



Cloud security

Checklist en de te stellen vragen



Voor deze publicatie geldt de Creative Commons Licentie "Attribution 3.0 Unported".

Meer informatie over deze licentie is te vinden op <http://creativecommons.org/licenses/by/3.0/>

Samenvatting

Onderwijs- en onderzoeksinstellingen ontdekken de mogelijkheden van “cloud computing”. In de cloud zijn resources echter niet langer onder volledige controle van de instelling. Daarnaast leggen cloud providers de instelling uniforme afspraken voor. Dit roept bij instellingen vragen op ten aanzien van beveiliging. Hoe veilig is de cloud nu eigenlijk? Kan ik specifieke afspraken maken met een cloud provider? Waar moet ik aan denken wanneer ik in zee wil gaan met een cloud provider?

Het doel van dit document is om een leidraad te bieden voor de beveiliging van cloud computing. Welke aspecten spelen er? Welke punten moet een onderwijs- of onderzoeksinstelling in ogenschouw nemen wanneer zij met een cloud provider zaken wil doen?

COLOFON

Project : SURFworks
Projectmanager : Rogier Spoor
Auteur(s) : Guido van der Harst (Gartner), SURFibo
Datum : December 2010

Dit project is tot stand gekomen met steun van SURF, de organisatie die ICT-vernieuwingen in het hoger onderwijs en onderzoek initieert, regisseert en stimuleert door onder meer het financieren van projecten. Meer informatie over SURF is te vinden op de website (www.surf.nl).



Inhoudsopgave

1	Inleiding	1
1.1	Achtergrond	1
1.2	Doel	1
1.3	Publiek	1
1.4	Leeswijzer	2
2	Cloud Computing	3
2.1	Kenmerken	3
2.2	Leveringsmodellen	3
2.3	Afnamemodellen	4
2.4	Risico's	4
3	Rol als opdrachtgever	6
3.1	ICT-strategie en governance	6
3.2	Gewenste dienstverlening	6
3.3	Business case	7
3.4	Gebruikersgedrag	8
3.5	Gebruikersovereenkomsten	8
3.6	Inkoopvoorwaarden	8
4	Eisen aan de cloud provider	9
4.1	Stabiliteit	9
4.2	Affiniteit met het onderwijs	9
4.3	Certificering	10
4.4	Adoptie open standaarden en open source	11
4.5	Bedrijfsethiek	11
5	Dienstverleningsaspecten	12
5.1	Levering functionaliteit	12
5.2	Gegevens	12
5.3	Operationele dienstverlening	13
5.4	Transitie	13
5.5	Uitstapsscenario	14
5.6	Juridische zaken	14
6	Slotwoord	16
	Werkgroep	17



1 Inleiding

1.1 Achtergrond

Onderwijsinstellingen ontdekken in toenemende mate de mogelijkheden van “cloud computing”. Google Apps en Microsoft Live@edu zijn voorbeelden van diensten waarbij de resources gedeeld worden door een grote groep eindgebruikers. De besparingen die Google en Microsoft dankzij de schaalvoordelen realiseren zien de afnemers terug in het prijskaartje. Andere aantrekkelijke voordelen van het uitbesteden van ICT-diensten aan “cloud providers” liggen op het vlak van flexibiliteit, beheer en up-front investeringen.

In de cloud zijn resources niet langer onder controle van de instelling. Sterker nog: de resources worden gedeeld met derden. Om de schaalvoordelen daadwerkelijk te realiseren leggen cloud providers hun klanten uniforme afspraken voor. Dit roept bij onderwijs- en onderzoeksinstituten vragen op ten aanzien van beveiliging. Hoe veilig is de cloud nu eigenlijk? Kan ik eventueel specifieke afspraken maken met een cloud provider? Waar moet ik aan denken wanneer ik in zee wil gaan met een cloud provider?

Dit document gaat in op deze en vergelijkbare vragen.

1.2 Doel

Het doel van dit document is om een leidraad te bieden voor de beveiliging van cloud computing. Welke aspecten spelen er? Welke punten moet een onderwijs- of onderzoeksinstituten in ogenschouw nemen wanneer zij met een cloud provider zaken wil doen?

De bredere context van cloud computing in het onderwijs achtergronden, mogelijkheden, valkuilen en ontwikkelingen zijn beschikbaar in een aparte publicatie die SURFnet samen met Kennisnet heeft uitgebracht onder de titel “Cloud computing in het Onderwijs”.¹

Een belangrijk aspect van beveiliging is privacy. Op dit gebied gelden specifieke wettelijke richtlijnen. Deze richtlijnen hebben invloed op de afspraken die een onderwijsinstelling met een cloud provider moet maken. De privacy-aspecten van cloud computing zijn dermate specifiek dat deze niet passen binnen dit document. SURFnet heeft hiervoor een apart white paper geschreven met de titel “De wolk in het onderwijs”.²

1.3 Publiek

Dit document is geschreven voor ICT-verantwoordelijken van onderwijs- en onderzoeksinstituten die gebruik maken van cloud computing of die overwegen om gebruik te gaan maken van cloud computing.

