VERTROUWEN IN DE CLOUD

WHITEPAPER

ONLINE TRUST COALITIE

02-2021 Whitepaper

INHOUD

Inleiding

Op initiatief van het Ministerie van Economische Zaken en Klimaat is de Online Trust Coalitie (OTC) gevormd, waarin ruim twintig organisaties afkomstig uit overheid, bedrijfsleven en wetenschap zich hebben verenigd. Het doel van de OTC, zoals neergelegd in het manifest van september 2020, is het verkennen, ontwikkelen en beschikbaar maken van meer eenduidige, efficiëntere en laagdrempelige methoden waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn en die het validatieproces van de afnemers ondersteunen.

De OTC richt zich op de manier waarop vertrouwen wordt geboden, gevraagd, geleverd en onderbouwd; niet zozeer op de beheersingsmaatregelen van informatieveiligheid of continuïteit van diensten en de gegevens zelf.

In dit whitepaper beschrijft de OTC een aantal acties die bijdraagt aan het aantonen van de betrouwbaarheid en veiligheid van clouddiensten. Daarmee wordt het vertrouwen in de cloud vergroot. Deze acties zijn gericht op alle betrokkenen, vanuit de overtuiging dat een betrouwbare en veilige cloud een gezamenlijke verantwoordelijkheid is. De intentie is dat de in dit whitepaper opgenomen acties worden opgepakt in de overtuiging dat met deze aanpak Nederland op dit terrein een koploperspositie kan innemen die navolging zal vinden in de rest van Europa.

Leeswijzer

Het whitepaper is als volgt opgebouwd. Na een algemene introductie over de aard van de vertrouwensproblematiek bij clouddiensten, wordt een onderscheid gemaakt tussen vertrouwen, betrouwbaarheid en zekerheid. Bij elk van deze aspecten worden er tekortkomingen geconstateerd: deze vormen de basis voor een zestal acties, geformuleerd in het slothoofdstuk.

1. Vertrouwen in clouddiensten

De cloud is niet meer uit onze samenleving weg te denken. De cloud speelt een belangrijke rol in onze dagelijkse activiteiten, in bedrijven, bij digitale innovaties en het beantwoorden van de grote maatschappelijke vraagstukken waar de samenleving voor staat.

Wat is de cloud

De OTC gebruikt voor clouddiensten de volgende definitie:

"Clouddiensten zijn een samenstel van IT-middelen, processen en organisatiestructuren dat via een netwerk op afstand toegang faciliteert tot een schaalbare en flexibele hoeveelheid capaciteit aan fysieke of virtuele IT-middelen met 'self-service' levering en beheer op aanvraag."

In eenvoudiger bewoording: in plaats dat je zelf een computercentrum hebt met eigen computers, randapparatuur, software en beheerders die de zaak draaiende houden, maak je gebruik van computercentra, computers, randapparatuur en software die door anderen worden beheerd en die je in de vorm van diensten ("as a Service") naar behoefte huurt om te gebruiken. De toegang tot die computercentra etc. loopt veelal via het internet en soms weet je zelfs niet waar die computercentra etc. zich fysiek bevinden.

Door voortdurende groei en specialisatie zijn clouddiensten in de praktijk vrijwel altijd opgebouwd uit andere clouddiensten, die door verschillende aanbieders worden geleverd.

Een groot voordeel hiervan is de schaalbaarheid. Je betaalt voor wat je gebruikt. Heb je (tijdelijk) meer nodig, dan is dat beschikbaar zonder dat je daar structurele investeringen voor hoeft te doen. Een ander groot voordeel is dat je altijd bij je gegevens en applicaties kunt zolang je toegang tot een netwerk (veelal internet) hebt. Je kunt dus je werk blijven doen waar je ook bent en met welke apparatuur (PC, laptop, tablet, mobiele telefoon) je ook maar werkt. Daarnaast nemen de leveranciers van clouddiensten je een hoop zorgen uit handen: zij zorgen er bijvoorbeeld voor dat de dienst optimaal beschikbaar is en dat je gegevens veilig zijn. Die ontzorging is een van de redenen waarom het gebruik van clouddiensten zo'n grote vlucht heeft genomen.

Het vraagstuk van vertrouwen in de cloud?

