TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Cloud computing

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Cloud Computing’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het cloud computing beleid door organisaties binnen de Rijksoverheid. Deze beleidsuitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR. Deze beleidsuitgangspunten zijn opgenomen in hoofdstuk 4 ‘Cloud computing beleid’.

Doelgroep

Dit document is van belang voor de directie en de bestuurlijk eindverantwoordelijke (voor het beleid), Hoofden I&A (management verantwoordelijk voor IV-voorzieningen), het Systeembeheer en voor de gebruikers.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 10.2 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsmaatregelen die overheidsorganisaties dienen te nemen in relatie tot cloud computing.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Contracten, waaronder SLA’s of bewerkersovereenkomsten

Inhoudsopgave

1 Inleiding 5

1.1 Doelstelling handreiking 5

2 Cloud computing 6

2.1 Karakteristieken van cloud computing 6

2.2 Soorten cloud computing (deployment model) 7

2.3 Servicemodellen cloud computing 8

2.4 Voordelen van cloud computing 9

2.5 Nadelen en risico's van cloud computing 9

3 Cloud aandachtspunten 11

3.1 Gegevens in het buitenland 11

3.1.1 De VS 11

3.2 Cloud en Privacy 12

3.3 Bijzondere persoonsgegevens 13

3.4 Informatiebeveiliging en de cloud 13

3.5 Contracten en de cloud 14

3.6 Cloud en beheer van informatiesystemen 14

3.7 Risico's bij cloud computing 15

4 Cloud computing beleid 17

1 Inleiding

Cloud computing wordt door organisaties binnen de Rijksoverheid gebruikt om via het internet, of een andere breedbandige verbinding gebruik te maken van hardware, software en gegevens. Deze cloud kan zich overal bevinden. Cloud computing is relevant voor de BIR omdat het afnemen van clouddiensten gevolgen heeft voor de plaats waar informatiebeveiligingsmaatregelen worden uitgevoerd. Hierbij is het van belang dat als een overheidsorganisatie van clouddiensten gebruik maakt, de organisatie altijd verantwoordelijk blijft voor de juiste beveiliging van haar gegevens en ook de privacy waarborgt.

Cloud computing is volgens de NIST1 een model om op afroep op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare computer resources (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers. Het woord ‘cloud’ komt van het woord ‘wolk’ waarmee in een netwerkontwerp vaak het internet of een netwerk wordt getekend. Deze wolk staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt. De eindgebruiker weet meestal niet waar de computers zich in de cloud bevinden en ook niet waar de software draait of waar gegevens zich bevinden.

Doordat veelal niet duidelijk is waar de clouddiensten zich fysiek bevinden of binnen welke ondernemingsstructuur de dienst wordt aangeboden, kan dit onzekerheid opleveren ten aanzien van het geldende recht betreffende de diensten en de data. Afhankelijk van het type cloud kan de afnemer meer of minder eigenaar zijn van de gebruikte infrastructuur.

1.1 Doelstelling handreiking

De hier voorgestelde cloud computing handleiding beschrijft een good practice voor cloud computing. De leidraad biedt algemene handvatten en handvatten ten aanzien van informatiebeveiliging om rekening mee te houden als over cloud computing wordt nagedacht of wanneer implementatie wordt overwogen.

[1] National Institute of Standards and Technology (NIST) (USA).

2 Cloud computing

Bij cloud computing worden hardware, software en gegevens beschikbaar gesteld via het internet. De eindgebruiker weet vaak niet meer op welke computers en waar zich de diensten (fysiek) bevinden die hij of zij afneemt. De eindgebruiker is geen eigenaar meer van de hard- en of software, maar afnemer van een dienst. Er zou gesteld kunnen worden dat het gaat om virtuele infrastructuur en diensten. Voor de eindgebruiker lijkt het alsof met cloud computing servers, desktops en ook applicaties worden gevirtualiseerd. Dit heeft zowel voordelen als nadelen. Voor het concept van cloud computing en de risico's met betrekking tot informatiebeveiliging is niet relevant welke licentiemodel (bv. pay-per-use, userlicentie, open source) wordt gebruikt. Ook veelgebruikte gratis diensten als Dropbox, Googledrive en Datumprikker moeten gezien worden als clouddiensten.