¹ Zie http://www.surfnetkennisnetproject.nl/attachments/session=cloud_mmbase+2178257/PublicatieCloudComputing_webversie.pdf

² Het document genaamd “De wolk in het onderwijs” wordt in januari 2011 gepubliceerd.



1.4 Leeswijzer

Dit document kiest voor een pragmatische insteek. Hoofdstuk 2 behandelt de achtergrond van cloud computing en waarom er voor cloud computing andere zaken van belang zijn dan bij reguliere uitbesteding van ICT-diensten. Vervolgens kijkt hoofdstuk 3 naar welke zaken een onderwijsinstelling moet hebben geregeld voordat een cloud provider kan worden geselecteerd en gecontracteerd. Hoofdstuk 4 gaat in op de belangrijkste te stellen criteria aan de leverancier van de cloud diensten. Hoofdstuk 5 staat stil bij de essentiële beveiligingsaspecten ten aanzien van de dienstverlening zelf. Hoofdstuk 6 eindigt het document met een slotwoord.



2 Cloud computing

In dit hoofdstuk geven we een definitie van cloud computing. We kijken naar de kenmerken en leverings- en afnamemodellen en staan stil bij de specifieke risico's.

2.1 Kenmerken

Gartner definieert cloud computing als "een manier om computerkracht te leveren waarbij schaalbare en flexibele ICT-capaciteiten als een dienst beschikbaar worden gesteld aan verscheidene externe klanten op basis van internettechnologie". Cloud computing kent in deze definitie vijf karakteristieken:

- geleverd als dienst;
- schaalbaar en flexibel;
- gedeeld met derden;
- betalen naar gebruik;
- gebaseerd op internettechnologie.

2.2 Leveringsmodellen

Het Amerikaanse National Institute of Standards and Technology onderkent drie leveringsmodellen van cloud computing die inmiddels algemeen worden gehanteerd:

- *IaaS* – Infrastructure as a Service is de basisvariant. Hierin wordt pure reken- of opslagcapaciteit ter beschikking gesteld. Voorbeelden zijn: Amazon EC2 & S3, GoGrid en Rackspace Cloud.
- *PaaS* – Platform as a Service gaat een stap verder. Hierbij wordt een ontwikkelomgeving ter beschikking gesteld op basis waarvan afnemers zelf applicaties kunnen ontwikkelen, beheren en exploiteren. Voorbeelden zijn: Appian, Cordys, Microsoft Windows Azure, Tibco Silver.
- *SaaS* – Software as a Service gaat het verst. Hierbij bestaat de dienstverlening uit een kant-en-klare applicatie. Voorbeelden zijn: Basecamp, Dropbox, Google Apps, Microsoft Live@edu, Salesforce.com.

Elk leveringsmodel kent andere vormen en mogelijkheden tot risicobeheersing. In het SaaS-model waarbij nagenoeg alles is uitbesteed is de provider verantwoordelijk voor praktisch alle beveiligingsaspecten met uitzondering van het beheren van gebruikers en gebruikersrechten (functioneel beheer). Een SaaS-afnemer heeft maar beperkt de mogelijkheid om beveiligingsmaatregelen toe te voegen, aan te passen en te controleren. Denk hierbij aan het gehanteerde authenticatiemechanisme en logging.

In het PaaS-model liggen de beveiligingsopties redelijk vast binnen de ontwikkelomgeving en het platform. Hierbij hebben zowel de provider als de afnemer beide een verantwoordelijkheid.

In het IaaS-model is de afnemer voor een groot deel verantwoordelijk voor het adequaat implementeren van beveiligingsmaatregelen. De provider is in dit model nog steeds verantwoordelijk voor de fysieke beveiliging en voor de hardware en kan optreden als verkeersregelaar voor het netwerk dat gedeeld wordt door alle afnemers.



