CLOUD-STRATEGIEËN BIJ BUITENLANDSE OVERHEDEN

KRISTOF VERSLYPE

Abstract. Voor overheden wereldwijd stelt zich de vraag welke houding aan te nemen tegenover het gebruik van de cloud. Vooral met betrekking tot gevoelige gegevens kan dit vraagtekens oproepen. Deze research note gaat in op de stategieën die buitenlandse overheden hierrond aannemen. Er wordt niet enkel ingezoomd op Nederland, Frankrijk, Duitsland, het Verenigd Koninkrijk en de Verenigde Staten, maar ook een aantal andere landen komen ter sprake. De trend is dat overheden in de bekeken landen gevoelige gegevens onder de eigen jurisdictie houden, wat zich vertaalt in het houden van deze gegevens binnen de eigen landsgrenzen en samenwerking met eigen, nationale spelers. Ten slotte wordt de situatie in België bekeken.

Résumé. Pour les administrations publiques à travers le monde, la question est de savoir quelle attitude adopter face à l'utilisation du cloud. Notamment en ce qui concerne les données sensibles, il y a matière à s'interroger. Cette research note est consacrée aux stratégies que les administrations publiques étrangères appliquent à cet égard. Non seulement les Pays-Bas, la France, l'Allemagne, le Royaume-Uni et les États-Unis sont passés en revue, mais aussi d'autres pays sont abordés. La tendance est que les autorités des pays étudiés tiennent des données sensibles de leur propre juridiction, de sorte qu'elles tiennent ces données à l'intérieur de leurs frontières et qu'elles collaborent avec leurs propres acteurs nationaux. Enfin, la situation en Belgique est analysée.

Contents

1. Inleiding

De cloud eist een steeds prominentere rol op in het IT-landschap. Er kan relatief snel gebruik van gemaakt worden, biedt een ongekende flexibiliteit en dit tegen lage prijzen. Voor overheden stelt zich dan de vraag welke houding aan te nemen tegenover het gebruik van de cloud. Vooral met betrekking tot gevoelige gegevens kan dit vraagtekens oproepen. We onderzochten de situatie in een aantal landen, zonder daarbij te claimen exhaustief te zijn.

2. Nederland

Nederland had een tweetal jaar terug beslist richting een gesloten overheidscloud te gaan die in Nederland gelokaliseerd zou worden en die door de overheid zelf beheerd zou worden, zoals blijkt uit onderstaande fragmenten uit een brief aan de Kamer op 20 april 2011.

> *"Wat informatiebeveiliging betreft blijkt dat het via een 'open' cloud uitbesteden van ICT-diensten, dan wel opslag van informatie buiten Nederland, risico's met zich meebrengt die nog niet voldoende kunnen worden afgedekt."*
>
> *"Het aantal leveranciers en cloud-diensten is vrij groot, maar slechts een klein deel daarvan is bedrijfsmatig volwassen genoeg om daadwerkelijk ingezet te kunnen worden voor de Nederlandse overheid."*
>
> *"Het kabinet kiest er daarom voor om een gesloten Rijkscloud in eigen beheer in te richten als een voorziening die **generieke diensten** levert binnen de Rijksdienst. Deze voorziening wordt ingericht **binnen een eigen beveiligd netwerk en wordt beheerd door een eigen, rijksbrede organisatie**."*

Helaas is het sindsdien wat stil geworden hierrond, en is het onduidelijk hoever dit project momenteel staat.

Het Nederlandse *KPN* heeft een volledig Nederlandse cloud opgezet onder de naam *CloudNL*. De gegevens die daar verwerkt worden blijven dus in Nederland en worden door een Nederlandse Telco beheerd. *KPN* kondigde in september 2012 aan dat de overheidsdienst *UWV* (Uitvoeringsinstituut Werknemersverzekeringen) als eerste gebruik zou maken van *CloudNL* door 20.000 werkplekken er naartoe te brengen. Het UWV reageerde daarop door te stellen dat *CloudNL* maar één van de bekeken opties was, wat door *KPN* toegegeven moest worden.

3. Frankrijk

In april en mei vorig jaar werd de vorming van twee consortia aangekondigd: *Cloudwatt* en *Numergy*. Elk consortium staat in voor de bouw en het beheer van zijn cloud. In beide pompte de regering 75 miljoen euro in ruil voor een belang van 1/3. De resterende 2/3 wordt bij *Cloudwatt* gevormd door *Orange* en *Thales* en bij *Numergy* door *SFR* en *Bull*. Deze vier bedrijven zijn alle Frans.