In deze handreiking wordt ingegaan op specifieke aandachtspunten voor overheidsorganisaties met betrekking tot cloud computing. Onder meer het Nationaal Cyber Security Center (NCSC) heeft documenten gemaakt over cloud computing. Daarnaast heeft het Instituut voor Informatierecht van de Universiteit van Amsterdam in 2012 een onderzoek gepubliceerd over clouddiensten in het hoger onderwijs en de USA Patriot Act. Tilburg University heeft in opdracht van SURFnet uitgebreid onderzoek gedaan naar de privacy aspecten bij het gebruik van cloud services in het onderwijs. Hoewel toegespitst op het onderwijs, staan veel algemene privacyaspecten in uitgelegd.

Dit document is geen juridisch sluitend stuk. In dit document wordt algemeen ingegaan op wetgeving. Het is raadzaam om bij twijfel over de omgang met cloud computing en/of de verwerking van (persoons)gegevens in het buitenland een jurist te raadplegen. Alvorens gebruik te maken van diensten op basis van cloudcomputing dient door de directie een afgewogen keuze gemaakt te worden.

Bij het afnemen van clouddiensten door overheidsorganisaties wordt geen verantwoordelijkheid overgedragen. Een organisatie is en blijft verantwoordelijk voor de manier waarop een cloud leverancier omgaat met informatiebeveiliging. In het geval van persoonsgegevens is dit geregeld in artikel 14 Wbp.

2.1 Karakteristieken van cloud computing

De volgende karakteristieken zijn kenmerkend voor cloud computing:

- *Zelfbediening (On-demand self-service)*

De afnemer van clouddiensten kan - vaak binnen bepaalde grenzen - servertijd en opslag zonder tussenkomst van de aanbieder wijzigen als dat nodig is.

- *Breedbandige toegang*

Er is toegang mogelijk via breedbandverbindingen met verschillende soorten cliënt platformen (fat cliënt, thin cliënt, mobiele apparatuur etc.).

- *Gedeelde middelen (resource pooling)*

De fysieke en logische middelen van de cloudaanbieder worden door alle afnemers gebruikt en als nodig dynamisch toegewezen. De afnemers gebruiken dezelfde applicaties waarbij data wel per afnemer gescheiden wordt opgeslagen (Multi Tenancy Model). De afnemer heeft geen weet van de locatie waar de middelen zich bevinden. Voorbeelden van middelen zijn: opslag, rekenkracht, geheugen en netwerk bandbreedte.

- *Elasticiteit*

Middelen kunnen op korte termijn (automatisch) worden toegewezen en vrijgegeven op basis van vraag. De middelen lijken op elk moment onbeperkt voor de afnemer.

- *Meetbare service*

De cloudsystemen controleren en optimaliseren middelen door middel van toepasselijke metingen (opslag, geheugen, rekenkracht etc). Het gebruik van middelen wordt transparant gemonitord, gecontroleerd en gerapporteerd aan de afnemer en de aanbieder van de gebruikte dienst.

2.2 Soorten cloud computing (deployment model)

Cloud computing kan op verschillende manieren worden toegepast. Er zijn drie verschillende vormen: een externe of publieke cloud, waarbij diensten en gegevens bij een externe partij zijn opgeslagen, een private cloud binnen bijvoorbeeld een rekencentrum van een overheidsorganisatie, en er is een hybride vorm.

- Bij een **publieke of externe cloud** staan de hardware, software en de gegevens volledig bij de externe dienstverlener en er wordt een generieke (voor alle afnemers gelijke) dienst geleverd.
- Bij een **private cloud** werkt men op een private ICT-infrastructuur waarop servers/desktops en applicaties worden gevirtualiseerd. In deze cloud heeft een organisatie de volledige controle over gegevens, beveiliging en kwaliteit van de dienst. Vaak ligt de verantwoordelijkheid voor onderhoud en beheer bij een overheidsorganisatie zelf, maar in de praktijk wordt dit vaak door een leverancier uitgevoerd. De private cloud kan in een datacentrum van een overheidsorganisatie draaien, maar ook bij een leverancier. In dat geval wordt de gevirtualiseerde infrastructuur niet gedeeld met andere klanten.
- Een bijzondere vorm van een private cloud is de **Community cloud**, hierbij wordt cloud Infrastructuur gebruikt door een specifieke groep afnemers die een gemeenschappelijk belang hebben. Denk hierbij aan taak, missie, beveiligingseisen, beleid- en nalevingeisen. Deze cloud kan in eigendom zijn en beheerd worden door een van de deelnemers, een derde partij of een combinatie. Hierbij kan gedacht worden aan een overheidscloud.
- De **hybride cloud** is een combinatie van een publieke en private cloud. Dat wil zeggen dat er clouddiensten worden afgenomen van een derde aanbieder terwijl daarbij ook gebruik wordt gemaakt van een eigen cloud