2.3 Afnamemodellen

Naast de drie leveringsmodellen kunnen we ook onderscheid maken naar verschillende typen afnamemodellen die voor onderwijs- en onderzoeksinstellingen interessant zijn. Deze modellen zijn:

- *Zelfstandige inkoop public cloud* – Hierbij neemt een individuele onderwijsinstelling cloud diensten af van een cloud provider. Deze diensten biedt de cloud provider ook aan derden aan. De ingezette resources worden altijd met derden gedeeld.
- *Gezamenlijke inkoop public cloud* – Dit is hetzelfde afnamemodel maar de inkoop geschiedt door een groep van instellingen. Deze vorm van afname kan zorgen voor een betere onderhandelingspositie ten opzichte van de cloud provider. Dit kunnen ad hoc combinaties zijn van instellingen die op een bepaald gebied hetzelfde doel nastreven. Ook is het mogelijk dat bijvoorbeeld op generieke vlakken SURFnet of SURFdiensten optreden als inkoper namens alle (aangesloten) instellingen.
- *Gezamenlijke inkoop private cloud* – De inkoop vindt hier net als in het vorige model gezamenlijk plaats, echter de resources die door de cloud provider worden ingezet, zijn in belangrijke mate exclusief toegewezen aan de afnemende instellingen. Er is maar zeer beperkt sprake van het delen van resources buiten het consortium. In dit model kan ook een onderwijs- of onderzoeksinstelling zelf optreden als cloud provider voor andere deelnemende instellingen.
- *Individuele inkoop private cloud* – Voor de volledigheid noemen we deze mogelijkheid ook nog. Volgens de definitie is hier eigenlijk geen sprake meer van cloud computing omdat de resources niet worden gedeeld met andere partijen.

De mogelijkheden tot risicobeheersing nemen in bovengenoemde afnamemodellen toe. Bij zelfstandige inkoop van public cloud diensten zijn de mogelijkheden beperkt. Bij gezamenlijke inkoop kan de inkoopcombinatie door de sterkere onderhandelingspositie stringenter eisen stellen. Bij gezamenlijke inkoop van private cloud diensten kunnen door het exclusieve karakter de meeste eisen worden gesteld.

2.4 Risico's

De volgende drie dimensies bepalen de risico's van een computersysteem:

- *Uitbreidbaarheid* – de mate waarin nieuwe code kan worden toegevoegd aan een systeem. Alle computersystemen hebben een bepaalde graad van uitbreidbaarheid. Besturingssystemen kunnen eenvoudig nieuwe code accepteren in de vorm van bijvoorbeeld device drivers en patches. Nieuwe code brengt nieuwe risico's met zich mee.
- *Toegankelijkheid* – het gemak waarmee toegang kan worden verkregen tot het systeem. Hoe eenvoudiger het is om toegang te krijgen, hoe makkelijker het is om misbruik te maken van het systeem. "Het enige veilige systeem is een computer, ingepakt in een laag van zes meter gewapend beton, die uitstaat."
- *Complexiteit* – de complexiteit van het systeem in termen van code en componenten. Het aantal regels code bepaalt het aantal zwakke punten in een systeem. Het aantal componenten bepaalt de beheerbaarheid.

Wanneer we cloud computing tegen deze dimensies aanhouden zien we dat met name de toegankelijkheid en complexiteit hoog scoren. Daar komt bij dat cloud providers onder druk van concurrenten hun business modellen uitbreiden met andere vormen van dienstverlening. SaaS-providers voegen PaaS-diensten toe, IaaS- en PaaS-leveranciers experimenteren met SaaS-diensten. Elke uitbreiding verhoogt de kans op onacceptabele zwakheden in het systeem.



Risico's met cloud computing zijn voor een deel vergelijkbaar met andere extern geleverde ICT-diensten. Te denken valt aan gegevenssegregatie, privacy, toegang, stabiliteit leverancier, beschikbaarheid en herstel. De locatie-onafhankelijkheid en de mogelijkheid dat een cloud provider gebruik maakt van diensten van derden brengen voor cloud computing specifieke risico's met zich mee.

Daarnaast kent cloud computing ook beveiligingsvoordelen. Door de schaalvoordelen zijn beveiligingsmaatregelen goedkoper te implementeren. Ook kunnen cloud providers beveiligingsmiddelen sneller en dynamischer inzetten. Tot slot beschikken cloud providers vaak over diep inhoudelijke beveiligingskennis die aan de afnemerszijde ontbreekt.



3 Rol als opdrachtgever

Voordat een onderwijsinstelling een cloud provider kan selecteren en contracteren is het eerst zaak om de volgende aspecten goed op een rij te hebben:

- ICT-strategie en governance
- Om welke dienstverlening gaat het?
- Is er een business case voor cloud computing?
- Gebruikersgedrag
- Welke gebruikersovereenkomsten gaat dit raken?
- Zijn de inkoopvoorwaarden up-to-date?