Eerder had *Dassault Systèmes* aangekondigd uit *Cloudwatt* te stappen aangezien het niet langer geloofde dat het project voldoende competitief kon worden. *Orange* en *Thales* benadrukten dan weer het extra vertrouwen in hun consortium in vergelijking met de concurrentie.

De eerste toepassingen van *Cloudwatt* zullen zich richten op de opslag, de synchronisatie en het delen van bestanden en zullen tussen juni en september beschikbaar gemaakt worden. In een volgende fase zullen er virtuele machines aangeboden worden. Hun nieuwe datacenter is tier 4 gecertificeerd, wat de hoogst mogelijke categorie is en dus onder meer een beschikbaarheid van 99.995 % garandeert. *Numergy* biedt reeds virtuele machines en servers aan en vanaf september zal ook opslag voorzien worden. De *Numergy* datacenters zijn tier 3+ gecertifieerd.

Cloudwatt en *Numergy* richten zich zowel op ondernemingen als overheden.

4. Duitsland

In Duitsland verdedigde Hans-Peter Friedrich, de minister van Binnenlandse Zaken, in december 2011 het gelijkaardige idee voor een 'Bundescloud' voor de overheden. Deze zou aan strenge veiligheidsvereisten moeten voldoen. Er zouden gesprekken geweest zijn tussen de regering, T-systems (een dochter van Deutsche Telekom) en het BSI (Bundesambt für Sicherheit in der Informationstechnik, wat de nationale overheidsdienst voor informatieveiligheid is). Daarnaast werd het idee gelanceerd om cloudaanbieders en hun producten te certificeren om zo potentiële afnemers van cloud-diensten te overtuigen de cloud te gebruiken.

Een Bundescloud wordt momenteel gerealiseerd in twee initiatieven: de *Deutsche Wolke* en de *Trusted Cloud*.

Een verbond van zowel Duitse als internationale organisaties startte in 2005 met de uitbouw van een "*cloud made in Germany*" onder de naam *Deutsche Wolke* en is onderdeel van de *Open Source Business Alliance*. Het project werd voor het eerst officieel voorgesteld op *CeBit 2011*. De *Deutsche Wolke* maakt enkel gebruik van open-source software, bevindt zich uitsluitend in Duitsland en enkel Duitse bedrijven kunnen bij het beheer en de uitbating betrokken worden. Er wordt gebruikgemaakt van datacenters verspreid over het land waarbij de gegevens geografisch ontdubbeld worden. De *Deutsche Wolke* wil voldoen aan de strengste veiligheidsrichtlijnen en wil transparant en betrouwbaar zijn.

Momenteel zou de *Deutsche Wolke* de volgende diensten aanbieden:

- IaaS (Infrastructure as a Service), gebruikmakend van Het Duitse *Univention*, Het Duitse *SuSe* en het Amerikaanse *RedHat*.
- DMS (Document Management System), gebruikmakend van Het Duitse *Agorum*.
- Groupware, gebruikmakend van de Europese *Zarafa*-applicatie.
- CRM (Customer Relationship Management), gebruikmakend van het Duitse *Information Desire*.
- ERP (Enterprise Resource Planning), gebruikmakend van het Oostenrijkse *HeliumV*.

In de toekomst zou het aanbod verder uitgebreid worden met sociale media, business continuity services en virtuele desktops.

Het door de Duitse overheid in 2011 gestarte technologieprogramma '*Trusted Cloud*' heeft als doel het ontwikkelen en testen van innovatieve, veilige en rechtsconforme cloudcomputing-oplossingen en ontvangt 50 miljoen euro aan overheidssteun en nog eens ongeveer 50 miljoen van de privépartners. De *Trusted Cloud* richt zich niet alleen op KMO's, maar ook op de gezondheidszorg en publieke sector. Bij diverse projecten voor de publieke diensten en gezondheidszorg (*Cloud4health, GeneCloud, TRESOR, CloudCycle* en *goBerlin*) wordt overwegend samengewerkt met Duitse bedrijven en Duitse universiteiten, maar ook met een aantal buitenlandse bedrijven zoals *IBM* en *Atos*.

Het publieke debat leek zich de afgelopen periode te concentreren rond de toenemende controle die de Duitse regering via de cloud wil uitoefenen. De Duitse overheid zou zelfs toegang hebben tot gegevens in Amerikaanse cloud-diensten. Een dergelijk klimaat kan de uitbouw van een Bundescloud wel bemoeilijken wanneer een zich in bredere weerstand omzettende vrees bestaat dat dit een stap is in de verdere uitbouw van een nieuwe Duitse Überwachungsstaat. De recente onthullingen omtrent afluisterpraktijken door onder meer de Verenigde Staten en het Verenigd Koninkrijk kunnen enerzijds resulteren in een autarkische reflex, maar anderzijds kan het een algemeen wantrouwen tegenover 'de cloud' stimuleren.