Als een private cloud niet in een rekencentrum van een overheidsorganisatie staat, maar op een aparte infrastructuur bij een leverancier dan is dat technisch gezien een dienst die in een externe cloud wordt afgenomen op specifieke gevirtualiseerde omgevingen. In dat geval zijn de eisen in dit document onverkort van toepassing.

2.3 Servicemodellen cloud computing

De volgende manieren van het aanbieden van cloud computing worden onderkend:

- SaaS – Software as a Service
- PaaS – Platform as a Service
- IaaS – Infrastructure as a Service

Deze drie vormen staan bewust in deze volgorde: van onder af aan wordt begonnen met de infrastructuur waarop platforms draaien die het mogelijk maken applicaties te draaien.

Cloud-applicaties: Software as a Service (SaaS)

Bij Software as a Service worden applicaties via de cloud aangeboden aan eindgebruikers. Er zijn verschillende organisaties die applicaties nu al via een SaaS-model afnemen en dat gebeurt in publieke en private clouds. Vaak worden hier webapplicaties aangeboden die met moderne technologieën zoals Ajax en HTML5 gemaakt zijn. Voor de eindgebruiker is het volledig onduidelijk waar de applicatie zich bevindt, op welk platform de applicatie draait en waar de gegevens zich bevinden.

Cloud-platforms: Platform as a Service (PaaS)

Als een organisatie zelf software wil installeren in een cloud, dan kan gebruik worden gemaakt van PaaS. Bij PaaS kunnen binnen grenzen de software en de configuratie zelf worden geregeld. De eindklant van een PaaS-oplossing is vaak de eigen ICT-organisatie. Op de PaaS-omgeving worden vaak uiteindelijk weer de eigen applicaties geplaatst voor de eindgebruiker.

Cloud-infrastructuur: Infrastructure as a Service (IaaS)

Indien nog meer vrijheden gewenst zijn, kan alleen de (gevirtualiseerde) infrastructuur worden afgenomen. Hieronder worden servers, netwerkcomponenten, opslagcapaciteit en andere infrastructuur begrepen. Dit kan de ICT-organisatie van een organisatie volledige vrijheid geven over de hardware die virtueel wordt afgenomen. Bovenop de IaaS hardware kan de ICT-organisatie weer platformservices draaien en daar bovenop weer eigen software. Beheer kan op afstand worden gedaan.

Schematisch wordt dit als volgt weergegeven:

Servicemodellen	Eigen rekencentrum	Infrastructuur als een service	Platform als een service	Software als een service
	Applicatie	Applicatie	Applicatie	Applicatie

Lagen	Applicatie platform	Applicatie platform	Applicatie platform	Applicatie platform
	Fysieke infrastructuur	Fysieke infrastructuur	Fysieke infrastructuur	Fysieke infrastructuur

Blauw = zelf doen, wit = laten doen

2.4 Voordelen van cloud computing

- De clouddiensten zijn via internet te benaderen. Het ondersteunt in dat geval ook flexibel (plaats en tijd onafhankelijk) werken.
- Clouddiensten kunnen flexibel omgaan met wijzigende vragen. Er kan eenvoudig worden geschaald al naar gelang de behoefte, en dat in korte tijdsspannen.
- Er zijn flexibele verrekenmechanismes: betalen per gebruiker, betalen per virtuele machine of dienst.
- Er wordt uitgegaan van een hogere beschikbaarheid - hoewel dit afhankelijk is van het serviceniveau van de aanbieder.
- De aanbieder heeft vaak de beschikking over voldoende gespecialiseerd personeel. Bij een organisatie zelf zijn minder gespecialiseerde beheerders nodig. Met het gebruik van cloud worden dus niet alleen gegevens op afstand gezet, maar ook de complexiteit van de systemen.