Daarnaast gelden er specifieke wettelijke verplichtingen bij het vastleggen van persoonsgegevens, die de onderwijsinstelling moet nakomen. Deze verplichtingen vallen buiten de scope van dit document maar zijn uitvoering beschreven in het SURFnet white paper “De wolk in het onderwijs”.³

3.1 ICT-strategie en governance

Nog voordat een instelling overweegt om gebruik te maken van cloud computing is het essentieel om over een basis te beschikken die de instelling in staat stelt om de externe leverancier vakkundig aan te sturen. Deze basis bestaat uit de volgende elementen:

- *Regieorganisatie* – binnen de instelling zijn taken als ICT-leiderschap, visie en architectuur, leveranciersmanagement, service management en functioneel beheer eenduidig belegd. Vakinhoudelijke kennis is aanwezig om het aanbod en het presteren van de cloud provider te beoordelen. De instelling is in staat om langdurig op verschillende niveaus relaties te onderhouden met de cloud provider.
- *ICT-strategie* – de stip op de horizon (4-5 jaar) ten aanzien van ICT is gedefinieerd en gedragen onder de stakeholders van de instelling. Er is een sourcingstrategie die bepaalt wat de instelling zelf doet en wat er wordt overgelaten aan de markt. Ten slotte is er een roadmap van projecten om de stip op de horizon te bereiken.
- *Governance* – de besluitvorming rond projecten en de ICT-operatie is ingeregeld. Verantwoordelijkheden en bevoegdheden van alle betrokkenen liggen vast. Er wordt actief gestuurd op het realiseren van de roadmap.

3.2 Gewenste dienstverlening

Voordat er gesproken wordt met cloud providers is het belangrijk om een goed en scherp beeld te definiëren van de gewenste dienstverlening. Om welke functionaliteiten gaat het? Bestaan er normenkaders waar de instelling zich aan moet conformeren ten aanzien van deze functionaliteiten? Hoe vertalen deze normenkaders zich naar service levels? Welke service levels zijn gewenst? Hierbij is het ook van belang om zicht te hebben op de classificatie van de gegevens die straks in de “cloud” terechtkomen.

Het volgende is een checklist van punten waar een instelling invulling aan moet geven:

³ Het document genaamd “De wolk in het onderwijs” wordt in januari 2011 gepubliceerd.



- Break-down van functionaliteiten
- Niet functionele eisen
 - *Beschikbaarheid* – de mate waarin de dienstverlening beschikbaar is voor de gebruikers in termen van continuïteit en prestaties
 - *Integriteit* – de betrouwbaarheid van een gegeven in termen van volledigheid, juistheid, tijdigheid en de mate waarin de gegevens alleen gewijzigd kunnen zijn door een daartoe geautoriseerde persoon
 - *Vertrouwelijkheid* – de waarborg dat gegevens alleen te benaderen zijn door personen die daartoe zijn geautoriseerd
 - *Onweerlegbaarheid* – de waarborg dat ontvangst en/of verzending van gegevens niet kan worden ontkend door betrokken partijen
 - *Bedienbaarheid* – de mate van gemak waarmee gebruikers de dienst kunnen bedienen

Ten slotte is het zaak om de parameters rond de dienstverlening in kaart te brengen. Om hoeveel gebruikers gaat het? Hoeveel gegevens? Hoeveel transacties? Deze parameters bepalen in belangrijke mate de kosten die de cloud provider in rekening brengt.

3.3 Business case

Een high-level business case kan inzicht bieden in de beslissing om wel of niet voor een cloud provider te kiezen. De business case zet de volgende vier elementen tegenover elkaar:

- Dekking dienstverlening bij zelf doen
- TCO zelf doen
- Dekking door cloud provider
- TCO bij gebruik cloud provider

Onder “dekking dienstverlening” verstaan we de mate waarin de gedefinieerde functionaliteiten en het gedefinieerde niveau van dienstverlening (zie paragraaf 3.1) kan worden gerealiseerd, aan de ene kant door de instelling zelf, aan de andere kant door de cloud provider.

“TCO” staat voor Total Cost of Ownership. Dit zijn de totale kosten voor het ontwikkelen en beheren van het systeem voor de gedefinieerde dienstverlening gedurende de life cycle van het systeem. Voor de eigen TCO gaat het om de volgende posten:

- Eenmalige initiële investeringskosten
 - Licenties
 - Ontwikkelkosten
 - Project management voor ontwikkeling en transitie
 - Transitiekosten (conversie, migratie en roll-out)
- Verwachte uitstapkosten (kosten om de dienstverlening uit te faseren)
- Jaarlijks terugkerende operationele kosten
 - *Leverancierskosten* – periodieke licenties, onderhouds- en consultancykosten.
 - *Beheerkosten* – kosten van functioneel, applicatie en technisch beheer.
 - *Afschrijvingen* – afschrijving van hardware nodig voor het operationeel houden van het pakket.
 - *Training* – terugkerende trainingskosten voor beheerders, helpdesk en eindgebruikers.



