Beveiligingsbeleid clouddiensten

Versie 2.3 (excl ADR)

Een CIP-bewerking van:
"*UWV beveiligingsbeleid clouddiensten*" v.0.9
Marcel Koers, Jeroen Kulk, Paul de Koning
UWV 8 januari 2013

Bewerking en redactie: Ruud de Bruijn
Centrum voor Informatiebeveiliging en Privacybescherming

6 augustus 2013 : versie 2.0
20 december 2013 : versie 2.2 (lichte tekstaanpassingen)
4 april 2014 : versie 2.3 (creative commons licentie)

'38% personeel bewaart werkbestanden in Dropbox'
(Security.nl 4 juni 2013)

Inhoud

1 Inleiding

1.1 Doel van dit document

Het doel van dit document is om praktische richtlijnen te geven voor het gebruik van clouddiensten in overheidsgerelateerde organisaties die (grote) persoonsregistraties voeren.[1]

Het document is in lijn met de gangbare algemene baselines, normenkaders en best practices, met name de ISO 2700x normen en de Code voor Informatiebeveiliging, en tevens de BIR-TNK voor zover van toepassing[2]. Deze uitgangspunten zijn - mutatis mutandis - ook op het gebruik van clouddiensten van toepassing, maar cloudcomputing brengt ook een typisch eigen dimensie met zich mee die specifieke aandacht behoeft.

1.2 Herkomst en status

Dit document is een bewerking van: Marcel Koers e.a. *UWV beveiligingsbeleid clouddiensten* v.0.7, UWV 8 januari 2013, op basis van een review door deelnemers uit het veld van CIP.
Het origineel is een UWV-intern beleidsstuk. Deze publicatie heeft die status natuurlijk niet en is dan ook ontdaan van specifieke verwijzingen naar UWV-beleid, tenzij het passages betreft die als voorbeeld of illustratie kunnen dienen.

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd.
De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden.

De CIP-documenten zijn voor iedereen vrij te gebruiken en te becommentariëren. Zij hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als het besloten www.cip-pleio.nl.

Om extra duidelijkheid te scheppen labelt CIP de documenten volgens deze indeling:

1. Individuele praktijk: een toepassing bij een van de organisaties die werkt, als handreiking voor hergebruik binnen geïnteresseerde organisaties.
2. Becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties.
3. Gecommitteerde praktijk: een namens meerdere in CIP samenwerkende organisaties onderschreven praktijk, als sterk advies voor hergebruik bij alle organisaties binnen de uitvoerende overheid.
4. Verplichtende praktijk: een praktijk die door de in CIP samenwerkende organisaties is bekrachtigd als basis voor zelfregulering binnen deze kring en met een sterk advies om dat voor de gehele overheidslaag van de uitvoering toe te passen.

---

[1] Het vertrekpunt voor dit document is een UWV-beleidsstuk. Het zijn dan ook typisch ZBO's en soortgelijke organisaties die hier worden bedoeld.

[2] BIR-TNK is specifiek gericht op de *Rijks*overheid

Een individuele praktijk is al bruikbaar nadat een individuele organisatie die aanreikt. Een becommentarieerde praktijk ondergaat eerst een reviewslag binnen een CIP-domeingroep en/of door de CIP-Leesgroep. Een praktijk is pas gecommitteerd of verplichtend als bestuurders daarvoor hebben gekozen. Dat zijn geen inherente eigenschappen van CIP-documenten.

Op www.cip-overheid.nl kunt u een uitgebreidere versie van dit protocol raadplegen:
"De totstandkoming en status van CIP-publicaties v1_1.doc".

Deze publicatie valt in de categorie 2.

1.3 Uitbreidingen, ontwikkelingen

Aanvankelijk waren door reviewers bij de ADR (Auditdienst Rijk) twee uitgebreide en waardevolle aanvullingen ingezonden. Deze teksten hebben bij de ADR echter nog conceptstatus en zijn, op verzoek van de ADR, tot nader order uit deze versie verwijderd.

Na eerste publicatie van dit document zijn door deelnemers aan de leesronde nog twee suggesties aangeleverd voor verwerking in dit document:

- De "*cloudbrief van Donner*". Een kamerstuk uit 2011[3], met in essentie een zeer voorzichtige houding ten aanzien van (open) cloud en 'cloud first'-beleid. Een 'gesloten Rijkscloud' zou in eerste instantie wel tot de mogelijkheden behoren, onder meer om ervaring op te doen. Hierover is veel discussiemateriaal op internet te vinden. Ik meen dat de relevantie van dit thema voldoende duidelijk naar voren komt in de bespreking van de verschillende cloudtypen (paragrafen 3 en 4.3).
  Overigens heeft onlangs De Nederlandse Bank laten weten - onder voorwaarden - geen bezwaren te hebben tegen banken die hun business willen onderbrengen bij Amazon bijvoorbeeld. Geen overheidsbusiness weliswaar, maar toch wel kritische infrastructuur en gevoelige informatie te noemen?

- Relateren aan *VIR-BI 2013*. De suggestie die is gedaan luidt: "rubricering van gegevens op het recent door de kamer goedgekeurde VIR-BI 2013; wat doe je daarmee in de cloud?"
  Voor de behandeling van vertrouwelijke informatie bij de Rijksoverheid is een aanvullende set van maatregelen van toepassing: Het Voorschrift Informatiebeveiliging – Bijzondere Informatie (VIR-BI). In dit voorschrift worden voor 4 categorieën van informatie extra eisen gesteld. Het betreft de volgende risiconiveaus: Departementaal Vertrouwelijk, Staatsgeheim Confidentieel, Staatsgeheim Geheim, Staatsgeheim Zeer geheim.

Het beoogde niveau van de in paragraaf 1.1 al genoemde BIR is "departementaal vertrouwelijk en WBP risicoklasse II". De vereisten in relatie tot 'cloud' voor drie zwaardere VIR-BI categorieën laten zich denk ik wel raden, zeker tegen de achtergrond van de Donner-brief.

1.4 Een ware wolk aan literatuur

Over 'de cloud' is en wordt ondertussen heel wat geschreven en geconfereerd, maar van een stabiele, breed geaccepteerde en gebruikte 'best practice' is nog geen sprake.
In het publieke domein alleen al is een zeer ruim aanbod aan voorbeeldarchitecturen, cloudnormen, checklists en best practices voorhanden, maar er is nog geen toepassingstraditie ontstaan, zoals bijvoorbeeld het geval is rond de Code voor Informatiebeveiliging. Ook worstelt de auditwereld nog met de vraag of dit betrekkelijk nieuwe toepassingsgebied wel met de traditionele auditmethoden zinvol benaderd kan worden en hoe dat dan precies moet.[4]

---

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

[4] Persoonlijke communicatie, RdB.

Twee documenten verdienen in dit kader bijzondere aanbeveling:

- ENISA 'Cloudcomputing: Benefits, risks and recommendations for information security', november 2009 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment;
- NCSC Whitepaper NCSC 'Cloudcomputing & security', januari 2012 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html

Met name de laatstgenoemde publicatie is een zeer uitgebreid, maar wel toegankelijk overzicht van een veelheid aan aspecten die cloudcomputing aankleven, inclusief bijvoorbeeld een checklist voor de keuze van type cloud en leverancier. Dat geldt ook voor bijlagen over virtualisatie, 'security-patterns', en een referentietabel met de relatie tussen beveiligingsaspecten en (artikelen in) vigerende normenkaders.