2.5 Nadelen en risico's van cloud computing

- Bij publieke of externe clouds is voor een gebruiker niet inzichtelijk op welke systemen en in welke landen gegevens zich bevinden. Dit kan ook op plaatsen zijn waar gegevens niet mogen staan volgens onze wetgeving of waar andere wetgeving geldt dan in Nederland of Europa.
- Voor de toepasselijkheid van wetgeving maakt het vaak niet uit *waar* data fysiek staat. Als een Amerikaans bedrijf een dochteronderneming met datacenters in Ierland heeft, dan is het Amerikaans recht op die gegevens in Ierland van toepassing. In zoverre dat die gegevens onder de reikwijdte van een Amerikaans datavorderingsbevel kunnen vallen. Ook in het geval dat een Amerikaans bedrijf dochterondernemingen heeft met datacenters over de hele wereld, dan heeft dat Amerikaanse moederbedrijf in principe toegang tot die data, en valt daarmee die data onder de reikwijdte van Amerikaanse wetgeving. Een ander perspectief: als een organisatie gebruik maakt van een clouddienst uit de Verenigde Staten (VS), dan is die Nederlandse overheidsorganisatie wettelijk gezien ervoor verantwoordelijk dat de gegevens in de VS behandeld worden volgens de Nederlandse privacywetgeving.
- Clouddiensten zijn niet altijd storingsvrij. Bij het gebruik van een externe cloud bestaat voor de continuïteit de afhankelijkheid van een derde partij. Hoe meer diensten en gegevens in de cloud staan, hoe problematischer storingen kunnen zijn.
- Aangezien clouds via internet kunnen worden benaderd, zijn ze daarmee inherent ook lastiger te beveiligen.

- Als bekend is waar de clouddienst draait, is het ook zaak om na te gaan via welke weg deze clouddiensten benaderd worden. Het kan goed zijn dat de clouddienst zich in Nederland bevindt, maar dat de netwerkleverancier een niet-Europees bedrijf is.
- Bij het aangaan van een cloudservice is het zaak goed af te spreken wat de gevraagde en afgesproken dienstverlening is. Het is belangrijk dat beide partijen dezelfde beelden hebben over de afgesproken dienstverlening.
- Met name bij externe clouds is niet te controleren of, en in hoeverre, de leverancier diensten en gegevens kan inzien.
- Als gegevens in de cloud staan, blijkt het veelal lastig deze er weer uit te halen of te migreren naar een andere cloudprovider. Houd derhalve rekening met een lock-in probleem en het formuleren van een passende exitstrategie.

2.6 Links

Een overzicht betreffende cloud computing is te vinden bij het NCSC:

https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloud computing.html

Het onderzoek van de afdeling Instituut voor informatierecht van de UvA naar het gebruik van clouddiensten in het hoger onderwijs en de USA Patriot Act:

http://www.ivir.nl/publicaties/vanhoboken/clouddiensten_in_HO_en_USA_Patriot_Act.pdf

Het onderzoek van het Tilburg Institute for Law, Technology and Society (Tilburg University) naar privacy aspecten bij cloud services:
http://www.surfsites.nl/cloud/download/De_wolk_in_het_onderwijs_feb2011.pdf

Kamerbrief over cloud computing:

http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing.html

Cloud computing op de KING website:

http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/cloud-computing

Een document van het Waterschapshuis naar cloud computing voor waterschappen:

http://www.forumstandaardisatie.nl/fileadmin/os/documenten/20131028_Rapport_Cloud_computing_voor_de_waterschappen.pdf

Een document van CIP met het beleid voor een veilig gebruik van clouddiensten:

http://www.cip-overheid.nl/wp-content/uploads/2014/04/Beveiligingsbeleid-clouddiensten-CIP-DEF-v2_3-excl-ARD.pdf

