bekend is. Om aan dit gesprek zo zinvol mogelijk bij te dragen helpt het om vast te stellen over welk type cloud- en/of beheersdiensten we het hier hebben. Daarom vermelden we hier de duiding van DigiD zelf met betrekking tot de verhouding tussen de Rijksoverheid en hun leverancier Solvinity:

> *"DigiD wordt beheerd door de Nederlandse overheidsorganisatie Logius, onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Solvinity levert het platform waar DigiD op draait. Dit platform draait in een overheidsdatacentrum. Dit maakt Solvinity een leverancier van DigiD, niet eigenaar."* - digid.nl/solvinity

Cloudgebruik en autonomie: Risico's begrijpen, beoordelen en beheersen

Waarom cloud relevant is

Cloudgebruik is voor veel organisaties geen keuze meer, maar een randvoorwaarde. Deze cruciale rol in de digitale economie in combinatie met grote geopolitieke verschuivingen leidt ertoe dat de discussie over digitale autonomie maatschappelijk hoog op de agenda is komen te staan. Met name voor publieke toepassingen is dit ook een prioriteit in de Nederlandse Digitalisering Strategie (NDS). NLdigital pleit ervoor deze discussie te voeren op basis van risico's en beheersmaatregelen. Niet met simplificaties als 'binnenlands is veilig' en 'buitenlands is risicovol', maar met volwassen risicomanagement dat past bij het type data en de mate waarin de toepassingen kritiek zijn.

Cloudtechnologie bestaat in vele soorten en maten, van een volledig maatwerksysteem tot generieke, publiek beschikbare oplossingen. Cloudoplossingen kunnen organisaties voordelen opleveren. Denk aan schaalbaarheid, flexibiliteit en snelle innovatie. Uitbesteding aan gespecialiseerde dienstverleners geeft bovendien vaak toegang tot moderne veiligheidsfunctionaliteit, en vaak ook een gunstiger energie- en kostenplaatje door schaal en standaardisatie.

Doel en afbakening

Dit document is bedoeld als praktische duiding van leveranciersrisico bij cloudgebruik in de context van digitale autonomie. Het betreft daarbij cloudgebruik van de bekende openbare publieke diensten tot volledig op maat gebouwde cloudoplossingen, en alles wat daar tussenin zit. Het biedt een kader om risico's te begrijpen, te beoordelen en te beheersen. In dit document doen we een handreiking voor de vragen die hierbij gesteld moeten worden, maar deze voorbeelden zijn niet uitputtend. De antwoorden hierop zijn niet in algemeenheid te geven, omdat de verscheidenheid in cloud-vormen en toepassingen zo groot is. Dit kader sluit aan bij bestaande beleidskaders als het Cloudbeleid Rijksoverheid (2022) en wettelijke vereisten uit de Cyberbeveiligingswet (o.a. exit plannen, cybersecurity-maatregelen), de Data Act (interoperabiliteit & keuzevrijheid) en AVG (eisen aan opslag gevoelige data).

NLdigital pleit ook voor het vergroten van investeringen in Europese oplossingen. Wij constateren dat de EU achter dreigt te blijven bij de VS en China. Lees daarover meer in onze reactie op het Rapport Wennink. Voor NLdigital is de cloud geen zero-sum game, we kunnen een open economie die internationaal profiteert van buitenlandse innovatie combineren met meer eigen investeringen en het verhogen van onze autonomie.

Wat is leveranciersrisico in de context van digitale autonomie?

Leveranciersrisico omvat alle situaties waarin de beschikbaarheid, betrouwbaarheid of keuzevrijheid ten aanzien van een dienst of product wordt beïnvloed door factoren buiten directe controle van de klant. In de context van digitale autonomie gaat het om de vraag hoeveel controle je uit handen geeft, en welke risico's dat met zich meebrengt voor vertrouwelijkheid, integriteit (zijn gegevens ongewijzigd en betrouwbaar) en beschikbaarheid van data en diensten. Risico's bestaan in elke keuze. Bij eigen beheer ben je bijvoorbeeld afhankelijk van hardwarecomponenten, firmware (laag tussen hardware en software), open source onderdelen en gespecialiseerde kennis, die vaak internationaal van aard is. Dat maakt niet dat alle afhankelijkheden gelijk zijn.

Kans en impact verschillen sterk per leverancier, per dienst en per organisatie. Het gaat erom verschillen expliciet te maken en keuzes te onderbouwen. Bij het nemen van besluiten over uitbesteding in de digitale wereld is samenwerking met anderen onontkoombaar. Daarom moeten voordelen ook worden meegewogen in samenhang met risico's: niet alleen het risico van iets wél doen telt, ook het risico van iets níet doen. De vraag is wat tot het meest controleerbare risiconiveau leidt.