Voor de TCO bij het gebruik van een cloud provider moet de instelling denken aan de volgende posten:

- Eenmalige initiële investeringskosten
 - Projectmanagement voor transitie
 - Transitiekosten (conversie, migratie en roll-out)
- Verwachte uitstapkosten (kosten om bij de cloud provider weg te gaan)
- Jaarlijks terugkerende operationele kosten
 - *Leverancierskosten* – vergoeding cloud provider: verwacht gebruik maal verwachte prijs per eenheid.
 - *Beheerkosten* – kosten van functioneel beheer en service management
 - *Training* – terugkerende trainingskosten voor beheerders, helpdesk en eindgebruikers.
 - *SaaS Escrowkosten* – kosten om bij het structureel wegvallen van de dienstverlening van de provider toch nog toegang te blijven houden tot de dienstverlening en de eigen gegevens.

3.4 Gebruikersgedrag

Bij de overstap naar cloud computing is het verstandig om het huidige gebruikersgedrag te analyseren. Hoe bewust zijn de gebruikers zich van de risico's? Hoe gaan ze om met hun wachtwoorden? Weten ze wat ze met welke data mogen? Kennen ze het begrip *social engineering*?⁴

Wanneer het bewustzijn laag is, kan de instelling een bewustwordingscampagne overwegen.

3.5 Gebruikersovereenkomsten

Ook is het belangrijk om relevante bestaande gebruikersovereenkomsten van de onderwijsinstelling zelf goed onder de loep te nemen. Hierbij gaat het vooral om de service levels en de voorwaarden waaronder de dienstverlening wordt geleverd. Bij gebruik van een cloud provider kunnen de service levels per definitie niet hoger zijn dan hetgeen de cloud provider biedt. Ook bij de voorwaarden is het zaak om goed de vergelijking te maken met de voorwaarden van de cloud provider.

3.6 Inkoopvoorwaarden

Tot slot spelen de eigen inkoopvoorwaarden een rol. Zijn deze voldoende met de tijd meegegaan?

Bij gesprekken met cloud providers is het aan te bevelen om de eigen voorwaarden als eerste op tafel te leggen. Zie ook paragraaf 5.6.

⁴ Lees hiervoor bijvoorbeeld het boek "De kunst van het misleiden" of in het Engels "The art of deception" van Kevin D. Mitnick uit 2002



4 Eisen aan de cloud provider

Wanneer helder is welke dienstverlening gewenst is en er is een positieve business case voor cloud computing dan is de volgende stap het selecteren van een cloud provider. Nadat getoetst is of een provider de gewenste functionaliteit kan leveren, is het zaak om de volgende aspecten nader te onderzoeken:

- Stabiliteit
- Affiniteit met het onderwijs
- Certificering
- Adoptie open standaarden en open source
- Bedrijfsethiek

4.1 Stabiliteit

Hierbij gaat het om de continuïteit van de provider als organisatie. Welke mate van zekerheid heeft de instelling dat de cloud provider gedurende de verwachte contractduur blijft bestaan. Faillissementen en overnames hebben meestal een negatieve impact op de dienstverlening.

De stabiliteit van een provider kan worden bepaald door te kijken naar:

- *Marktstrategie* – Op welke markten is de provider actief? Wat is het marktaandeel in deze markten? Op welke markten ligt de focus? Wat is de groeistrategie? In welk marktstadium bevinden de producten van de leverancier zich? Dog, Star, Cash-Cow of Question Mark?⁵
- *Business model* – Op welke manier verdient de provider geld? Kent de provider verschillende business modellen?
- *Innovatie* – Hoe innoverend is de provider? Hoe vaak worden nieuwe functionaliteiten toegevoegd aan het portfolio? Hoe uniek is de dienstverlening? Hoe groot is het R&D budget?
- *Geografische aanwezigheid* – Opereert de provider wereldwijd of richt deze zich op een bepaald geografisch gebied? In welke landen heeft de provider fysieke kantoren?
- *Financiële gezondheid* – Wat zijn de financiële kerncijfers van het bedrijf? Winst, omzet, liquiditeit, solvabiliteit en terugbetalingscapaciteit.

4.2 Affiniteit met het onderwijs

Voor een goede samenwerking is het altijd prettig wanneer de cloud provider enige affiniteit heeft met de onderwijswereld. Welke reputatie heeft de provider? Welke positie neemt de provider in bij andere Nederlandse onderwijs- en onderzoeksinstellingen? Is er een goede verstandhouding tussen de provider en de SURF-organisatie? Kan de provider referenties uit onderwijsland overhandigen?