3 Cloud aandachtspunten

3.1 Gegevens in het buitenland

In de Wet Bescherming Persoonsgegevens (Wbp) hoofdstuk 11, artikelen 76-78 staan regels omtrent gegevensverkeer met landen *buiten* de Europese Unie (EU). Binnen de EU zijn data-uitwisselingen zonder meer toegestaan, omdat de Europese privacywetgeving daar van kracht is. Het verzenden en opslaan van persoonsgegevens in landen buiten de EU is toegestaan in de volgende gevallen:

- Er wordt door de niet-EU staat een passend niveau van gegevensbescherming geboden. Welke landen dit zijn, wordt bepaald door de Europese Commissie. Momenteel zijn dit: Noorwegen, IJsland, bepaalde Kanaaleilanden, Argentinië, Canada, Zwitserland en de VS (Safe Harbor);
- Er is geen passend beschermingsniveau, maar er wordt voldaan aan een uitzondering in de Wbp. Hieronder zijn begrepen de situaties waarbij degene op wie de gegevens betrekking hebben hiertoe ondubbelzinnige toestemming heeft verleend, de minister hiertoe een vergunning heeft verleend en de verwerking noodzakelijk is in het kader van de uitvoering van een contract. Zie verder art. 77 Wbp.

3.1.1 De VS

Op basis van de Safe Harbor VS-EU regeling mogen in beginsel persoonsgegevens naar Amerika worden verzonden en daar worden verwerkt, mits de organisatie die de gegevens verstrekt controleert dat de cloudleverancier zich daadwerkelijk houdt aan de beginselen van het gegevensbeschermingsrecht. Dat kan bijvoorbeeld door een verklaring van een auditor te vragen. Safe Harbor bevat principes die gebaseerd zijn op de Europese privacywetgeving. Amerikaanse organisaties kunnen bijvoorbeeld door middel van het TRUSTe[2] keurmerk aangeven dat ze aan die principes voldoen. Persoonsgegevens mogen dan ook alleen worden uitgewisseld met organisaties die dat keurmerk hebben. Er is echter al geruime tijd discussie over deze regeling. Het TRUSTe keurmerk wordt namelijk verkregen op basis van zelfcertificatie en een externe controle op naleving van de Safe Harbor principes door die organisaties ontbreekt, terwijl de verantwoordelijkheid op controle bij de organisatie die de gegevens verstrekt ligt. Er bestaan daarom grote maatschappelijke twijfels over de mate waarin de Safe Harbor regeling waarborgt dat Europese privacystandaarden door Amerikaanse organisaties worden nageleefd. Safe Harbor heeft geen betrekking op de toegang tot gegevens op basis van andere wetgeving.

[2] TRUSTe is a company based in San Francisco, California, with an offshore facility Cebu City, Philippines, best known for its online privacy seals. TRUSTe operates a privacy seal program, certifying websites, mobile apps, and cloud services for more than 5,000 businesses, including Apple, eBay, HP, Intuit, LinkedIn, Microsoft and Zynga.

Daarnaast is er maatschappelijke discussie over de reikwijdte van buitenlandse, en vooral Amerikaanse securitywetgeving zoals de Amerikaanse Patriot Act, die ondermeer de FISA (Foreign Intelligence Surveillance Act) heeft geamendeerd. Op basis van die wetgeving kan data die bij Amerikaanse bedrijven en hun (buitenlandse) dochterondernemingen is opgeslagen door de Amerikaanse overheid worden ingezien, ten behoeve van intelligence verzameling/spionage, strafrechtelijk onderzoek en nationale veiligheid. Voor toepassing van die wetgeving hoeven de gegevens niet fysiek in Amerika te staan. Als er een Amerikaans bedrijf of bedrijf met Amerikaanse banden betrokken is, moet ervan uitgegaan worden dat de Patriot Act van toepassing is.

De discussie over de extraterritoriale reikwijdte van de Amerikaanse securitywetgeving bracht veel onrust met zich mee. In respons op die onrust werd door een aantal grote Amerikaanse cloudproviders aangegeven dat zij konden garanderen dat Europese gegevens op Europese datacenters zou blijven staan, en dat die data daarmee veilig zouden zijn van de Amerikaanse overheid. Zoals hierboven is beschreven, lijkt de Patriot Act onverkort van toepassing.

In het algemeen en betreffende Amerikaanse securitywetgeving is het aan te bevelen bij het gebruik van cloudtechnologie te onderzoeken aan welk recht een bepaalde cloudprovider moet voldoen.