2 Reikwijdte van dit document

De inzet van clouds en daarmee van clouddiensten past in de verschuiving die gaande is van maatwerkoplossingen naar standaardoplossingen[5]. Clouddiensten zijn in beginsel eenvoudig te vervangen door andere diensten en zijn, indien zij technisch en organisatorisch goed zijn ingericht, niet per definitie onveilig. Aandachtspunt hierbij is wel dat bij een toename van het aantal diensten en daarmee het aantal dienstenleveranciers de risico's en mogelijk ook de overheadkosten toenemen.

Dit document geeft aanwijzingen voor een verantwoorde inzet van gecontracteerde clouddiensten en kan gebruikt worden om cloudbeleid voor de eigen organisatie te formuleren, dan wel om bestaand beleid binnen de organisatie aan te vullen of aan te scherpen.[6]
Het document gaat concreet in op de inzet van diensten die worden afgenomen in de cloud, in het bijzonder op de beveiligingsaspecten die ingeregeld moeten worden bij het aangaan van een clouddienst. De te nemen beveiligingsmaatregelen zijn afhankelijk van de risicoanalyse en risico-afweging van de diverse beveiligings- en privacyaspecten.

In dit document wordt als weergave van de globale risico-inschatting nog gebruik gemaakt van de traditionele classificatie van de gegevens, afgeleid van G.W. van Blarkom en J.J. Borking "*A&V23: Beveiliging van persoonsgegevens*"(Registratiekamer, 2001).

3 Cloud nader uitgelegd

Er bestaan meerdere definities van een cloud. De definitie van cloud(computing) is volgens het Amerikaanse *National Institute of Standards and Technology* (NIST) als volgt:

"*Cloud Computing is een model om vanaf iedere locatie gemakkelijk en op afroep via een netwerk toegang te verlenen tot computermiddelen (netwerken, servers, storage, applicaties en diensten) die snel kunnen worden aan- en opgeleverd met minimale beheerinspanning of interactie van de leverancier van de dienst*".

3.1 Karakteristieken en voordelen

Cloud is een generieke term voor een omgeving waarin één of meer leveranciers functionaliteit en/of diensten aanbieden in de vorm van een technologische "black box". De afnemer van een clouddienst heeft geen inzicht in wat er binnen de black box precies gebeurt en hoe deze technisch in elkaar zit.

---

[5] En overigens ook de verschuiving van vast naar mobiel.

[6] Inclusief uitbesteding en leveranciersmanagement in deze kaders.

De meest essentiële karakteristieken van clouddiensten zijn:

- *On Demand Self service*: Een afnemer kan zelfstandig diensten aanvragen en geleverd krijgen zonder de tussenkomst van de service provider;
- *Brede toegang via het netwerk*: De dienst is beschikbaar via het netwerk en toegankelijk via standaard mechanismen;
- *Resource Pooling*: De computermiddelen worden vanuit een grote pool toegewezen aan meerdere afnemers;
- *Snelle elasticiteit*: De middelen kunnen snel en elastisch worden op- en afgeschaald. Voor de afnemer lijken de middelen onbeperkt;
- *Dienst op maat:* De middelen worden automatisch gecontroleerd en geoptimaliseerd, gebruik makend van een meetsysteem dat gebruik op enige wijze meet en rapporteert aan zowel de afnemer als de leverancier.

Voordelen zijn onder andere:

- De klant hoeft de voorziening (software en hardware) niet aan te schaffen, maar betaalt slechts voor het gebruik;
- De software en hardware worden niet bij de klant geïnstalleerd, maar bij de leverancier. De klant heeft toegang tot de dienst via een publiek of privaat netwerk;
- De inzet van een clouddienst is relatief laagdrempelig door het gebruik van webstandaarden.

Nadelen en risico's zijn er ook. Zij komen uitgebreid aan de orde in paragraaf 3.4.

3.2 Deploymentmodellen (cloud'typen')

De deployment van een dienst geeft aan hoe een dienst wordt aangeboden. De keuze van een deploymentmodel moet worden meegenomen bij de keuze van een cloudoplossing. We onderscheiden de volgende deploymentmodellen:

- *Private cloud*: is exclusief voor één afnemer ingericht, volgens tussen de leverancier en de afnemer overeengekomen normen;
- *Shared cloud*: ook wel *Community cloud* genoemd, is voor meerdere afnemers ingericht, waarbij de afnemers bepaalde gemeenschappelijke eisen en wensen hebben en deze gezamenlijk aan een leverancier opleggen. De Shared cloud wordt ingericht volgens de grootste gemene deler van de gemeenschappelijke eisen en wensen;
- *Public cloud*: Een verzameling van inrichtingen voor meerdere afnemers die niet noodzakelijkerwijs dezelfde eisen en wensen hebben. In een *Public cloud* bepaalt de leverancier in hoge mate de eisen en wensen die aan de dienst kunnen worden gesteld. Afnemers hebben slechts de keuze deze te accepteren of niet;
- *Hybrid cloud*: dit is een combinatie van twee of meer van de andere modellen die weliswaar gescheiden zijn en daardoor hun eigen karakteristieken behouden, maar wel zijn gekoppeld op enigerlei wijze.

Voorbeeld UWV
Voor UWV is het Hoofd Reken Centrum bij IBM te classificeren als een hosted dienst binnen het UWV private (netwerk)domein, in dit document aangeduid als "UWV Private cloud". De applicaties worden geïnstalleerd op een niet met andere partijen gedeelde infrastructuur en middleware. Hierbij bepaalt UWV in hoge mate de inrichting van de infrastructuur, middleware en de applicatie die op de middleware is geïnstalleerd. Er is echter geen self service en de elasticiteit is beperkt in vergelijking met cloudomgevingen. Voor UWV is de in ontwikkeling zijnde Overheidscloud (Gesloten Rijkscloud) een Shared cloud. Het voordeel van deze cloud is dat diverse (beveiligings-)maatregelen en de benodigde audits daarop éénmalig voor de overheid gedaan kunnen worden.

3.3 Servicemodellen

Bij de clouddiensten worden services aangeboden. Hierbij kan onderscheid gemaakt worden tussen verschillende servicemodellen. De belangrijkste servicemodellen zijn:

- *Software As A Service (SaaS)*: hierbij wordt de complete standaardfunctionaliteit van een applicatie geleverd;
- *Platform As A Service (Paas)*: hierbij wordt functionaliteit op middlewareniveau geleverd waarmee de afnemer een applicatie kan inrichten;
- *Infrastructure As A Service (IaaS)*: hierbij worden slechts de servers, storage en netwerkverbindingen geleverd waarop de afnemer middleware en applicatiesoftware kan installeren.

3.4 Nadelen en risico's

Het gebruik van clouddiensten kent een aantal risico's:

- Het aantal leveranciers neemt toe. Voor elke leverancier moet worden bepaald of de veiligheid en de continuïteit van de dienst en de gegevens zijn gewaarborgd. Hierdoor neemt de overhead voor de organisatie toe.
- Door een keuze voor een clouddienst buiten de Private cloud c.q. het traditionele rekencentrum neemt ook het aantal koppelvlakken met Internet toe, wat de informatiebeveiliging complexer en in potentie kwetsbaarder maakt.
- De dienst wordt as-is geleverd. Afgezien van de in de dienst ingebouwde configuratie-mogelijkheden zijn er geen mogelijkheden om de dienst aan de specifieke eisen en wensen van een gebruiker aan te passen. Dit kan overigens ook als voordeel worden gezien.
- De leverancier van clouddiensten verzorgt het volledige beheer, inclusief het ontwikkelen van nieuwe functionaliteit, het installeren van nieuwe versies en updates en de beveiliging van de diensten. Gebruikersbeheer kan zowel bij de leverancier als bij de klant liggen.
- Het afnemen van clouddiensten bij meerdere leveranciers kan leiden tot een grotere integratielast in beheer van IT-componenten.

