08.09.2015 - OVERHEIDSDATA IN DE CLOUD: IS ER EEN HEMELSE TOEKOMST VOOR ONZE RIJKSGEGEVENS?

Advocatenkantoor time.lex onderzocht de veiligheid en betrouwbaarheid van cloud diensten voor de opslag van Vlaamse overheidsgegevens in juridisch-politieke context.

Wanneer zij bepaalde overheidsgegevens in een publieke cloud wensen te stockeren zullen de Vlaamse overheidsdiensten mogelijk met juridische conflictsituaties geconfronteerd worden naar aanleiding van strijdige rechtstelsels. Teneinde aan haar verplichtingen met betrekking tot de vertrouwelijkheid en beschikbaarheid van overheidsgegevens te voldoen lijkt het uitgesloten dat de overheid standaardcontracten kan afsluiten met de meeste bekende cloudaanbieders.

Aangezien meerdere landen zichzelf extraterritoriale bevoegdheden hebben toegekend met betrekking tot kennisname van gegevens opgeslagen in de cloud, is het echter geen goed criterium om een cloudaanbieder af te schrijven louter omwille van het feit dat deze onderworpen is aan het Amerikaanse recht.

Een adequaat niveau van encryptie is ten zeerste aangeraden vooraleer gevoelige data zoals bijvoorbeeld gegevens uit het Rijksregister aan een cloudaanbieder worden toevertrouwd.

Een onderzoek naar de veiligheid van clouddiensten impliceert het aftoetsen of 3 kernprincipes van de informatieveiligheid worden gerespecteerd: confidentialiteit, integriteit en beschikbaarheid. (voetnoot : Confidentialiteit heeft betrekking op de capaciteit om informatie enkel ter kennis te stellen van zij die er gerechtigd zijn toegang tot te nemen. Integriteit heeft te maken met de eigenschap dat de informatie accuraat en onveranderd is ten aanzien van een origineel. Beschikbaarheid ten slotte betekent dat de informatie op ieder moment toegankelijk is voor diegene die er gerechtigd is toegang tot te nemen.)

Want een kandidaat-cloudaanbieder moet kunnen waarborgen dat deze drie kernprincipes integraal en essentieel deel uitmaken van de door hen geleverde diensten.

Cloud services zijn wereldwijd aan een indrukwekkende opmars bezig. Ze bieden significante voordelen voor de optimalisatie van de beschikbare IT resources en zowel particulieren, bedrijven als overheden opteren er voor om hun gegevens toe te vertrouwen aan gespecialiseerde dienstverleners. De gevaren die hieraan verbonden zijn, zijn niet alleen technisch of economisch van aard maar evenzeer juridisch-politiek. De recente Snowden-onthullingen hebben immers duidelijk aangetoond dat de Amerikaanse overheid haar bevoegdheden tot kennisname in de praktijk ook succesvol weet aan te wenden. Dit betekent voor een Vlaamse overheidsdienst dat zij moet nagaan:

- welke cloudaanbieders met een bevel tot overlegging geconfronteerd kunnen worden,
- op welke gronden en onder welke voorwaarden dit gebeurt, en
- hoe men de gevolgen van een dergelijke overlegging kan vermijden dan wel beperken in het licht van de verplichtingen uit het nationale recht.

De bevoegdheid van kennisname door buitenlandse mogendheden

De bevoegdheden tot kennisname door buitenlandse mogendheden ten aanzien van informatie die beschikbaar wordt gesteld via het internet heeft in de meeste gevallen een wettelijke grondslag in de interne juridische orde van de desbetreffende Staat. Dat is een gevolg van het soevereiniteitsbeginsel. Maar de daadwerkelijke uitoefening van deze bevoegdheden kunnen een schending impliceren van de soevereiniteit van een andere Staat, wanneer er overheidsgegevens of gegevens betreffende de burgers van deze laatste Staat worden afgevangen.

Time.lex onderzocht de centrale juridische bekommernissen uit het Belgische en Vlaamse recht die in conflict kunnen komen met deze buitenlandse bevoegdheden, in het bijzonder de Amerikaanse onderzoeksbevoegdheden, omdat nu eenmaal de meeste cloudaanbieders Amerikaans zijn. De gemaakte aanbevelingen moeten de overheidsdiensten in staat stellen om weloverwogen voor een cloudoplossing voor kritische en minder kritische overheidsgegevens te kiezen of niet.