5. Verenigd Koninkrijk

Het Verenigd Koninkrijk bouwt zijn *G-Cloud* uit. Ondernemingen kunnen er hun diensten in een centrale catalogus laten opnemen, waardoor de overheden en ambtenaren makkelijker de weg vinden naar cloud-diensten. Contracten en betalingen kunnen via het *G-Cloud*-platform geregeld worden. Het project kreeg af te rekenen met heel wat kritiek[1,2,3] wat niet abnormaal is voor grote projecten. Momenteel bieden 450-500 aanbieders - waarvan ¾ KMO's – 3000 à 3500 diensten aan via de *G-Cloud* en de regering kondigde aan dat er via de *G-Cloud* reeds een omzet van 18,2 miljoen pond gerealiseerd werd. Twee bemerkingen daarbij zijn:

1) Het overgrote deel van de contracten gaat op dit moment naar consultancy.
2) Eén van de drijfveren van de *G-Cloud* is het geven van kansen aan de eigen, lokale spelers, om toch maar niet overrompeld te worden door *Google*, *Amazon*, etc.

De Britse overheid hanteert sinds kort een *cloud first-beleid*. Indien de on-premise en cloud-alternatieven gelijkwaardig zijn, dan wordt gekozen voor een cloud-oplossing. De overheden zelf blijven weliswaar risicomijdend wanneer het om gevoelige gegevens gaat.

In het Verenigd Koninkrijk wordt een classificatie voor gevoelige gegevens gehanteerd, lopend van *IL0* (*No impact*) tot *IL6* (*Top secret*). Om het veiligheidsniveau van gegevens te bepalen, zijn er zes tabellen beschikbaar.

- Defence, International Relations, Security and Intelligence

[1] *Is it all over for UK.gov's G-Cloud 3.0? A footnote in history awaits*. Gavin Clarken, The Register, 4 december 2012

[2] *U.K. Government Cloud Ambitions Bigger Than Achievements, Critics Say*. Gary Flood, InformationWeek. 20 februari 2013

[3] *Has the G-Cloud been a success?* Alastair Mitchell, ITProPortal, 11 maart 2013

- Public Order, Public Safety and Law Enforcement
- Trade, Economics and Public Finance
- Public Services
- Critical National Infrastructure (CNI)
- Personal / Citizen

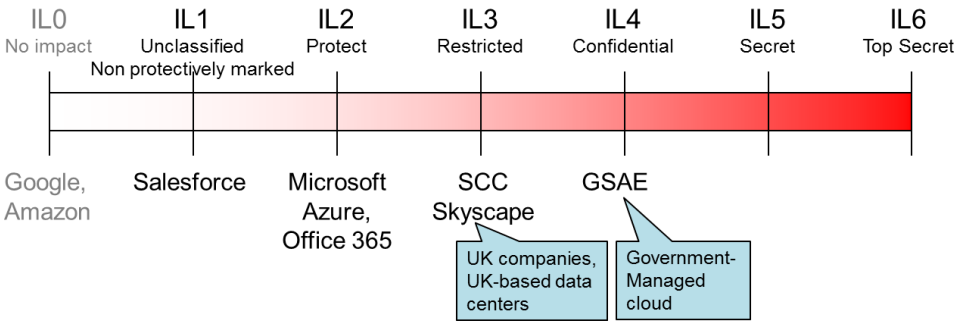
Figuur 1 toont een uittreksel uit de tabel *'Personal / Citizen'* tot (business)impact level IL4 voor het bepalen van de impact op de burger.

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4
Impact on health and safety of the Citizen	None	Minor injury or illness with a quick (within one week) and complete recovery to an individual	Compromise an individual's personal safety or security.	Minor injuries to a group of individuals or serious injury to an individual involving slight to moderate pain for 2-7 days. Thereafter some pain/discomfort for several weeks. Some restrictions to work and/or leisure activities over several weeks/months. After 3-4 months return to normal health with no permanent disability.	Serious injury to several individuals or compromise of a group of individuals personal safety
Impact on the Privacy of the Citizen	None	Loss of control of a citizen's personal data beyond those authorised by the citizen.	Loss of control of many citizens' personal data beyond those authorised by each citizen.	Loss of control of a citizen's sensitive data beyond those authorised by the citizen. A compromise to the identity or financial status of an individual citizen.	Loss of control of many citizens' sensitive or financially significant personal data beyond those authorised by each citizen. A compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack.
Impact on the Identity of the Citizen.	None	Illicit access using one individual's identity on behalf of another would cause inconvenience to the victim.	Illicit access using one individual's identity on behalf of another would allow the entry of incorrect information, thereby causing distress, or access to payments intended for that person or could further a subsequent impersonation attack on that individual.	Illicit access using several individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on several individuals.	Illicit access using many (thousands of) individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on many individuals.