Herkomst alleen is te simpel

In het publieke debat wordt de herkomst van een cloudleverancier soms gebruikt als snelle indicator voor betrouwbaarheid. Dat is in de praktijk te kort door de bocht. Vooral bij publieke cloud- en beheerdiensten speelt de vraag wat de relevante jurisdictie is: onder welke wetgeving valt de leverancier, en welke verplichtingen kan die wetgeving opleggen, ook als data fysiek in Europa staat. Wetgeving rond data-verzoeken bestaat in meerdere jurisdicties (VS CLOUD Act, EU e-evidence). De vraag is niet óf overheden toegang kunnen vorderen, maar welke waarborgen, transparantie en rechtsbescherming gelden. Daarom hoort 'jurisdictie en toepasselijk recht' standaard op de checklist bij leverancierskeuzes.

Maar ook bij uitbesteding van beheer van private clouds spelen op dit vlak vragen. Het is daarbij van belang wie bij systemen en data kunnen, en hoe de toegang gecontroleerd wordt. Het scenario waarin de leverancier vanuit de gehele wereld beheer kan uitvoeren op jouw systemen verschilt wezenlijk van het scenario waarin toegang tot enkele specifieke personen in dezelfde jurisdictie als de afnemer beperkt is.

Duidelijke contractuele afspraken zijn noodzakelijk om deze zaken te beheersen. Maar sommige wettelijke verplichtingen van een leverancier kunnen niet contractueel worden uitgesloten. Deze kunnen in een deel van de gevallen door technische maatregelen zoals versleuteling waarbij de leverancier de data niet kan ontsleutelen, strikte toegangscontrole tot fysieke opslaglocaties en het aanbrengen van virtuele muren tussen systeemnetwerken in de praktijk juist wél het risico substantieel reduceren.

De afweging tussen controle en capaciteit

Meer controle klinkt aantrekkelijk, maar controle vraagt om investeringen: specialistische kennis, continue beveiliging, compliance en schaal om bij te blijven met snelle technologische ontwikkelingen. Daarom is de kernvraag niet 'alles zelf doen of alles uitbesteden?', maar waar op het spectrum de juiste balans per toepassing ligt. Wat voor staatsgeheimen onacceptabel is, kan voor een standaard bedrijfsproces beheersbaar zijn.

Als je het tot het extreme doortrekt: een keuze voor maximale soevereiniteit zonder passende investeringen kan leiden tot een slechter beveiligingsniveau en daarmee tot minder weerbaarheid. De risico's door statelijke actoren en kwaadwillende insiders kunnen daardoor groter en acuter worden dan de risico's die je wilde oplossen. Het streven naar controle, naar autonomie en keuzevrijheid, is alleen mogelijk met realistische keuzes die passen bij de gewenste toepassing, beschikbare middelen, dreigingsbeeld en wettelijke eisen.

Gebruik beschikbaarheid, integriteit en vertrouwelijkheid als kader

Een praktische manier om leveranciersrisico te structureren is aan de hand van drie veiligheidsdoelen die breed worden toegepast in cybersecurity: beschikbaarheid, integriteit en vertrouwelijkheid. Per toepassing kun je hiermee expliciet maken wat het belangrijkste is, en welke maatregelen nodig zijn.

Beschikbaarheid: hoe zeker is toegang wanneer nodig?

Kernvragen hierbij zijn: zijn systemen bereikbaar bij technische storingen, incidenten of juridische beperkingen? Wat zijn de directe gevolgen wanneer een dergelijk incident optreedt? Kan een leverancier ondersteunen bij incidentbestrijding en hoe snel? Welke back-up en herstel afspraken zijn er, en is overstappen in een noodscenario realistisch?

Integriteit: wie kan wat wijzigen?

Wie kan software updates doorvoeren en hoe wordt dat gecontroleerd? Welke controles zijn er op wijzigingen? Is er een vier ogen principe voor kritieke wijzigingen, worden alle handelingen geregistreerd en/of is er onafhankelijke controle op beheerhandelingen?

Vertrouwelijkheid: wie heeft toegang tot wat?

Wie kan bij de data en wie kan bij de systemen? Is toegang alleen mogelijk tijdens beheeractiviteiten, of is er permanente toegang? Worden rechten technisch afgedwongen of alleen contractueel geregeld? En onder welke jurisdictie vallen organisatieonderdelen en medewerkers die beheer uitvoeren?

Welke scenario's moet je doordenken?

Leveranciersrisico is breder dan alleen technische 'uitval'. Het is verstandig om ten minste de volgende scenario's expliciet te doordenken, inclusief waarschijnlijkheid, impact en waarschuwingssignalen:

Juridische scenario's

- Kan wetgeving in het land waar de leverancier onder valt verplichtingen opleggen tot gegevensverstrekking of beperking van toegang, zowel op organisatieniveau als voor individuen?
- Wat betekent dit voor verschillende typen data, bijvoorbeeld persoonsgegevens, bedrijfsgeheimen en operationele gegevens?
- Welke technische en organisatorische maatregelen beperken risico's, bijvoorbeeld versleuteling waarbij de leverancier geen toegang heeft tot de ontsleutelingsmogelijkheden?