Specifieke zorgpunten bij de huidige praktijk van cloud computing kunnen zijn:

- Minder grip op de data, datalekken, herstelprocedures e.d. - je zit minder dicht bij het vuur;

- Onvoldoende specifieke en evenwichtige contracten met cloud providers: er is nog weinig traditie opgebouwd met deze materie en er is nog geen 'voorbeeldencatalogus', zoals het geval is bij de meer conventionele vormen van uitbesteding;

- Ook hier bestaat het gevaar van een 'lock in'. Was dat voorheen een *vendor* lock in, nu is het risico een *technologische* lock-in. Besteed aandacht aan:
  - standaardisering en interoperabiliteit van gegevensformaten,
  - toegankelijkheid en portabiliteit van gegevens,
  - het gebruik van open cloudtechnologie en
  - controle over wijzigingen;

- Onder welke wetsdomein(en) valt de leverancier? Welk recht is geldig ten aanzien van:
  - eigendom van de gegevens die in cloudtoepassingen worden gecreëerd,
  - toegankelijkheid (privacywaarborgen) in relatie tot vigerende wetten,
  - aansprakelijkheid voor calamiteiten en gebrekkige dienstverlening (zoals uitvaltijd of verlies van gegevens),
  - faillissementsvraagstukken en het voorkomen van dataverlies (bijvoorbeeld via een escrow-regeling of een trusted third party),
  - de wijze waarop geschillen worden beslecht.

4 Uitgangspunten en richtlijnen

4.1 Risicoanalyse en gegevensclassificatie

De geschiktheid van een clouddienst voor gegevensverwerking en opslag moet worden getoetst met een grondige risicoanalyse[7]. Afhankelijk van de risicocategorieën waarin de gegevens vallen, kan het gebruik van een clouddienst al of niet acceptabel zijn.

Bij het wegen van de risico's is het van belang onderscheid te maken in de mate van vertrouwelijkheid van de verschillende typen gegevens in de organisatie. Voor dit doel hanteren we de volgende vertrouwelijkheidclassificatie voor bedrijfs- en persoonsgegevens.

RK-0 : Openbaar
RK-I : Voor intern gebruik
RK-II : Vertrouwelijk
RK-III : Geheim of strikt vertrouwelijk[8]

RK-0 vereist een beperkte set aan beschermende maatregelen; RK-III de maximale set.

4.2 Algemene Richtlijnen

Alle (gecontracteerde) clouddiensten en daarmee samenhangende processen moeten voldoen aan de beveiligingsnorm zoals die is gedefinieerd voor de 'traditionele' IT-voorzieningen, waarvan de organisatie gebruik maakt. De richtlijnen in dit document zijn *aanvullende, cloudspecifieke* richtlijnen.

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	Minimale beveiligingseisen				
CD 1	De leverancier toont aan dat hij en zijn dienst ten minste voldoen aan de standaarden ISO2700x i.c. de Code voor Informatiebeveiliging, mutatis mutandis de daarvan afgeleide kaders die de afnemende organisatie hanteert.	•	•	•	•
CD 2	De uiteindelijke keuze wordt gebaseerd op een businesscase waarvan een beveiligingsrisicoanalyse onderdeel uitmaakt.	•	•	•	•
CD 3	De resultaten van de beveiligingsrisicoanalyse zijn verwerkt in het contract (bijvoorbeeld in de vorm van een toegevoegde beveiligingsovereenkomst) en afgeleiden zoals de SLA e.d.	•	•	•	•

4.3 Risicoprofielen van de verschillende deploymentmodellen

Public cloud
De opzet van de *Public cloud* kent een relatief groot '*attack surface*'– dit is het gedeelte van een dienst dat wordt blootgesteld aan aanvallen door kwaadwillenden. Dit is inherent aan het publieke karakter van deze dienst. Omdat bovendien in een Public cloud de leverancier in hoge mate de eisen

[7] Werken op basis van risicoanalyses wordt door het CBP in de plaats gesteld van het hanteren van het risicoclassificatiestel van A&V23. Dat betekent niet dat risicoclassificatie gediskwalificeerd of niet langer nuttig zou zijn (feb 2012: CBP-Richtsnoeren Beveiliging van persoonsgegevens).

[8] Cf. A&V23 of vergelijkbare gevoeligheid. Deze klasse kan ook van toepassing worden verklaard op vertrouwelijke bedrijfsinformatie ('company confidential'). De Rijksoverheid kent een aanvullende set van maatregelen: het *Voorschrift Informatiebeveiliging - Bijzondere Informatie* (VIR-BI). In dit voorschrift worden voor 4 categorieën van informatie extra eisen gesteld: Departementaal Vertrouwelijk, Staatsgeheim Confidentieel, Staatsgeheim Geheim, Staatsgeheim Zeer geheim.

en wensen bepaalt die aan de dienst worden gesteld, is de Public cloud *ongeschikt* voor verwerking van gegevens in de klasse RK-III en voor inzet binnen kritische bedrijfsprocessen.

Shared cloud
De inzetbaarheid van een *Shared cloud* wordt bepaald door het beveiligingsniveau zoals dat door de *community* is gedefinieerd. Afhankelijk van dit beveiligingsniveau is een Shared cloud *mogelijk inzetbaar* voor alle gegevensklassen.

Private cloud
Binnen een *Private cloud* stelt de organisatie zelf de eisen aan het beveiligingsniveau en derhalve is deze *inzetbaar* voor alle gegevensklassen.

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	Keuze voor een deploymentmodel				
CD 4	Bij de keuze van het deploymentmodel is de classificatie van de gegevens en processen bepalend.	•	•	•	•
CD 5	De onderbouwing en de keuze van het deploymentmodel zijn vastgelegd en meegegeven in het proces voor de inzet van de clouddienst.	•	•	•	•

4.4 Integrale werking van de informatievoorziening

Het is van belang dat de integrale werking - inclusief de veranderbaarheid - en de continuïteit van de bedrijfsinformatievoorziening gegarandeerd zijn. Een oplossing buiten de Private cloud vergroot de complexiteit en daarmee de kans dat de integrale werking van de informatievoorziening nadelig wordt beïnvloed. Om de integrale werking te verzekeren worden de volgende richtlijnen gehanteerd:

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	De integrale werking en continuïteit worden gewaarborgd				
CD 6	Clouddiensten voldoen (minimaal aan de grenzen) aan de open overheids- en webstandaarden. [9]	•	•	•	•
CD 7	Communicatie tussen de Private cloud en Public clouds vindt uitsluitend plaats via binnen de DMZ aangeboden webservices. Deze koppelingen moeten gecertificeerd zijn.	•	•	•	•
CD 8	Alleen clouds met vergelijkbaar beveiligingsniveau mogen gekoppeld worden.	•	•	•	•
CD 9	Oplossingen buiten de Private cloud vereisen géén aanpassingen binnen de Private Cloud, werkplekvoorzieningen daarbij inbegrepen.	•	•	•	•
CD 10	Een leverancier levert zijn diensten als één integraal werkende dienst (geaggregeerde dienst), waardoor geen additionele integratielast bij de organisatie ontstaat.	•	•	•	•
CD 11	De leverancier moet, ten behoeve van migratie naar een andere oplossing of mogelijke verwerking door een ander systeem, altijd een gegevensdump kunnen leveren van alle in zijn systeem aanwezige organisatiegegevens.	•	•	•	•

[9] Vooropgesteld natuurlijk dat de organisatie zelf eveneens aan deze standaarden voldoet.