Figuur 1. Uittreksel uit de tabel 'Personal / Citizen' voor het bepalen van het impactlevel betreffende de burger.

Bedrijven kunnen accreditaties bekomen voor hun cloud-diensten bij de overheidsinstantie CESG[4]. De voornaamste worden getoond in Figuur 2. *Google*, *Gmail* en *Amazon* hebben op dit moment geen accreditaties en mogen dus enkel voor gegevens van IL0 gebruikt worden. *Salesforce* heeft een accreditatie voor IL1, *Microsoft Office 365* en *Microsoft Azure* kregen IL2 (*PROTECT*). *SCC* en *Skyscape*, beiden Britse bedrijven met datacenters in het Verenigd Koninkrijk, kregen elk een IL3-accreditatie (*RESTRICTED*). IL4-gegevens (*CONFIDENTIAL*), ten slotte, mogen momenteel enkel in de GSAE (Government Secure Applications Environment) bewaard worden, wat een door de overheid beheerde cloud is. IL5- (*SECRET*) en IL6-gegevens (*TOP SECRET*) komen sowieso niet in de cloud.

[4] *CESG* (oorspronkelijk *Communications-Electronics Security Group*) levert ondersteuning aan overheidsinstellingen betreffende communicatieveiligheid. De *CESG* is onderdeel van de *GCHQ* (*Government Communications Headquarters*), de Britse inlichtingendienst die verantwoordelijk is voor het capteren en analyseren van elektronische informatiestromen.



Figuur 2. Belangrijkste accreditaties in de G-Cloud

Het Verenigd Koninkrijk heeft een vrij verfijnd classificatiesysteem, maar ook hier zien we dat de iets gevoeligere gegevens het land niet verlaten en door de overheid of Britse bedrijven beheerd worden. Wel bouwen buitenlandse bedrijven zoals *Oracle* en *SalesForce* datacenters in het Verenigd Koninkrijk met het doel om hogere accreditaties te bekomen om zo toch in aanmerking te komen voor meer overheidsopdrachten, niettegenstaande de bezorgdheden in het Verenigd Koninkrijk betreffende de verwerking van gevoelige gegevens door Amerikaanse bedrijven.

6. Verenigde Staten

De federale overheden in de Verenigde Staten hanteren een cloud first strategy. Diverse bedrijven nemen dan ook initiatieven richting de overheid. Zo biedt *Microsoft Office 365* aan in een afgeschermde community-cloud die enkel voor ambtenaren toegankelijk is. Ook *Amazon* biedt met zijn *GovCloud* een afgescheiden omgeving aan, waarin extra veiligheidsmaatregelen van toepassing zijn om te voldoen aan reguleringen zoals *ITAR*[5] en *FedRAMP*[SM6]. De *Amazon GovCloud* garandeert dat zowel logische als fysieke toegang enkel door burgers van de Verenigde Staten zelf gebeurt. Ook de Amerikaanse overheden lijken dus te kiezen voor de eigen nationale spelers, met dat verschil dat deze nationale spelers vaak ook de dominante internationale spelers zijn.

Anderzijds werd de in 2009 gelanceerde *Cloud Store* eind 2012 stilgelegd. Dit initiatief was vergelijkbaar met de Britse *G-cloud*-catalogus in die zin dat het als doel had via een centrale catalogus makkelijk cloud-diensten aan te bieden aan overheden.

Tot voor kort beschikten de Amerikaanse overheden over zo'n 3000 datacenters[7]. In het kader van het *Federal Data Center Consolidation Initiative (FDCCI)* tracht men dit tegen 2015 met 40 % af te bouwen, waarbij er meer gebruikgemaakt zou moeten worden van cloud-principes. Hoe deze federale cloudomgevingen zich

[5] *International Traffic in Arms Regulations* (*ITAR*) is een overheidsregulering voor de in- en uitvoer van goederen en diensten gerelateerd aan Defensie.

[6] Het *Federal Risk and Authorization Management Program* (*FedRAMP*) is een overheidsbreed programma dat een gestandaardiseerde aanpak aanbiedt voor veiligheidsassessments, authorisatie en permanente monitoring voor cloudproducten- en diensten.