Lees hiervoor ook het volgende document van het CBP:
http://www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-cloud-computing.pdf

3.2 Cloud en privacy

De Wet Bescherming Persoonsgegevens stelt eisen aan het verwerken van persoonsgegevens en aan de verantwoordelijke en de bewerkers van die gegevens, en de relatie tussen beiden (zie art. 14 Wbp). Een leverancier van clouddiensten kan als bewerker worden gezien, waarmee de verantwoordelijke, in dit geval een overheidsorganisatie, een aantal zaken moet organiseren. Deze vereisten staan opgesomd in art. 14 Wbp. Dit zijn wettelijke vereisten waaraan men moet voldoen. Daarnaast wordt door het NCSC de verantwoordelijkheden en verdeling van beveiligingsmaatregelen van alle partijen goed weergegeven. In ieder geval moeten bij het afnemen van clouddiensten, waarbij persoonsgegevens worden bewerkt een aantal maatregelen worden genomen:

1. Passende maatregelen nemen. De Baseline Informatiebeveiliging Rijksdienst (BIR) is voor overheidsorganisaties een goed startpunt. Bij twijfel over het beveiligingsniveau van de baseline moet door de verantwoordelijke (de overheidsorganisatie) altijd een risicoanalyse worden uitgevoerd op het gebruik van de clouddienst.
2. Toezien op naleving van de maatregelen. Als verantwoordelijke is de organisatie verplicht om Opzet, Bestaan en Werking van maatregelen te (laten) toetsen.
3. Alle beveiligingsafspraken dienen te worden vastgelegd in een bewerkersovereenkomst of een contract.

Het uitgangspunt is dat de directie te allen tijde een bewust keuze moet maken of persoonsgegevens in de cloud kunnen worden verwerkt. De verantwoordelijke, een overheidsorganisatie, is eindverantwoordelijk voor de naleving van de Wbp.

3.3 Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens, zoals beschreven in artikel 16 van de Wbp, dient te worden vermeden in de cloud. Deze mogen slechts in zeer beperkt gevallen worden verwerkt. Onder bijzondere persoonsgegevens zijn onder meer begrepen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven.

Bij het verwerken van medische gegevens van een inwoner van een Nederland kan beter geen gebruik gemaakt worden van een cloudoplossing als de bewerker (leverancier van clouddiensten) toegang kan hebben tot deze gegevens. Ook hier geldt dat de Wbp moet worden nageleefd en dat er altijd een risicoanalyse nodig is om het juiste beveiligingsniveau vast te stellen en te controleren op naleving. Het gaat er om dat de vastgestelde eisen bij de leverancier geborgd worden. De directie dient een bewuste keuze te maken omtrent het verwerken van bijzondere gegevens in de cloud en bij voorkeur wordt vooraf juridisch advies gevraagd.[3]

3.4 Informatiebeveiliging en de cloud

Voor het handhaven van vertrouwelijkheid, integriteit en beschikbaarheid van de informatiesystemen en/of gegevens van organisaties in de cloud zijn beveiligingsmaatregelen nodig. Deze maatregelen moeten zowel door de organisatie als de cloudleverancier worden uitgevoerd. Voor de verdeling van verantwoordelijkheden voor de uitvoering van maatregelen tussen beide partijen kan het eerder genoemde document van het NCSC goed worden gebruikt. Een verdeling van de verantwoordelijkheden voor de uitvoering van specifieke maatregelen kan als volgt worden gemaakt:

- Gebruiksbeheer (wie heeft toegang tot een systeem) is een taak voor de overheidsorganisatie, evenals het maken van toegangsbeleid. Het maken van een auditlog over toegang is weer een leverancierstaak.
- Het maken van back-ups van een cloudsysteem is een leverancierstaak, bij IaaS is dit weer een taak van de organisatie.
- Zorg voor gegevensencryptie zowel in de cloudomgeving alsmede gedurende transport van gegevens als afschermende maatregel.
- Alle overige afhankelijkheden en gerelateerde afhankelijkheden meenemen voor beschikbaarheid van een dienst (dienst kan beschikbaar zijn, maar netwerk/internet kan problemen leveren).