⁵ Terminologie van de BCG-matrix van de Boston Consulting Group zie <http://nl.wikipedia.org/wiki/BCG-matrix>



4.3 Certificering

Cloud providers leveren cloud diensten op basis van zeer complexe, gedistribueerde en gevirtualiseerde infrastructures waar meerdere klantgroepen gebruik van maken. Dit resulteert in een aantal uitdagingen op het gebied van risicobeheersing waar bestaande evaluatiemethodieken niet direct mee om weten te gaan. ISO/IEC 27001 en SAS 70⁶ in het bijzonder zijn opgesteld met de aanname dat alle ins en outs van het onderhavige systeem volledig bekend zijn. Het mooiste zou zijn wanneer cloud providers direct onderworpen kunnen worden aan afhankelijkheids- en kwetsbaarheidsanalyses zoals de sector die de afgelopen dertig jaar heeft vormgegeven. In de praktijk zijn echter maar weinig providers bereid om hieraan mee te werken.

Een groeiend aantal providers stelt dat ze een SAS70-evaluatie hebben ondergaan. Hoewel dit interessante informatie kan bieden, gaat SAS70 alleen in op de processen van een provider, niet op de technische kwetsbaarheden. In veel cloud assessments wordt vaak het doorlopen ontwerp-, ontwikkel- en testtraject buiten beschouwing gelaten. Zonder zicht echter op hoe dit traject doorlopen is, zijn uitspraken ten aanzien van het beheer van de cloud provider prematuur en misleidend.

Hoe nieuwer en complexer de onderliggende technologie is, hoe kleiner de kans dat assessments als SAS70 en ISO 27001 alle relevante risico's zullen identificeren. Bij het opvragen van informatie rond de beveiliging van de cloud provider is daarom het verstandig om naast SAS70, ISAE3402 en ISO 2700x verklaringen vooral ook te letten op:

- Geldigheid van alle statements;
- Een goed gedocumenteerd assessment van het ontwikkelproces van de cloud provider door een onafhankelijke expert;
- Het recht van de instelling om periodiek een audit te laten uitvoeren op de processen van de cloud provider door een onafhankelijke expert;
- Screening van medewerkers;
- Behaald CMMI level;
- ITIL-certificaten;
- Kwalificaties van de medewerkers (ITIL, Microsoft-certificaten, CCISP, opleidingsniveau);
- De beveiligingsrichtlijnen die de provider intern hanteert en diens omgang met urgente meldingen zoals viruswaarschuwingen;
- Implementatie van een vorm van business continuity management, bij voorkeur gebaseerd op BS 25999⁷ en indicatie dat crisissituaties regelmatig worden geoefend;
- Of een provider voldoet aan PCI, een Amerikaanse beveiligingsrichtlijn van de betaalkaartindustrie.⁸

⁶ ISAE 3402 is de opvolger van SAS 70. De belangrijkste verschillen zijn: ISAE 3402 kan verder gaan dan alleen de financiële rapportage, ISAE 3402 vereist ook een formele bevestiging van het management van de gebruikte controlemechanismen en ISAE 3402 geeft ook aan wat de bijdrage van de interne auditdienst was bij het onderzoek.

⁷ BS 25999 is een Britse standaard ontwikkeld door een groep experts afkomstig uit verschillende sectoren waaronder de overheid. De standaard geeft invulling aan het proces, de principes en terminologie van Business Continuity Management. Zie <http://www.bsigroup.com/>

⁸ Zie <http://www.pcicomplianceguide.org/pci-basics.php>



4.4 Adoptie open standaarden en open source

Wanneer een provider open standaarden toepast, kan dit ten goede komen aan de koppelbaarheid met andere systemen en biedt dit een zekere mate van onafhankelijkheid ten opzichte van de provider. Zicht op de "openheid" van de provider is daarom van belang. Is de provider lid van standaardisatie-organen als OMG en Oasis⁹? In welke mate draagt de provider bij aan de ontwikkeling van open standaarden? Welke open standaarden heeft de provider op zijn naam staan?

Open source is een ander aspect dat op twee manieren tot uiting kan komen. De provider kan (delen van) zijn oplossing als open source ter beschikking stellen. Op deze manier draagt de provider bij aan kennisdeling. De provider kan zelf ook gebruik maken van open source oplossingen. Hoe actief is de provider in de open source wereld? Welke producten stelt de provider met een open source licentie ter beschikking? Welke open source producten gebruikt de provider?

4.5 Bedrijfsethiek

Mogelijk streeft de onderwijsinstelling bepaalde doelen op het vlak van duurzaamheid na. Indien dit het geval is, is het van belang om de bedrijfsethiek van de provider nader te beschouwen. Is er een code of conduct? Zijn er duurzaamheidsverklaringen? Is er een maatschappelijk jaarverslag beschikbaar?

⁹ Zie <http://www.omg.org/> en <http://www.oasis-open.org/>



5 Dienstverleningsaspecten

Dit hoofdstuk gaat in op de punten die van belang zijn bij de evaluatie van de dienstverlening van de cloud provider. De wijze waarop de beoogde provider omgaat met deze punten zals een doorslaggevende rol spelen bij de uiteindelijke selectie. We gaan ervan uit dat de instelling heeft geverifieerd in welke mate de provider kan voldoen aan de in paragraaf 3.2 opgestelde eisen.