4.5 Eén Identiteit en Access Management systeem

Een centrale Identiteit en Access Management (IDM) omgeving borgt dat acties onweerlegbaar terug te leiden zijn naar natuurlijke personen en dat de controle op toegang en functiescheiding mogelijk zijn. Clouddiensten, die buiten de Private cloud worden aangeboden, moeten gebruik maken van de centrale IDM-omgeving. Dit is mogelijk door middel van (bijvoorbeeld) een veilig gebruik van een LDAP-extensie op de Active Directory of van de protocollen SAML 2.0 en XACML.

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	Clouddiensten in één integraal IDM-systeem				
CD 12	Voor de gebruiker en het beheer van de digitale identiteit en de toegangrechten is het niet merkbaar dat een oplossing binnen of buiten de organisatie wordt aangeboden.	•	•	•	•
CD 13	Bij SaaS-diensten wijkt de digitale identiteit (de *user-id*) niet af van die binnen de *Private cloud*. Het beheer van toegangsrechten, inclusief de bewaking van functie-scheiding, geschiedt vanuit één (logisch) IDM-systeem. Implementatie bij voor-keur in een *Single Sign On* systeem met behulp van - bijvoorbeeld - SAML.	•	•	•	•
CD 14	Alle toegangsrechten worden beheerd vanuit één IDM-systeem.	•	•	•	•

4.6 Exclusiviteit

Wanneer het inzetten van diensten en infrastructuur *uitsluitend ten behoeve van de organisatie* een belangrijk principe is voor de organisatie of de desbetreffende dienst(en), dan impliceert dat op voorhand uitsluiting van het gebruik van Public en Shared clouds.

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	Voor de inzet van clouds geldt de exclusiviteitclausule				
CD 15	Een leverancier levert de dienst(en) binnen het exclusiviteitprincipe			•	•

CD 16	De leverancier toont aan dat:
	• de organisatiegegevens logisch en functioneel zijn gescheiden van de overige afnemers. Een logische en functionele scheiding wordt gegarandeerd;
	• het afgesproken beveiligingsniveau van de dienst en de achterliggende organisatie is gegarandeerd;
	• er geen afhankelijkheid bestaat van andere afnemers in geval van:
	  ○ onderhoud- en releasewerkzaamheden;
	  ○ technische uitwijk;
				•	•

	• de performance niet lijdt onder de piekbelastingen door andere afnemers van de infrastructuur; • de schaalbaarheid en flexibiliteit niet worden beperkt. Voorts mag geen sprake zijn van ontvlechtingproblematiek bij afloop van het contract en wordt volledig inzicht gegeven in wijze waarop de infrastructuur wordt gedeeld. Dit inzicht wordt op verzoek geleverd d.m.v. een Third party Memorandum (TPM).				
CD 17	De dienst dient enkel en alleen benaderbaar te zijn vanaf de UWV infrastructuur.			•	•

4.7 Dataprivacy en data-integriteit internationaal

Bijna alle (semi-)overheidsorganisaties verwerken grote hoeveelheden privacygevoelige gegevens van klanten/burgers. Dit schept de verplichting om de vertrouwelijkheid en de integriteit van de gegevens te garanderen. Een passend beveiligingsniveau is daarbij essentieel.
De in potentie - en in de praktijk vaak daadwerkelijk aanwezige - internationale dimensie van opslag, beheer en verwerking van gegevens in de cloud vereist extra aandacht.

Er bestaat een lijst van de Europese commissie over de "International <data> transfers Adequacy". Afhankelijk van het standpunt van de organisatie ten aanzien van het karakter van de desbetreffende (persoons)gegevens, is de lijst, behalve curieus, waarschijnlijk niet onomstreden als het gaat om gegarandeerde privacy of 'auditability' van de dienst.
Oordeel zelf:

> "*The Commission has so far recognized Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the US Department of Commerce's Safe harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.*"

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	De diensten kennen een passend beveiligingsniveau bij grensoverschrijdende gegevensverwerking				
CD 18	De afnemer van de clouddienst blijft eigenaar van alle informatie die hij binnen de cloud verwerkt en/of opslaat.	•	•	•	•
CD 19	De leverancier waarborgt dat opslag van gegevens en bedrijfsregels plaatsvindt in landen die geacht worden een passend beveiligingsniveau te hebben. Een aanwijzing daarvoor kan gevonden worden in een lijst opgesteld door de Europese Commissie: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm).		•	•	•
CD 20	Beheer op en monitoring van systemen waarbinnen privacygevoelige / medische informatie wordt opgeslagen of verwerkt - is alleen toegestaan vanuit landen die genoemd zijn in richtlijn 19.		•	•	•
CD 21	Dienstverlening – waarbinnen privacygevoelige / medische informatie wordt opgeslagen of verwerkt - vanuit de Verenigde Staten is in verband met de Patriot Act niet toegestaan.		•	•	•

4.8 Beveiligingsaspecten van de overeenkomst

Het primaire doel van informatiebeveiliging is het beschermen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de UWV-gegevens.

Richtlijn	Omschrijving	RK-0	RK-I	RK-II	RK-III
	De leverancier heeft aantoonbaar informatiebeveiliging ingericht cf. de organisatiestandaarden				
CD 22	De dienstverlening vindt plaats onder de werking van een beveiligingsovereenkomst die is ondertekend met de leverancier. Daarin is vastgelegd dat de omgang met gegevens door de leverancier plaatsvindt binnen de vereisten die de afnemer daaraan stelt.	•	•	•	•

(vervolg)