DE EXTRATERRITORIALE BEVOEGDHEDEN VAN DE VSA MBT KENNISNAME VAN GEGEVENS IN DE CLOUD

De in het interne Amerikaanse recht opgenomen bevoegdheid die toelaat dat de Amerikaanse overheid gegevens van buitenlandse oorsprong capteert en er kennis van neemt is bedreigender dan de mogelijkheden uit de bi- en multilaterale verdragen voor wederzijdse rechtshulp, waarbij soevereine Staten aan elkaar toezeggen onder bepaalde voorwaarden kennis en informatie te zullen overdragen ter bestrijding van misdrijven en ter preventie van terrorisme. Immers, bij dergelijke verdragen behoudt de geviseerde staat zelf ook enige inspraak over de uitoefening van een opeising van data.

In de 3 instrumenten die de belangrijkste bevoegdheden bevatten in de Verenigde Staten (Executive Order 12333, Foreign Intelligence Surveillance Act en Electronic Communications Privacy Act) is de rol van de cloudaanbieder dan wel verschillend, de conclusie is dezelfde, namelijk dat de rechtsbescherming voor buitenlanders in het Amerikaanse recht zo goed als onbestaande is. Bovendien kan men als buitenlander niet rekenen op de grondwettelijke bescherming geboden door de Amerikaanse Grondwet, en ook de bescherming geboden door het statutaire recht is weinig effectief voor buitenlanders.

Time.lex besloot hieruit dat het een illusie is om te denken dat standaard publieke clouddiensten een 'veilige haven' kunnen bieden waar men gegevens kan opslaan zonder dat deze blootstaan aan de mogelijkheid tot kennisname door een vreemde overheid.

Time.Lex wijst er wel op dat, aangezien verschillende landen zichzelf extraterritoriale bevoegdheden hebben toegekend met betrekking tot kennisname van gegevens opgeslagen in de cloud, het geen goed criterium is om een cloudaanbieder af te schrijven louter omwille van het feit dat deze onderworpen is aan het Amerikaanse recht.

VERTROUWELIJKHEIDSVEREISTEN VOOR OVERHEIDSGEGEGEVENS

Tegenover de hierboven aangehaalde bevoegdheden tot kennisname uit het buitenlandse recht staan de vertrouwelijkheidsverplichtingen uit het eigen recht, waarmee ook de Vlaamse overheidsdiensten zich geconfronteerd weten. Het zijn deze plichten die de keuze van een welbepaalde cloudoplossing in belangrijke mate beperken. Voor de persoonsgegevens waarover de overheid het beheer voert, zal zij de verplichtingen van de bescherming van de privacy in de Belgische wetgeving moeten naleven, ook in een cloud-context.

De cloudaanbieder zal de verplichting hebben om de veiligheid van de persoonsgegevens te waarborgen middels contractueel vastgelegde technische en organisatorische beveiligingsmaatregelen. Daardoor moeten de gegevens beschermd worden tegen toevallige of ongeoorloofde vernietiging, toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Gegevens uit het Rijksregister verdienen een bijzondere aandacht, gelet op de centrale positie die hen wordt toebedeeld – zowel op Belgisch als op regionaal niveau - in het kader van het elektronische bestuurlijke gegevensverkeer en dienstenintegratie. Dit impliceert dat standaardovereenkomsten met (publieke) cloudaanbieders niet mogelijk zijn voor gegevens in het Rijksregister, en dat een overeenkomst met een aanbieder met een voldoende systematische band met de VS hiervoor moeilijk lijkt.

Time.lex beveelt dan ook de Vlaamse Overheid aan om deze kritische gegevens bij te houden in een cloud volledig in eigen beheer, op servers gelegen in België, zonder betrokkenheid van aanbieders die onderworpen zijn aan bevelen van een vreemde overheid tot overlegging van deze gegevens. Vlaanderen zou daarmee overigens geen unieke positie innemen: ook in Duitsland kondigde de overheid inmiddels aan om te evolueren naar een nationaal cloudsysteem waarbij gegevens steeds in Duitsland zouden blijven, en buiten bereik van andere overheden.

VERSLEUTELEN VAN GEGEVENS

Time.lex adviseert in conclusie bovendien dat het voor de meeste gevoelige gegevens ten zeerste aan te raden is om deze maar aan de cloudaanbieder toe te vertrouwen wanneer zij versleuteld zijn op een manier die overeenstemt met de technologische state-of-the-art, en die het noch de cloudaanbieder noch een eventuele buitenlandse overheid mogelijk maakt om van de gegevens kennis te nemen. Met dergelijk adequaat niveau van encryptie zou het mogelijk zijn om in heel wat gevallen te voldoen aan de wettelijk opgelegde en contractueel uitgewerkte vertrouwelijkheidsverplichtingen.

Zie ook : time.lex