5.1 Levering functionaliteit

- Hoe snel kan de provider bepaalde wijzigingen in de services leveren en op welke wijze wordt de prioriteitsstelling bepaald?
 - Nieuwe gebruikers
 - Nieuwe functionaliteiten
 - Security fixes
- Op welke wijze evolueert de provider zijn dienstverlening?
 - Is de roadmap van de provider openbaar? Tot hoe ver gaat de roadmap?
 - In welke mate heeft de instelling invloed op de roadmap? Is er keuze? Kan een instelling kiezen om niet mee te gaan met nieuwe functies?
 - Kan de instelling kiezen om beta-functionaliteit aan of uit te zetten?
 - Hoe is de gebruikersvereniging georganiseerd? Zijn de verslagen openbaar?
- Het is ook belangrijk om zicht te hebben op de keten van providers en de wijze waarop beveiliging in de keten ingericht is.
 - Welke afhankelijkheden kent de provider?
 - Welke afspraken heeft de provider gemaakt met zijn onderaannemers?
- Hoe gaat de provider om met identity management?
 - Is aansluiting op de user directory van de instelling mogelijk?
 - Is aansluiting op SURFfederatie mogelijk?
 - Ondersteunt de provider de op dit vlak gangbare standaarden (bijvoorbeeld SAML 2.0)?

5.2 Gegevens

Ten aanzien van de gegevens die in de cloud worden opgeslagen zijn de volgende vragen relevant:

- Wie is verantwoordelijk voor de integriteit en vertrouwelijkheid van de gegevens? De meeste cloud providers zijn geneigd deze verantwoordelijkheid bij de klant te leggen.
- Hoe wordt het transport van gegevens van de instelling naar de provider en vice versa versleuteld? Welke vorm van encryptie wordt toegepast met welke sleutellengte? Worden de gegevens bij de provider ook versleuteld opgeslagen?
- Welke garanties geeft de provider op het doorvoeren van wijzigingen? Is bijvoorbeeld verwijderen ook echt verwijderen?
- In hoeverre is de provider aanspreekbaar op dataverlies als gevolg van een calamiteit? Is er een bonus-malus regeling gedefinieerd?



- Welke procedures en garanties heeft de provider voor back-up en recovery?
 - Kan dit periodiek worden getest door de instelling?
 - Welke fijnmazigheid geldt er voor back-up en recovery (individueel, groep en instelling)?
- Waar worden gegevens in de "cloud" opgeslagen? Er zijn providers die de garantie geven dat gegevens in bepaalde geografische regio's blijven. Dit kan belangrijk zijn in verband met wettelijke regels omtrent locaties waar bepaalde gegevens zich mogen bevinden.
- Blijft de instelling intellectueel eigenaar van de gegevens? Voor de meeste providers lijkt dit het geval. Er zijn echter uitzonderingen. Zo staat in de voorwaarden van Facebook dat het copyright op afbeeldingen die geplaatst worden op Facebook in eigendom komt van Facebook.
- Mag de cloud provider gegevens al dan niet geanonimiseerd doorverkopen of -spelen aan derden?

5.3 Operationele dienstverlening

Om een beeld te krijgen van de risico's ten aanzien van de operationele dienstverlening kan een instelling de volgende vragen stellen aan de cloud provider:

- Welke service levels hanteert de helpdesk van de provider?
 - Openingstijden
 - Reactietijden
 - Afhandelingstijden
- Hoe verloopt de afhandeling van calamiteiten en storingen?
 - Wie communiceert er met wie wanneer?
 - Welke rapportages levert de provider?
 - Welke rol heeft de eigen helpdesk?
 - Wat gebeurt er indien (onverhoopt) de gegevens van de instelling onder de hoede van de provider in het ongereede zijn geraakt?
- In hoeverre volgt de provider het gebruik van de dienstverlening door de instelling? Zijn de rapportages beschikbaar? Welke metagegevens (specifieke gegevens over het gebruik) worden door de provider vastgelegd, met wie worden die gedeeld en onder welke voorwaarden?

5.4 Transitie

De transitie omvat de migratie van de bestaande ICT-oplossing naar de dienstverlening van de cloud provider. Veelal gaat het hier om het migreren van (stam)gegevens, configuratie-instellingen en mogelijk ook het leggen van koppelingen met andere systemen.

Vragen die hier moeten worden gesteld zijn:

- Welke standaarden en procedures hanteert de cloud provider voor datamigratie? Welke mogelijkheden zijn er?
- Kan een configuratie (bijvoorbeeld de standaard sorteervolgorde van e-mail, gebruikte tags) worden gemigreerd van en naar de cloud provider?