CD 23	De leverancier beschikt over een gecertificeerd (ISO27001 of vergelijkbaar) Informatie Beveiliging Management Systeem (ISMS) , gerelateerd aan de te leveren diensten.		•	•	•
CD 24	De leverancier levert controleerbaar bewijs, in de vorm van een formele audit-verklaring, van de opzet, bestaan en werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van het geheel van de te leveren dienst(en).			•	•
CD 25	De afnemer heeft het recht de door de leverancier geleverde dienst en bijbehorende processen te auditen, deze audit door een derde partij te laten uitvoeren en de statutaire rechten van de auditors te benoemen.	•	•	•	•
CD 26	De leverancier monitort actief alle beveiligingsmaatregelen, correleert de status en de signalen (logging en events) afkomstig van deze beveiligingsmaatregelen.		•	•	•
CD 27	Activiteiten worden gelogd en gemonitord. Vooraf gedefinieerde activiteiten van gebruikers en alle activiteiten van beheerders, alle uitzonderingen en alle informatiebeveiligingsgebeurtenissen worden vastgelegd in logbestanden.		•	•	•
CD 28	De logbestanden, voor zover ze betrekking hebben op dienstverlening aan de afnemer, worden gedurende een overeengekomen periode bewaard en op verzoek aan de afnemer verstrekt.	•	•	•	•
	Er is een Service Level Agreement (SLA)				
CD 29	Het beoogde serviceniveau en onaanvaardbare serviceniveaus zijn in de SLA beschreven.	•	•	•	•
CD 31	De leverancier meet en bewaakt de vooraf gedefinieerde en verifieerbare (K)PI's van de dienst en rapporteert hierover aan de afnemer.	•	•	•	•
CD 32	De wijze waarop de noodzakelijke IT beheerprocessen[10] aan de kant van de afnemer zijn gekoppeld aan de leverancier, zijn beschreven.	•	•	•	•
	Verplichtingen zijn vastgelegd				
CD 33	De verplichting dat de leverancier na beëindiging van de overeenkomst alle vertrouwelijke gegevens van de afnemer correct uit haar systemen verwijdert, is contractueel vastgelegd.		•	•	•
CD 34	Iedere wijziging op een dienst wordt door de leverancier beoordeeld op impact op de informatiebeveiliging en compliancy met de beveiligingsbaseline en beleid van de afnemer.		•	•	•
CD 35	Iedere wijziging (change) in/op de dienst met een hoge impact of geconstateerde afwijking op de beveiligingsbaseline en/of het beleid van de afnemer, wordt door de leverancier aan de afnemer ter beoordeling voorgelegd en waar mogelijk voorzien van een alternatief voorstel en/of een overzicht van mitigerende maatregelen, inclusief een indicatie van de tijdelijkheid van afwijking (gedoogsituatie).			•	•
CD 36	De respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst zijn betrokken, zijn contractueel vastgelegd.	•	•	•	•
CD 37	De leverancier en bijgeval diens personeel ondertekenen een geheimhoudings-verklaring, als onderdeel van het contract.	•	•	•	•

[10] Dit betreft in ieder geval incident management

(vervolg)

CD 38	In het geval van een (dreigend) beveiligingsincident onderneemt de leverancier alle acties die noodzakelijk zijn om het risico voor de afnemer tot een minimum te beperken en meldt deze onmiddellijk aan de afnemer conform een vooraf afgesproken procedure.	•	•	•	•
CD 39	Ten aanzien van voorspelbare beveiligingsincidenten (o.a. malware-uitbraken, denial-of-service attacks, phishing attacks) beschikt de leverancier over periodiek geteste standaardscenario's, die in geval van een incident per direct in werking treden.	•	•	•	•

Bijlage 1: Surfnet [2010]: Privacy en security in the cloud;

Privacy en security in de Cloud

In het onderwijs neemt online samenwerking en het gebruik van online applicaties steeds meer toe. Verantwoordelijkheden omtrent data en persoonsgegevens worden als gevolg hiervan diffuser. Deze verantwoordelijkheid verschuift namelijk naar derde partijen (waaronder Coud Computing diensten) die online applicaties aanbieden, of er is sprake van gezamenlijke verantwoordelijkheid.
Het blijkt dat veel instellingen vragen hebben op dit gebied.

Cloud privacy

SURFnet heeft samen met SURFdirect - de digitale rechten expertise community van SURF - en Kennisnet, aan het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg gevraagd om antwoorden te formuleren op gesignaleerde vragen. Het resultaat is een rapport met als titel 'De wolk in het onderwijs: privacy aspecten bij Cloud Computing Services'. Hierin komen onderwerpen rond Cloud Computing aan bod waar basisscholen, middelbaar onderwijs en bij SURF aangesloten instellingen vragen over hebben. Dit rapport stelt de instellingen in staat om beter gefundeerde keuzes te maken over het inzetten van online applicaties.

Een onderwijsinstelling die een cloud dienst wil afnemen, zal daarvoor een contract moeten met de cloud leverancier sluiten. Het is belangrijk om op privacy afspraken te letten. De publicatie 'Cloud Computing & Privacy : Checklist privacy afspraken' is hierbij een handig hulpmiddel.
In deze checklist wordt aangegeven welke privacy afspraken verplicht en welke wenselijk zijn in het aangaan van een contract met een cloud leverancier.
Het betreft hier dus contractuele verplichtingen aangaande persoonsgegevens.

Cloud security

Voor onderwijsinstellingen die gebruikmaken van clouddiensten, of overwegen om dit te gaan doen, ontwikkelde SURFnet in samenwerking met SURF-IBO en Gartner de Checklist Cloud Security.
In deze checklist is vastgelegd welke vragen en processen de opdrachtgever zelf dient in te vullen en welke aspecten bij de cloud leverancier aandacht behoeven.

Meer informatie over Cloud en Privacy

Download rapport 'De wolk in het onderwijs: privacy aspecten bij Cloud Computing Services' (2011) [- 412 Kb]
Cloud Computing & Privacy: Het juridisch kader [PDF 764 Kb]
Cloud Computing & Privacy: Informatie over privacy afspraken [PDF 814 Kb]
Cloud Computing & Privacy: Internationale regelgeving [- 322 Kb]
Cloud Computing & Privacy: De Wet bescherming persoonsgegevens [PDF 323 Kb]
Cloud Computing & Privacy: Achtergrond Wet bescherming persoonsgegevens [PDF 200 Kb]
Checklist Cloud Computing & Privacy afspraken [PDF 361 Kb]
Randvoorwaarden Cloud Computing: Identity Management [PDF 671 Kb]
Download privacy in de praktijk - voorbeelden van toepassingen van de wet [PDF 302 Kb]
Download de Checklist Cloud Security (2011) [PDF 116 Kb]
Artikel Cloud computing: het juridisch kader [application/pdf 82 Kb]
Artikel Hoe veilig is de Cloud? [application/pdf 80 Kb]
Cloud Computing & Security: Beveiliging van gegegevens [PDF 313 Kb]
Mediaprotocollen - veilig aan de slag [PDF 669 Kb]

Bijlage 2: Cloud diensten en de USA Patriot Act

Uit: *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act*
Dr. J.V.J. van Hoboken, Mr. A.M. Arnbak & prof. Dr. N.A.N.M. van Eijk, m.m.v. mr. N.P.H. Kruijsen
Instituut voor Informatierecht, Universiteit van Amsterdam, september 2012
http://www.ivir.nl
http://www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf

Managementsamenvatting

De overgang naar cloud computing levert de nodige vragen op. Een van de terugkerende vragen is of deze overgang consequenties heeft voor de toegang tot gegevens door buitenlandse overheden. Daarbij wordt typisch verwezen naar de Amerikaanse overheid en de zogenaamde Patriot Act, die het mogelijk zou maken dat gegevens van Nederlandse gebruikers van cloud diensten worden opgevraagd vanuit de VS. Deze notitie beantwoordt in opdracht van SURFdirect[11] de vraag in hoeverre dat het geval is, vanuit het perspectief van de kennisinstellingen in Nederland. Verder onderzoekt deze notitie de vraag hoe het beste omgegaan zou moeten worden met dit risico.

Er kan worden vastgesteld dat de Patriot Act een symboolfunctie is gaan spelen in het debat. Daarom wordt in deze notitie niet alleen gekeken naar deze specifieke wetgeving uit 2001, maar naar het bredere juridisch kader in de VS en Nederland voor wat betreft de toegang tot gegevens in het kader van strafvordering en nationale veiligheid. De notitie plaatst het vastgestelde juridische risico vervolgens in breder perspectief door te kijken naar de organisatie van de vertrouwelijkheid en veiligheid van gegevens in het algemeen. Op basis van de gemaakte analyse worden tenslotte aanbevelingen gedaan voor geïnformeerde besluitvorming in de sector.