Geopolitieke en handel scenario's

- Wat is de impact van verslechterende relaties, sancties of exportrestricties op dienstverlening, updates en support?
- In welke mate zijn ketens verweven? Ook Nederlandse en Europese bedrijven zijn onderdeel van wereldwijde waardeketens.
- Welke exit- en continuïteitsopties bestaan als omstandigheden snel veranderen?

Cybersecurity scenario's

- Wat is de kans op ransomware, aanvallen op de leveranciersketen, onjuiste configuraties, kwetsbaarheden in afhankelijkheden of identiteitsmisbruik? En hoe wordt dit risico beheerst?
- Hoe snel detecteert en reageert de leverancier op incidenten? Is dit vastgelegd zoals de Cyberbeveiligingswet (NIS2) vereist, in samenhang met leveranciersketen en bedrijfscontinuïteit?

Leverancierscontinuïteit scenario's

- Heeft de leverancier zijn beveiliging op orde? Zijn er onafhankelijke controles en beoordelingsrapporten die aantonen dat beveiliging op orde is?
- Wat als de leverancier wordt overgenomen, failliet gaat, een product uit faseert of aanpassingen vereist voor de nieuwste versie?
- Hoe afhankelijk ben je van unieke functionaliteit die elders niet beschikbaar is?
- Wat betekent wijziging van voorwaarden of kosten voor jouw continuïteit en wettelijke plichten?

Van vertrouwen naar verificatie

De les uit moderne beveiligingsarchitecturen is dat vertrouwen alleen onvoldoende is: de herkomst van een bedrijf levert geen veiligheid op zichzelf. Een benadering waarin je voortdurend controleert in plaats van blind vertrouwt, hoort de norm te zijn. Dat betekent technische verificatie, strikte controle op wie waartoe toegang heeft, opsplitsing van systemen, registratie van alle handelingen, controles en monitoring, ongeacht de nationaliteit van de leverancier.

Daarbij geldt dat cloudbeheersing een gedeelde verantwoordelijkheid is. Leveranciers kunnen aantoonbare technische en organisatorische maatregelen bieden, maar afnemers krijgen alleen controle door zelf ook verantwoordelijkheid te nemen voor zaken als het categoriseren van data naar gevoeligheid, beheer van toegangsrechten, configuratiebeheer en het beheren van versleuteling. Digitale autonomie kan niet verkregen worden wanneer het risico vooral uitbesteed wordt.

Diversificatie en voorkomen van leveranciersafhankelijkheid

Naast technische maatregelen kan diversificatie van leveranciers risico's spreiden. Dat kan via het combineren van verschillende cloudvormen of meerdere cloudleveranciers, of door kritieke componenten onder strenger

geselecteerde jurisdicties te plaatsen. Dit is geen doel op zich. Voor sommige organisaties verhoogt diversificatie de beheercomplexiteit, en daarmee het operationele risico. De afweging hangt af van het risicoprofiel, de volwassenheid van de organisatie en hoe kritiek de toepassing is.

Los van diversificatie is het voorkomen van leveranciersafhankelijkheid vaak cruciaal voor digitale autonomie. Scenario's voor het beëindigen van de samenwerking en het kunnen meenemen van data horen vanaf de start onderdeel te zijn van een cloudstrategie, en niet alleen voor uiterste gevallen. Regelgeving zoals de Data Act bevat uitgangspunten voor overstappen en samenwerking tussen aanbieders. Organisaties doen er goed aan om dit te vertalen naar contractuele afspraken (inclusief softwarelicenties), technische architectuurkeuzes en periodieke testen van overstapplannen.

Praktische handvatten voor organisaties en leveranciers

Organisaties die clouddiensten afnemen kunnen met leveranciers een gerichte dialoog voeren over risico's en beheersmaatregelen. IT-leveranciers en dienstverleners kunnen dit kader gebruiken om klantvragen te beantwoorden en transparant te maken hoe zij risico's beperken.

- Ga risico's niet uit de weg maar identificeer en adresseer ze.
- Categoriseer data en processen naar gevoeligheid en bepaal per categorie het gewenste risicoprofiel. Vraag om inzicht in beheerprocessen, toegangsmodellen en onderaannemers.
- Zorg voor maatregelen als fysieke toegangsbeveiliging, versleuteling, beheer van de digitale sleutels voor versleuteling, minimale toegangsrechten en monitoring.
- Vraag om aantoonbaarheid via onafhankelijke controles en beoordelingsrapporten, waar passend.
- Neem eigen controle waar digitale autonomie noodzakelijk is. Leg continuïteit en exit-eisen vast, en test deze periodiek.

Tot slot

De discussie over digitale autonomie in de context van verantwoord cloudgebruik verdient beter dan zwart-wit frames. Niet alles moet per definitie 'soeverein' zijn, en geen enkele oplossing is risicoloos. Wat wél werkt is per toepassing een bewuste keuze maken op basis van concrete risico's en aantoonbare maatregelen. De digitale sector kan hierin een constructieve rol spelen door organisaties te helpen de juiste vragen te stellen en passende maatregelen te treffen.