Er zijn echter ook nadelen. Doordat je het beheer van je IT uit handen geeft aan derden, creëer je afhankelijkheid. Je weet niet altijd waar je gegevens zich fysiek bevinden en wie daar allemaal bij kunnen. Dat levert een aantal vraagstukken op, zoals bijvoorbeeld:

- Wat gebeurt er met mijn gegevens en toepassingen als er iets met de leverancier gebeurt? Kan ik dan nog wel verder werken? Zijn mijn gegevens nog toegankelijk?
- Wie kijken er allemaal mee in mijn gegevens? De leverancier belooft mij dat alleen ik bij mijn gegevens kan, maar is dat ook zo? Onder welke wetgeving valt de (privacy) bescherming van mijn gegevens? Kan een overheid van de leverancier inzage eisen in mijn gegevens?
- Kan de leverancier zonder mijn goedvinden mijn software wijzigen?
- Als ik wil overstappen naar een andere leverancier, werkt mijn oude leverancier dan mee om mijn gegevens over te zetten? Heb ik dan nog toegang tot oude gegevens?

- Voldoet de dienst die ik afneem aan de voor mij geldende wet- en regelgeving? Kan ik dat continu aantonen?
- Hoe veilig ben ik tegen cyberaanvallen?
- Wat moet of kan ik als afnemer zelf doen om de beloofde veiligheid en betrouwbaarheid te realiseren?
- Hoe zit het met verantwoordelijkheden en aansprakelijkheid, als leveranciers niet doen wat ze hebben beloofd?

Deze lijst is verre van compleet. De vragen zijn redelijk generiek en spelen een rol bij de meeste clouddiensten.

Clouddiensten gedragen zich met betrekking tot verantwoordelijkheid, aansprakelijkheid, regie en control anders dan bij een traditionele uitbesteding. Bij traditionele uitbesteding is er altijd een (eind)verantwoordelijke partij, die regie heeft over de keten. Deze partij bepaalt de risico's en beheersmaatregelen, en implementeert de maatregelen in de keten. Dat werkt goed. De opdrachtgever stelt eisen aan opdrachtnemers lager in de keten. De regie over dit soort ketens bij uitbesteding werkt top-down.

Clouddiensten zijn daarentegen generiek, dat is de essentie van het cloud-businessmodel. Niet de individuele afnemers bepalen functionaliteit, risico's en de bijbehorende regimes, maar clouddienstverleners bepalen dat zelf. Zij doen dat op basis van eigen, generieke risicomodellen, en met een eigen keuze voor beheersingsregimes en normenkaders. Weliswaar doen ze dat met een scherp oog voor de beoogde gebruikers, maar zonder differentiatie van maatregelen voor elke afzonderlijke gebruiker.

De consequentie van dit businessmodel is dat de gebruiker slechts beperkt invloed heeft op hoe de leverancier zijn dienst inricht. Het enige wat hij kan doen, is het generieke regime van de leverancier beoordelen op geschiktheid voor het beoogde gebruik. Het gevolg daarvan is dat de gebruiker erop moet kunnen vertrouwen dat de door de cloudleverancier gepresenteerde informatie over de risico's en beheersmaatregelen beschikbaar, begrijpelijk, toegankelijk en correct is. Daarnaast moet hij erop kunnen vertrouwen dat de maatregelen in de praktijk voldoende effectief zijn. Want als er lacunes zijn of onjuistheden, wordt niet a priori de cloudleverancier maar de afnemer op dat falen aangesproken door respectievelijk de gebruikers, aandeelhouders en toezichthouders. Terwijl de gebruiker geen middelen in handen heeft om rechtstreeks in te kunnen grijpen als zich problemen voordoen.

Deze spanning tussen het businessmodel van clouddiensten en de behoefte van de verschillende belanghebbenden (afnemer, gebruiker, aandeel- en toezichthouders) wordt extra urgent door de maatschappelijke aandacht voor de bescherming van gegevens en weerbaarheid van onlinediensten. De betrouwbaarheid van de cloud wordt daarmee ook een maatschappelijke verantwoordelijkheid.

Tenslotte: leveranciers spelen een belangrijke rol in de betrouwbaarheid en veiligheid van clouddiensten. Dat neemt niet weg dat ook gebruikers een verantwoordelijkheid hebben. Zij moeten bijvoorbeeld vaststellen dat de clouddienst geschikt is voor het doel waarvoor deze gebruikt gaat worden.

Samenvattend: de toenemende afhankelijkheid van de cloud door de samenleving versterkt de spanning tussen het verdienmodel van de cloud (aan veel partijen een vrijwel dezelfde dienst bieden, kleine marges) en vertrouwen: de behoefte aan zekerheid dat een dienst voldoet aan eisen van gebruikers en samenleving.