Het antwoord op de gestelde vraag naar de mogelijkheden op toegang tot gegevens in de cloud voor justitie en veiligheidsdiensten in de VS is tegelijk simpel en complex. Wetgeving in de Verenigde Staten en Nederland zorgt ervoor dat politie, justitie of veiligheidsdiensten linksom of rechtsom een mogelijkheid hebben om gegevens van kennisinstellingen en betrokkenen op te vragen. De overgang naar cloud computing brengt hier in beginsel geen verandering in. Indien gebruik gemaakt wordt van een cloud dienst die onder Amerikaanse jurisdictie valt bestaat er de mogelijkheid dat gegevens direct in de VS bij de betreffende onderneming worden opgevraagd. Indien er geen jurisdictie is, bestaat de mogelijkheid dat gegevens worden opgevraagd via samenwerking met Nederlandse justitie of veiligheidsdiensten, bij een cloud dienst of bij de instelling zelf. Het voorkomen dat enige toegang plaatsvindt is gezien deze stand van zaken in elk geval juridisch niet mogelijk en garanties op dat punt zijn dus ook niet te geven.

Tegelijkertijd bestaan er significante verschillen tussen de mogelijkheden tot toegang door Amerikaanse autoriteiten. Zo is er in het geval dat gegevens direct opgevraagd kunnen worden bij de cloud dienst onder Amerikaanse wetgeving zeer beperkte rechtsbescherming voor Nederlandse gebruikers van deze dienst, terwijl zulke rechtsbescherming wel geldt in het geval van bevragingen onder Nederlandse wetgeving. De Amerikaanse constitutionele waarborgen op het gebied van bevragingen door de Amerikaanse overheid zijn niet van toepassing op Nederlandse gebruikers van de cloud. En de rechtsbescherming in specifieke Amerikaanse wetgeving ziet voornamelijk op Amerikaanse burgers en ingezetenen.

De betreffende Amerikaanse wetgeving biedt tegelijkertijd ruime mogelijkheden gegevens uit de cloud op te vragen, een mogelijkheid die in het geval van veiligheidsdiensten erg laagdrempelig is te noemen. Het gaat daarbij nadrukkelijk niet slechts om de Patriot Act uit 2001, maar om een complex en dynamisch geheel aan bevoegdheden van de Amerikaanse overheid op het gebied van opsporing

[11] SURFdirect is onderdeel van SURF, de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek.

en nationale veiligheid. Buiten het schetsen van het wettelijk kader, is er gezien het karakter van het handelen van deze diensten in de praktijk geen zicht te krijgen op de werkelijke bevragingen van gegevens vanuit de VS. Ondernemingen zullen typisch geen enkele mededeling kunnen doen over de vraag of bevragingen plaatsvinden. Wel is te verwachten dat het opvragen van gegevens uit de cloud door overheden zal toenemen. Het gebrek aan aandacht in de VS voor de belangen van vertrouwelijkheid van gegevens van niet-Amerikanen maakt de situatie er vanuit Nederlands perspectief niet beter op. Het verdient opmerking dat het gaat om een onderwerp dat reeds op de agenda is geplaats in het Nederlandse parlement, alsmede in Brussel bij het Europese Parlement, de Europese Commissie en de Artikel 29 Werkgroep voor gegevensbescherming.

Deze notitie concludeert dat het voor de instellingen zaak is om zicht te krijgen en blijven hebben op de verschillende modaliteiten van toegang door justitie en veiligheidsdiensten en de daarmee samenhangende risico's voor kennisinstellingen goed in kaart te brengen. Het verdient aanbeveling deze observatie deel te laten uitmaken van een algemene maatschappelijke kosten-baten analyse, waarin alle op het spel staande belangen op het gebied van de informatiehuishouding worden meegenomen. Daarbij moet gedacht worden aan de belangen van informatieveiligheid, en vertrouwelijkheid, de privacy van betrokkenen, alsmede de voor de instellingen karakteristieke belang van de academische vrijheid en het gevaar van chilling effects op het gedrag van betrokkenen. Het is aan te bevelen binnen de sector een risicoanalyse te maken op basis van een categorisering van de verschillende soorten gegevens die het onderwerp zou kunnen worden van bevragingen. Voor gegevens waarvoor het risico onaanvaardbaar wordt geacht dat deze daadwerkelijk in handen zouden kunnen komen van een buitenlandse overheid, zonder dat daarover enige transparantie bestaat, zouden alternatieven ontwikkeld kunnen worden binnen de sector.

Dat toegang door overheden plaatsvindt is uiteraard geen nieuw gegeven. De te maken afwegingen bij de overgang naar cloud computing kunnen voortbouwen op binnen de instellingen bestaande protocollen, voorlichting en afwegingen ten aanzien van daadwerkelijke bevragingen. Het onderwerp dient bij het aangaan van cloud diensten besproken te worden en voorkomen moet worden dat op dit punt schijnzekerheden worden geboden door cloud providers. De mogelijkheid dat bevragingen vanuit het buitenland plaatsvinden is geen risico dat door middel van contractuele waarborgen kan worden uitgesloten en Nederlandse wetgeving op het gebied van privacy is ook geen waarborg. De vraag of een onderneming onder Amerikaanse jurisdictie valt, hetgeen al snel het geval is, dient door de betreffende onderneming zelf en overtuigend beantwoord te kunnen worden. Het is een hardnekkige misvatting dat er geen jurisdictie bestaat onder Amerikaans recht als de gegevens niet op Amerikaans grondgebied zijn opgeslagen. Het criterium in dit kader is of de cloud provider structureel activiteiten binnen de VS ontplooit, bijvoorbeeld door een vestiging te hebben, of onderdeel te zijn van een in de VS gevestigde onderneming die controle heeft over de betreffende gegevens.

Door de overgang naar cloud diensten zal in beginsel sprake zijn van een vermindering van de autonomie van de instellingen ten aanzien van de omgang met bevragingen. Daarom dient goed gekeken te worden naar de specifieke risico's bij bepaalde categorieën van gegevens, waaronder de vraag of er gegevens zijn waarvoor dit gebrek aan autonomie onaanvaardbaar is. Verantwoordelijken binnen de instellingen dienen verder te beseffen dat het geen probleem betreft dat na een enkele besluitvormingsronde van tafel is. Het betreft een onderwerp dat een heldere plaats dient te krijgen in de doorlopende besluitvorming over cloud computing in de sector. Er dient op hoog niveau meegedacht te worden over alternatieven die betere rechtsbescherming zouden kunnen bieden. De gedachtevorming over een nationale cloud kunnen hier een uitkomst bieden. Er kan vanuit de sector input geleverd worden voor het politieke debat over de ruime jurisdictie en toegang die de Amerikaanse overheid zich toebedeelt. En er dient voorkomen te worden dat lock-in het onmogelijk maakt dat voortschrijdend inzicht kan leiden tot nieuwe besluitvorming over dit complexe onderwerp.

Bijlage 3: Patriot Act: het wordt nog erger

http://www.computable.nl/artikel/opinie/cloud_computing/4635150/2333364/patriot-act-het-wordt-nog-erger.html

Uit: *Computable* 21-01-2013, door Theo Loth

"(…) Intussen is er een nieuwe ontwikkeling gaande die de vertrouwelijkheid van data nog verder bedreigt. De werking van de in 2008 ingevoerde *Foreign Intelligence and Surveillance Amendments Act* (FISAA) wordt verlengd.