Op basis van de BIR-maatregelen en eventuele maatregelen uit een aanvullende risicoanalyse dient een vergelijkbare verdeling te worden gemaakt, waarbij de verantwoordelijkheid voor het uitvoeren van maatregelen en de controle erop wordt vastgelegd.

[3] Zie hiervoor ook: http://www.cbpweb.nl/downloads_inf/inf_va_geheimhouding_medische_gegevens.pdf

3.5 Contracten en de cloud

In contracten met een cloudleverancier dient aandacht te zijn voor de volgende zaken:

- Specifieke beveiligingsmaatregelen afkomstig uit een risicoanalyse of de BIR;
- Het verplicht melden van beveiligingsincidenten;
- Looptijd van het contract;
- Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven;
- Een ESCROW regeling (of cloud ECROW regeling)[4];
- Software licenties (van wie zijn deze en mogen deze in een cloud worden gebruikt);
- Conversie van gegevens;
- Overdacht van gegevens van- en naar de cloudomgeving;
- Eigenaarschap van gegevens;
- Vernietiging van gegevens bij contract beëindiging;
- Continuïteit van het systeem;
- Overdracht naar een andere leverancier;
- Back-up en uitwijk voorzieningen;
- Locatie gegevens en programmatuur;
- Additionele regels bij persoonsgegevens (bewerkersovereenkomst);
- Geheimhoudingsovereenkomst;
- Encryptie, versleutelen van gegevens;
- Onderaanneming en overdracht van rechten en plichten (of geen onderaanneming toestaan);
- Opschortingsrecht;
- Naleving wet- en regelgeving;
- Logging gegevens kunnen opvragen en inzien;
- Het recht om controles/audits te mogen (laten) uitvoeren over alle afspraken;
- Welk recht van toepassing is;
- Exit regels: wat als je de cloud-provider wilt verlaten, of de gegevens/diensten wilt migreren naar een andere provider? Hier wordt in de praktijk weinig over nagedacht;
- Beheerafspraken (zie onder).

3.6 Cloud en beheer van informatiesystemen

Beheerafspraken dienen in een Service Level Agreement (SLA) te worden vastgelegd dat onderdeel uitmaakt van het contract. Veel cloud leveranciers hanteren een standaard SLA omdat hun clouddienst generiek is opgezet voor meerdere afnemers en het eenvoudiger (en goedkoper) is om hun eigen dienstverlening zo generiek mogelijk in te richten. Laat in dat geval de standaard leveranciers-SLA beoordelen door een aantal mensen binnen de organisatie, zoals een ICT-beheerder, de directie en/of een informatiemanager. Neem geen genoegen met een standaard SLA als dit niet overeenkomt met de eigen behoefte. Bij een

[4] Bij een ESCROW worden afspraken gemaakt om broncode of programmatuur bij een escrow agent te stallen, zodat in het geval van een faillissement van de leverancier de eindgebruiker de beschikking krijgt over de broncode of software. Zie : http://nl.wikipedia.org/wiki/Broncode_escrow

aanbesteding dient hier in het programma van eisen aandacht voor te zijn. Aan additionele eisen naast de standaard SLA zullen in veel gevallen meer kosten verbonden zijn.

Alle beheerafspraken dienen in de SLA te staan. Er moet een duidelijke hiërarchie zijn tussen het contract, een SLA en de bewerkersovereenkomst, zodat duidelijk is welke eisen waar staan en wat de verhouding is tussen de documenten. Accepteer niet dat voor afspraken of eisen wordt verwezen naar een website. Websites zijn veranderlijk.

3.7 Risico's bij cloud computing

In dit document zijn een aantal risico's beschreven die verbonden zijn aan cloud computing. Deze risico's zijn onder andere:

Verlies van besturing (governance)

De afnemer legt een deel van de besturing in handen van de leverancier, dit betreft ook informatiebeveiliging.

Leverancier lock-in

Leveranciers hebben nog weinig te bieden aan tools, procedures of services om te kunnen migreren naar een andere cloudleverancier. Daarmee ontstaat het risico dat een organisatie voor langere tijd ongewenst vastzit aan die leverancier en dat het kostbaar wordt om clouddiensten te verhuizen.