De constatering van de deelnemers aan de Online Trust Coalitie is dat de gebruikers niet op een eenvoudige manier hun eisen kunnen stellen en hun vragen beantwoord krijgen. De leverancier heeft

onvoldoende mogelijkheden om op een eenvoudige manier die vragen te beantwoorden en bewijzen van betrouwbaarheid te laten zien.

In de volgende hoofdstukken gaan we in op de vraag wat vertrouwen en betrouwbaarheid is.

De aard van vertrouwen bij clouddiensten

Zoals toegelicht in de vorige paragrafen hebben we met het gebruik van clouddiensten het beheer van onze informatiesystemen de-facto grootschalig uitbesteed. We verwerken onze gegevens op plekken waarvan we vaak niet weten waar die zich fysiek bevinden en wie daar allemaal bij kunnen komen. We delen de IT-infrastructuur met potentieel miljoenen anderen. Onze persoonsgegevens worden verwerkt en opgeslagen door partijen waar we soms geen weet van hebben. Dat doen we, vanuit het vertrouwen dat alle betrokken partijen zich houden aan wet- en regelgeving en zich vastleggen op specifieke afspraken. Zonder dat vertrouwen, zou het gebruik van clouddiensten in onze digitale samenleving niet zo groot zijn als nu het geval is. Daarmee is vertrouwen cruciaal voor het gebruik van clouddiensten, nu en in de toekomst. Voor leveranciers van clouddiensten is het dan ook van belang om aan te kunnen tonen dat hun diensten te vertrouwen zijn. Voor gebruikers is het van belang dat zij dat bewijs eenvoudig kunnen verkrijgen en dat het begrijpelijk is.

Om de afnemer en aanbieder van een clouddienst te faciliteren bij het tot stand brengen van vertrouwen maken we in dit whitepaper een onderscheid tussen vertrouwen, betrouwbaarheid, zekerheid.

Doel waar dit whitepaper aan bijdraagt is vertrouwen in clouddiensten.

---

*Een afnemer **vertrouwt** een clouddienst als de afnemer voldoende zekerheid heeft om aan te nemen dat de clouddienst betrouwbaar is[1].*

Maar hoe krijg je vertrouwen in clouddiensten? De basis voor vertrouwen is een betrouwbare dienst: een dienst die voldoet aan beloften, gemaakte afspraken en wet- en regelgeving. Vervolgens wordt vertrouwen versterkt als hierover zekerheid kan worden geboden. Een belangrijk aspect van het geven van zekerheid is communicatie.

1 **Vertrouwen** is “met zekerheid hopen”. https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/VERTROUWEN. Geraadpleegd 10.11.2020

2. Betrouwbaarheid

Door gebruik te maken van clouddiensten vertrouwen wij hen de verwerking van onze persoonlijke, medische, financiële en bedrijfsgegevens en intellectuele eigendommen toe, in de verwachting dat zij hier op een verantwoorde wijze mee om gaan.

Clouddiensten zijn essentieel voor ons dagelijks functioneren en voor digitale innovaties. Zij kunnen dan ook alleen een belangrijke rol in de samenleving vervullen als zij beveiligd en betrouwbaar zijn en voldoen aan wet- en regelgeving.

Generiek of specifiek?

Op het eerste gezicht lijkt iedere situatie uniek te zijn, en is geen bedrijf hetzelfde. Maar bij nadere bestudering blijkt dat er toch generieke eisen of criteria zijn die betrekking hebben op de betrouwbaarheid van in principe iedere clouddienst. Het gaat dan bijvoorbeeld om juistheid, volledigheid, vertrouwelijkheid, tijdigheid en beveiliging. Voor specifieke toepassingsgebieden en gebruikers zullen er aanvullende eisen of criteria geformuleerd kunnen worden waarmee de geschiktheid van de clouddienst voor die specifieke toepassingsgebieden of doelgroep kan worden aangetoond. Als leveranciers dit proactief aantonen, dan hoeven gebruikers geen of weinig aanvullende eisen te stellen.

Verantwoordingsinformatie

De gebruikers van een clouddienst moeten vertrouwen hebben in de betrouwbaarheid van de clouddienst. Dit is een belangrijke basisvoorwaarde voor gebruik of adoptie van clouddiensten. In veel gevallen, met name bij particulier gebruik, wordt dit vertrouwen gebaseerd op de reputatie van de leverancier, ervaringen uit het verleden en commerciële uitingen.