[7] Het krijgen van een overzicht van alle datacenters van de Amerikaans overheden blijkt geen makkelijke taak.

zullen verhouden tot de cloudomgevingen van de privéondernemingen zoals *Amazon* en *Microsoft* is nog onduidelijk, maar allicht zal ook hier veel afhangen van de gevoeligheid van de gegevens en de mogelijke schaalvoordelen. Het plan om het aantal datacenters terug te dringen, betekent overigens niet dat ze zelf geen nieuwe meer bouwt. Zo is de *NSA*[8] momenteel bezig met de bouw van het Utah Data Center, wat qua oppervlakte het derde grootste ter wereld zal worden.

7. Andere landen

In **Oostenrijk** komen ondernemingen zoals *Google* en *Microsoft* niet in aanmerking voor gebruik door overheden en ambtenaren. Het is ambtenaren op nationaal niveau zelfs verboden e-mails door te sturen naar Gmail-accounts.

In **Noorwegen** is het gebruik van Google Apps door overheidsinstanties verboden en recentelijk nam ook de **Zweedse** overheid dezelfde beslissing.

In **Australië** bouwen verschillende cloud-aanbieders datacenters specifiek voor de publieke sector. Om een certificering te verkrijgen moeten ze voldoen aan hoge veiligheidsstandaarden. Zo zal het nieuwste datacenter van het Australische *Macquarie Telecom* zich in een bunker bevinden. Ook *Telstra*, de grootste Australische telco, bouwt lokaal datacenters om aan de data sovereignty requirements te voldoen, maar ook connectiesnelheid is een belangrijk argument in het uitgestrekte en geïsoleerde continent. *Telstra* wil cloud-diensten aanbieden aan zowel de overheid als ondernemingen. Australië heeft sinds kort een cloud first strategy met een bijhorende set regels om de cloud-adoptie in de publieke sector te versnellen. Momenteel wordt de *G-Cloud* in het Verenigd Koninkrijk door sommige politici in Australië als een na te streven voorbeeld beschouwd.

De **Singaporese** overheid heeft contracten afgesloten voor de bouw van een private cloud.

8. België

Doen we deze oefening over voor België, dan vinden we het volgende:

- Gemeentelijke overheden nemen hier en daar beperkte initiatieven. Houthalen-Helchteren maakt bijvoorbeeld gebruik van de cloud voor de e-mails en kalenders van haar personeel.
- De Vlaamse overheid wil Drupal as a Service kunnen aanbieden.
- *Capgemini* hielp de *VDAB* met de migratie van zijn 7000 mail-, agenda- en samenwerkingstoepassingen naar Google Apps. Bemerk dat dit in Oostenrijk, Noorwegen en Zweden niet toegelaten is.
- *Fedict* heeft op 4 mei 2013 een openbare aanbesteding gepubliceerd in het kader van de uitbouw van een cloud-infrastructuur voor de federale overheidsdiensten.

[8] Het *National Security Agency* (*NSA*) is een veiligheidsorganisatie van de Amerikaanse overheid die gespecialiseerd is in het afluisteren en analyseren van met name elektronische informatie uit communicatie via bijvoorbeeld telefonie en internet en het zo nodig ontcijferen van deze informatie via cryptoanalyse (Bron: Wikipedia).

9. Conclusie

Overheden wereldwijd stimuleren enerzijds wel het gebruik van de cloud in overheidscontext, maar anderzijds wordt ervoor gezorgd dat de gevoelige gegevens volledig en enkel onder de juridische bevoegdheid van het eigen land vallen. Dit wordt onder meer gerealiseerd door ervoor te zorgen dat enerzijds gegevens het nationale territorium niet verlaten en anderzijds dat de gegevens beheerd worden door hetzij een overheidsinstantie, hetzij door nationale bedrijven, hetzij door een samenwerking tussen beide. Het huidige dienstenaanbod in de verschillende landen varieert sterk.

De overwegingen lijken bovendien niet enkel te komen vanuit datasecurity-oogpunt, maar ook vanuit economische motieven, waarbij nationale overheden de eigen bedrijven kansen willen geven om cloud-diensten aan te bieden - gaande van IaaS en PaaS tot SaaS - en willen voorkomen dat de cloud-markt gedomineerd wordt door buitenlandse spelers.

In België zijn op nationaal vlak enkel *Fedict* en de *VDAB* zichtbaar in het cloud-landschap, al moet vermeld worden dat er nog diverse andere initiatieven zijn die voorlopig buiten de radar van de media blijven.