Omgeving afschermingsfouten bij gedeelde omgevingen (isolation failure)

Bij cloud computing maken in veel gevallen meerdere afnemers gebruik van deze software, waarbij alleen de data gescheiden wordt. Dit brengt het risico met zich mee dat de mechanismes falen die zorgen voor het scheiden van opslag, geheugen en routering tussen de verschillende afnemers.

Compliance risico's

Het is lastig om als afnemer zelf een controle of audit uit te (laten) voeren over een dienst die heel ergens anders wordt gehost of geleverd. Afgezien daarvan moet ook vertrouwd kunnen worden op auditrapporten of -certificeringen die op verzoek kunnen worden aangeleverd. Ook naleving van specifieke wetgeving door de leverancier is niet altijd goed na te gaan vanuit de positie van de afnemer.

Gegevensbeveiliging

Het beheer van de cloud door de cloudaanbieder voegt een risico toe dat beheerders van de leverancier de data kunnen van alle cloudafnemers. Adequate encryptie kan dit risico mitigeren.

Verplichtingen en verwachtingen wat betreft de gegevensbeveiliging

Het is zaak de verplichtingen waar partijen aan gehouden zijn goed te verwoorden in de overeenkomsten. Let wel: doorgaans geldt de regel dat hoe strakker de verplichtingen worden beschreven, hoe minder flexibel en minder meedenkend de dienstverlener is.

Het is ook zaak de wederzijdse verwachtingen duidelijk te maken. De verwachtingen wat betreft de beveiliging van de clouddienst bij de afnemer kan verschillen met die bij de cloudaanbieder. Zo kan het zijn dat de aanbieder in het kader van kostenreductie - door de afnemer ongewenste - keuzes maakt die het niveau van de beveiliging doet afnemen.

Onveilige of onvolledige verwijdering van gegevens

Als een gegeven in de cloud verwijderd moet worden, hoeft dat niet te resulteren in daadwerkelijke en volledige verwijdering. Er kan bijvoorbeeld data op andere plaatsen worden vergeten, zoals een back-up. Bovendien is het fysiek verwijderen van data door bijvoorbeeld het vernietigen van het opslag medium vaak niet te doen omdat andere afnemers van clouddiensten ook gebruik maken van een bepaalde disk. Daarnaast heeft een afnemer weinig controle over hergebruik van apparatuur of herinzet van cloud resources voor andere cloud afnemers.

Uitbreiding perimeter

Met het afnemen van clouddiensten wordt ook het eigen domein vergroot waar een verantwoordelijkheid voor is. Dus waar eerder alleen gekeken hoefde te worden naar het eigen fysieke pand of de panden wordt de beveiligingsfocus nu verlegd naar een grotere en daarmee moeilijker te controleren omgeving.

Beschikbaarheid en continuïteit

Met het gebruiken van clouddiensten wordt de afhankelijkheid van internetconnectiviteit (of een andere breedbandige verbinding) van de afnemer groter.

4 Cloud computing beleid

1. De directie is en blijft eindverantwoordelijk voor de gegevens en diensten die zij in de cloud opslaat en gebruikt, en dient een afgewogen keuze te maken of een informatiesysteem in de cloud gebruikt mag en kan worden.
2. Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.
3. De overheidsorganisatie blijft verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van uitbestede diensten.
4. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald, zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen. Bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen.
5. Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
6. Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
7. Er zijn continuïteitsplannen voor het herstel van incidenten, zoals aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.
8. Bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe BIR hoofdstuk 12.3.1.3.
9. Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
10. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
11. De in de bewerkersovereenkomst of dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld door audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).[5]
12. Er zijn voor beide partijen eenduidige aanspreekpunten.
13. In het geval van verwerken van persoonsgegevens is er een bewerkersovereenkomst, waarin helder alle rechten en plichten van de leverancier en de organisatie zijn vastgelegd. De vastgelegde beveiligingsmaatregelen worden jaarlijks door de overheidsorganisatie geaudit bij de leverancier (zie ook 11).

[5] Daarnaast kan men met de leverancier afspreken dat met een TPM kan worden voldaan aan de auditeis, echter dan moet deze wel dezelfde dekking hebben als de afspraken met een overheidsorganisatie.

Aldus vastgesteld door de bestuurlijk verantwoordelijke van *[organisatie]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____