Een randvoorwaarde bij migratie van vooral e-mailboxen is het gebruik van een domeinnaam die onafhankelijk is van de provider.

5.5 Uitstapsscenario

Na afloop van het contract met de cloud provider moeten de opgeslagen gegevens in een of andere vorm toegankelijk blijven voor de instelling.

- Welke procedures hanteert de provider op dit punt?
- Blijven gegevens inderdaad beschikbaar? Op welke wijze? Voor hoe lang? Sommige providers houden de gegevens tot 30 dagen vast na afloop. Bij anderen volgt directe vernietiging.
- Hoe eenvoudig kunnen de gegevens naar de instelling of naar een andere provider worden gemigreerd?
- Op welke wijze garandeert de provider dat de aan de instelling toevallende gegevens (ook metagegevens) daadwerkelijk vernietigd zijn nadat de instelling daartoe opdracht heeft gegeven?

5.6 Juridische zaken

Juridische zaken waar een instelling ondermeer op moet letten zijn:¹⁰

- *Acceptabel gebruik* – Alle providers hanteren clausules waarin aangegeven is dat de dienstverlening niet misbruikt mag worden. Een instelling moet de gewenste dienstverlening (zoals opgesteld in paragraaf 3.2) aanhouden tegen de definitie van acceptabel gebruik van de provider. Gegevens op bepaalde onderzoeksterreinen kan mogelijk buiten de definitie vallen. De recente case van Wikileaks en Amazon laat zien hoe een provider verdere dienstverlening onder verwijzing naar de clause van “acceptabel gebruik” kan weigeren.
- *Wijziging van de voorwaarden* – De condities waaronder de provider de voorwaarden mag wijzigen verschillen sterk per provider. Aankondigingen vooraf en schriftelijke bevestiging zijn aan te bevelen. Besteed hierbij ook aandacht aan de condities waaronder de instelling voortijdig van de overeenkomst af zou kunnen. Dit kan het geval zijn indien er een relatief lange looptijd is afgesproken en er zich in de tussentijd een alternatief aandient dat in alle redelijkheid veel beter is voor de instelling.
- *Arbitrage* – Sommige cloud providers prevaleren arbitrage boven een gerechtsgang. Instellingen moeten letten op vormen en locatie waar de arbitrage plaats dient te vinden. Hierbij zij opgemerkt dat een geschil betreffende een overeenkomst naar Nederlands recht natuurlijk te allen tijde door een contractpartij aanhangig gemaakt kan worden bij een Nederlandse rechter.

¹⁰ Een uitgebreidere juridische beschouwing is te vinden in het rapport “De wolk in het onderwijs” dat in februari 2011 wordt gepubliceerd.



- *Toepasselijk recht en jurisdictie* – De meeste cloud providers hanteren standaard het toepasselijk recht op de locatie waar hun hoofdkantoor is gevestigd. Om moeilijke situaties te voorkomen en te voldoen aan de Nederlandse wetgeving doen onderwijs- en onderzoeksinstituten er goed aan om het contract onder Nederlands recht te laten vallen en een clause op te laten nemen dat geschillen aan een vaste rechtbank in Nederland (in de buurt van de instelling) worden voorgelegd. Grotere providers bieden deze mogelijkheid meestal.



6 Slotwoord

De voordelen van cloud computing lonken. De voorgaande hoofdstukken zijn ingegaan op de aandachtsgebieden waar instellingen op moeten letten wanneer ze in zee willen gaan met een cloud provider. We hebben aangegeven waar een instelling allereerst zelf aan moet voldoen, welke eisen en wensen een instelling mag hebben ten aanzien van de cloud provider en wat de belangrijkste aandachtspunten zijn rond de dienstverlening.

We realiseren ons dat dit document slechts het begin vormt van de weg richting de afname van voldoende veilige dienstverlening in de cloud en dat het paper mogelijk meer vragen oproept dan het beantwoordt. We sporen de instellingen dan ook vooral aan om bij selectie en contractering van cloud providers de eigen kennis te verbreden en behaalde resultaten met elkaar te delen.

Succes!



Werkgroep

Dit document is mede tot stand gekomen op basis van een werkgroep van SURFibo. Aan deze werkgroep hebben de volgende personen deelgenomen:

- Eelco Braaksma, NHL Hogeschool
- Paul Dekkers, SURFnet
- Guido van der Harst, Gartner
- Bart van den Heuvel, Universiteit Maastricht
- Wim Koolhoven, Universiteit Twente
- Menno Nonhebel, KNAW
- Anita Polderdijk, Windesheim
- Jacques Schuurman, SURFnet
- Jens de Smit, SURFnet
- Rogier Spoor, SURFnet
- Bart Visser, Universiteit van Amsterdam