Artikel 1881a van de FISAA heeft de mogelijkheid geschapen voor grootschalige surveillance die specifiek is gericht op data binnen het Amerikaanse rechtsgebied van niet-Amerikaanse burgers. De Fourth Amendment beschermt Amerikaanse staatburgers tegen de FISAA, in die zin dat voor het monitoren van Amerikanen specifieke warrants nodig zijn. *Niet-Amerikanen zijn niet beschermd*. De scope van de surveillance strekt zich uit tot communicatie en tot data in de publieke cloud. Informatie die het voorwerp van onderzoek kan zijn, is 'foreign intelligence information', waaronder informatie van - vanuit de Amerikaanse optiek - buitenlandse politieke organisaties en entiteiten die de belangen van de VS in het buitenland raken. (…) "

Bijlage 4: 38% personeel bewaart werkbestanden in Dropbox

Uit: *Security.nl* 4 juni 2013,12:49, door Redactie

https://www.security.nl/artikel/46497/1/%2738%25_personeel_bewaart_werkbestanden_in_Dropbox%27.html?utm_source=rssfeed&utm_medium=rss&utm_campaign=rssfeed

"38% van de Amerikaanse werknemers bewaart werkdocumenten en andere zakelijke bestanden bij privé clouddiensten zoals Dropbox, Google Drive en Apple iCloud. Dat blijkt uit onderzoek van Ipsos MORI onder 2000 Amerikanen. Naast de cloud zegt 91% ook persoonlijke apparatuur te gebruiken om werkbestanden te bewaren, te delen en te benaderen.

Meestal worden werkbestanden op externe harde schijven bewaard (64%). 46% gebruikt USB-sticks, gevolgd door mensen die hun documenten op cd's en dvd's branden (16%). Mannen blijken vaker clouddiensten en persoonlijke opslagmedia te gebruiken dan vrouwen.

Als het gaat om het werken met computerbestanden raken werknemers vooral gefrustreerd door het feit dat ze via e-mail geen grote bestanden kunnen versturen en veel tijd kwijt zijn bij het zoeken naar elektronische documenten."

Bijlage 5: De uitdagingen van certificering

Uit: *Computable* 06-07-2012, 10:31 door Alexandra Schless.

http://www.computable.nl/artikel/opinie/cloud_computing/4536855/2333364/de-uitdagingen-van-certificering.html - ixzz206XfPmah

'*Cloud computing is niet veilig*'. *Ik hoor het nog regelmatig. Laat ik voorop stellen dat ik het een vrij logische gedachte vind, maar niet steekhoudend. Met certificering van cloud computing ligt een goede oplossing om vertrouwen te kweken binnen handbereik. Laten we deze belangrijke stap naar volwassenheid zetten.*
Huiverigheid omtrent cloud computing is nog altijd aan de orde van de dag. De echte grote acceptatie laat op zich wachten zolang potentiële gebruikers nog niet precies weten wat er met hun data gebeurt. Wij krijgen van onze klanten dagelijks de vraag hoe zaken als veiligheid en continuïteit zijn geregeld. Voor datacenters is dit niet zo zeer een issue. Wij zijn erop ingericht om te werken conform de afgesproken sla's met onze klanten en aan te tonen hoe zaken in ons bedrijf geregeld of gecertificeerd zijn. Grotendeels is het een onderbuik gevoel dat mensen hebben, waardoor ze nog ietwat wantrouwend zijn. Data uit handen geven aan een externe partij vraagt om loslaten. En dat vinden mensen moeilijk, dat zit in onze natuur. De mens stelt nu eenmaal hogere eisen aan een ander dan aan zichzelf. Eigenlijk is het een strijd tussen wat technisch mogelijk is en wat het menselijk brein accepteert. Opvallend daarbij is dat we op persoonlijk gebied veel minder moeite hebben met cloud computing.
Willen we de professionalisering en acceptatie van cloud computing naar een hoger niveau tillen, dan ontkomen we niet aan een toetsingsmethode, een leidraad voor de eindgebruiker. Certificering werkt als een benchmark voor de leverancier. Het maakt het keuzeproces een stuk eenvoudiger: het maken van een vergelijking tussen verschillende aanbieders is simpeler. We kweken er vertrouwen mee. Mensen willen nu eenmaal iets tastbaars in handen hebben. Iets wat tastbaar is, wordt sneller geaccepteerd. Certificering komt de integratie van cloud-oplossingen ten goede en het voorkomt wildgroei.

Voorkomen

Momenteel ontstaan er op verschillende niveaus certificeringen bij verschillende organisaties. Een goede zaak, denkt echter iedereen vanuit zijn eigen achterban. Dat moeten we juist voorkomen, anders zien gebruikers straks door de bomen het bos niet meer. En het moet vooral in de praktijk eenvoudig te toetsen zijn. Anders haakt een grote groep bedrijven af. Zinvoller is om te luisteren naar de verschillende initiatieven en daarin de grote gemene deler te vinden. Hieruit moet één certificering ontstaan die als basis dient voor iedere leverancier.
Ik ben me er van bewust dat het opzetten van een eenduidig certificeringsprogramma een dynamisch proces is en dat we niet alle cloud-oplossingen over één kam moeten scheren. Een cloud-oplossing bestaat immers uit verschillende deeloplossingen. Willen we een allesomvattende certificering die iedereen kan toepassen, dan hebben we met verschillende normen te maken. Het meest pragmatische is naar mijn idee te kijken naar deelgebieden. De leverancier moet ervoor zorgen dat alle deelgebieden gecertificeerd zijn en dit bij de eindgebruiker kunnen aantonen. Daar zal hij zelf tijd en middelen in moeten steken.
Wat nu concreet de volgende stap is? Het zou een goede zaak zijn als er een gerenommeerd en onafhankelijk instituut opstaat dat cloud certificering een formele status geeft. *Zo heeft NEN werkgroepen opgestart, die kijken naar wat er moet gebeuren en welke bestaande normen te hergebruiken zijn.* Het is een stap in de goede richting. Hoe sneller een certificering tot stand komt, hoe sneller acceptatie volgt. Als de grotere partijen het accepteren, volgen de kleinere vanzelf. Actie reactie.

Bijlage 6: SaaS-provider bij hack nauwelijks aanspreekbaar

Uit: Automatiseringsgids 1 augustus 2013 14:20 Rolf Zaal NIEUWS

http://www.automatiseringgids.nl/nieuws/2013/31/saas-provider-bij-hack-nauwelijks-aanspreekbaar

Cloud-dienstverleners doen veel te moeilijk over garanties rond databeveiliging. Onafhankelijke controle en afspreken dat een contract wordt ontbonden als de beveiliging tekortschiet, is doorgaans al te veel gevraagd. Consensus over wat als data-bescherming mag gelden en hoe dat contractueel wordt vastgelegd ontbreekt ten enenmale. Als zich een datalek voordoet, dan hebben klanten juridisch nauwelijks enige houvast.

Afnemers van clouddiensten zijn niet tevreden over de beveiliging van hun gegevens. Dat geldt met name waar het om cloud-applicaties ('SaaS') gaat. Dat constateert Gartner. De IT-marktonderzoeker stelt vast dat providers vaak nogal halfslachtige voorwaarden hanteren wat betreft het de handhaving van de vertrouwelijkheid van gegevens, de integriteit van de data en de mogelijkheden van dataherstel na calamiteiten. Afnemers storen zich daaraan. Onder meer omdat het hun positie bemoeilijkt als toezichthouders vragen hebben over het risicobeheer.

Jaarlijkse audit is wel het minimum
Volgens analist Alexa Bona van Gartner zouden SaaS-providers ten minste jaarlijkse audits door onafhankelijke deskundigen mogelijk moeten maken, met daaraan verbonden het recht om de overeenkomst op te zeggen als er duidelijke gebreken of fouten in de beveiliging aan het licht komen. Een online inbraak of datadiefstal zou al helemaal als een onbetwistbare grond voor ontbinding van de SaaS-overeenkomst moeten gelden.
Gartner ziet in die situatie niet snel verbetering optreden en zegt te verwachten dat volgend jaar nog altijd zo'n 80 procent van de IT-inkopers negatief zal zijn over de garanties die SaaS-providers hen voorhouden.

Standaard moet nog ontstaan
Ook verbaast het Bona dat veel providers niet alle informatie beschikbaar stellen die kopers nodig zouden hebben als ze hun keuze voor een aanbieder zouden willen baseren op een evaluatie aan de hand van de Cloud Controls Matrix (CCM). Dat is een door de Cloud Security Alliance (CSA) opgestelde spreadsheet waarin leden van de CSA de door hen relevant bevonden controle-aspecten in kaart brengen. Bona zegt er overigens wel vertrouwen in te hebben dat deze CCM op termijn tot een standaard kan uitgroeien doordat meer IT-inkopers hem zullen hanteren en providers er zodoende steeds minder omheen zullen kunnen.

Boetes die wat voorstellen
De bepalingen die bij SaaS-providers voor service-level-garanties (SLA's) door moeten gaan, zijn bij nadere lezing fors onder de maat, stelt Bona vast. "Hoe je zo'n SLA verwoordt doet er niet toe, maar IT-inkopers moeten er op kunnen rekenen dat hun gegevens worden gevrijwaard van aanvallen, dat hun bestanden na een calamiteit kunnen worden hersteld en dat de garanties daarvoor in het contract zijn terug te vinden. (..) *We raden aan dat ook reactie- en hersteltijden en de concrete maatregelen rond data-integriteit worden vermeld, samen met boetes die iets voorstellen indien die doelen niet worden gehaald.*"
Maar vooralsnog is er geen consensus over wat in de cloud als data-bescherming mag gelden en hoe dat contractueel kan worden vastgelegd. SaaS-providers grijpen die situatie aan om zichzelf zo min mogelijk op wat dan ook vast te leggen.

(cursiveringen door red.)

Referentiedocumentatie

Versie	Datum	Titel	Van
3.0	25-8-2011	UWV: Tactisch Beleid Beveiliging & Privacy	UWV intern
0.9	28-2-2011	UWV-Beleid kantoorautomatisering werkplek en netwerk	UWV intern
1.0	19-7-2005	UWV: Classificatiemodel	UWV intern
2.3	06-04-2011	UWV-Beveiligingsovereenkomst versie 2.3 definitief	UWV intern
0.3	april 2011	UWV/IT-Beleid & Strategie 2011	UWV intern)
	april 2001	Beveiliging van persoonsgegevens Achtergrondstudies en Verkenningen 23	G.W. van Blarkom drs. J.J. Borking
	februari 2013	CBP-Richtsnoeren Beveiliging van persoonsgegevens	CBP
	04-05-2011	http://nl.wikipedia.org/wiki/Software_as_a_service	
	06-07-2011	http://en.wikipedia.org/wiki/Cloud_computing	
	januari 2011	The NIST Definition of Cloud Computing	NIST
0.7	08-01-2011	UWV-beveiligingsbeleid clouddiensten	Marcel Koers e.a.
Toegevoegd aan oorspronkelijk (UWV-)document:			
	januari 2012	NCSC Whitepaper NCSC 'Cloudcomputing & security'	NCSC
	november 2009	ENISA 'Cloudcomputing: Benefits, risks and recommendations for information security'	ENISA
	7-06-2013	http://nl.wikipedia.org/wiki/Cloud_computing	
	[2010]	Privacy en security in de cloud	Surfnet
	september 2013	Clouddiensten in zowel hoger onderwijs als onderzoek en de USA Patriot Act -Managementsamenvatting	Van Hoboken e.a., Inst. voor Informatierecht, Univ. van Amsterdam
	21-01-2013	Patriot Act: het wordt nog erger	Theo Loth
	04-06-2013	38% personeel bewaart werkbestanden in Dropbox	security.nl
	06-07-2012	De uitdagingen van certificering	Alexandra Schless
	01-08-2013	SaaS-provider bij hack nauwelijks aanspreekbaar	Rolf Zaal

Aanvankelijk waren door reviewers bij de ADR (Auditdienst Rijk) twee uitgebreide en waardevolle aanvullingen ingezonden. Deze teksten hebben bij de ADR echter nog conceptstatus en zijn, op verzoek van de ADR, tot nader order uit deze versie verwijderd.

Lijst van afkortingen (in de hoofdtekst)

A&V23	Achtergrondstudies en Verkenningen 23
BIR-TNK	Baseline Informatiebeveiliging Rijksdienst (en Tactisch Normen Kader)
BKWI	Bureau Keteninformatisering Werk en Inkomen
BSN	Burger Service Nummer
CBP	College Bescherming Persoonsgegevens
CMM	Capability Maturity Model (-systematiek)
DPB	Domeingroep Privacy en Beveiliging (in Suwi-verband)
DMZ	Gedemilitariseerde zone (bufferzone in IT-landschap)
ENISA	European Network and Information Security Agency
GBA	Gemeentelijke Basis Administratie (voor persoonsgegevens)
GeVS	Gezamenlijke elektronische Voorziening Suwi
IDM	Identiteit en Access Management
ISO	Internationale Organisatie voor Standaardisatie
LDAP	Lightweight Directory Access Protocol
NCSC	Nationaal Cyber Security Centrum
NIST	National Institute of Standards and Technology
OTAP	Ontwikkeling Test Acceptatie en Productie
SAAS	Software as a service
SAML	Security Assertion Markup Language
SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
TPM	Third party mededeling (of: memorandum)
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VIR-BI	Voorschrift Informatiebeveiliging - Bijzondere Informatie (VIR-BI)
Wbp	Wet bescherming persoonsgegevens
XAMCL	eXtensible Access Control Markup Language
ZBO	Zelfstandig bestuursorgaan

Reviewers en verantwoording

Aan deze review van de UWV-conceptnotitie "UWV beveiligingsbeleid clouddiensten v.0.7" hebben meegewerkt en bijgedragen:
Jan Roodnat en Leon Dirks (ADR)
Rob Kuppens (CAK)
Chris Eyzenga (CJIB)
Anne Marie van Rooij (CVZ)
Peter de Witte (SVB)
Wim Vlaanderen Oldenzeel (UWV)
Marleen Hulshof (UWV)
Judith Unk (UWV)
Ruud de Bruijn (UWV/CIP)
Ruud de Bruijn tekent voor verwerking van de commentaren, de omwerking naar dit CIP-document en de keuze van bijlagen, met dank aan Ad Reuijl en Peter Ruyter (UWV) voor kritisch meelezen.

CIP, Amsterdam, april 2014
Documentnaam Word: [Beveiligingsbeleid clouddiensten CIP DEF v2_3 (excl ARD).doc]