---

*Een clouddienst is **betrouwbaar** als deze voldoet aan de afspraken die zijn gemaakt tussen aanbieder en afnemer, én aan algemene en specifieke kwaliteitseisen voor een clouddienst, én geschikt is om te voldoen aan relevante wet- en regelgeving.*

Voor andere, vaak professionele toepassingen, wordt zekerheid verlangd. Dit geldt ook voor aspecten die nadrukkelijk een maatschappelijk belang hebben en waarop toezicht gehouden wordt. Zoals dat bijvoorbeeld bij de bescherming van persoonsgegevens het geval is. Nu is zekerheid een relatief begrip. Absolute zekerheid over de betrouwbaarheid van clouddiensten bestaat niet. Wel kan een assurance-dienst tot op zekere hoogte zekerheid geven. Dit is van belang als gebruikers verantwoording moeten afleggen over de betrouwbaarheid van de door hen gebruikte clouddienst. Dit is bijvoorbeeld het geval als een accountant of auditor bij controle van de jaarrekening hierover navraag doet. Om zekerheid hierover te verschaffen, levert de leverancier verantwoordingsinformatie aan. Dit kan vergezeld gaan van een bevestiging van een derde partij, zoals een keurmerkinstelling die een certificaat of keurmerk heeft afgegeven.

Aansprakelijkheid

Een aspect dat in het verlengde ligt van zekerheid is aansprakelijkheid. Wat gebeurt er, als de geboden zekerheden in de praktijk toch niet zo zeker blijken te zijn? Wie draait op voor schade?

Deze materie is een gebruikelijk kat- en muisspel tussen aanbieders en gebruikers, en zeker niet uniek voor clouddiensten. Hoe groter het verschil is in macht en omvang tussen partijen, hoe gemakkelijker het voor de grotere partij zal zijn om de gevolgen van het niet nakomen van zekerheden bij de kleinere partij te leggen. Voor het aspect privacy, en daarmee dus ook voor informatieveiligheid en beschikbaarheid van gegevens, legt de wetgever de verantwoordelijkheid voor een belangrijk deel bij de top van de keten: de afnemer van een dienst. Toch dragen verwerkers binnen de keten ook verantwoordelijkheid.

De cloud-industrie beschikt nog niet over gestandaardiseerde of wettelijke modellen voor keten-aansprakelijkheid. Ook zijn er nog geen standaardmodellen voor verdeling van verantwoordelijkheden. Op het gebied van verzekeringen om schade te dekken bij crises, is nog weinig ontwikkeling.

3. Zekerheid

Vertrouwen in een clouddienst vereist als eerste betrouwbaarheid, zoals in het vorige hoofdstuk uiteengezet. Dit hoofdstuk gaat in op het tweede belangrijke aspect van vertrouwen: zekerheid. Hoe kunnen leveranciers van clouddiensten zekerheid bieden dat een clouddienst daadwerkelijk aan de (kwaliteits)eisen van afnemer en wetgever voldoet.

*Er is sprake van **zekerheid** over de mate van betrouwbaarheid van een clouddienst, als bij de afnemer en andere belanghebbenden de overtuiging bestaat dat de maatregelen die betrouwbaarheid waarborgen naar de huidige stand van de techniek effectief zijn.*

Bij het verkrijgen van zekerheid over de betrouwbaarheid zijn vier methoden te onderscheiden: assurance, certificering, zelfverklaring en onderzoek door de gebruiker zelf. Aan het einde van het hoofdstuk wordt een overzicht gegeven van de verschillen tussen de manier waarop zekerheid wordt gegeven.

Assurance

Een term die heel vaak gebruikt wordt als het gaat over het verschaffen van zekerheid, is het begrip ‘assurance’. Over dit begrip bestaat veel verwarring. Heel vaak wordt assurance in verband gebracht met ’insurance’ wat ‘verzekeren’ betekent. In de context van clouddiensten gaat het over het bieden van zekerheid dat een clouddienst aan de gestelde eisen voldoet. Dit wordt vastgesteld door een onafhankelijke deskundige derde partij, vaak aangeduid als ‘auditor’. Op basis van onderzoek (audit of conformiteitsonderzoek) stelt dat auditor vast dat voldaan wordt aan de gestelde eisen, die in dat geval ‘criteria’ worden genoemd.

In de financiële wereld is ‘assurance’ een bekend begrip. Accountants en auditors die de jaarrekening of interne beheersingsprocessen controleren, maken gebruik van wereldwijd erkende assurance-standaarden (International Standards on Assurance Engagements, ISAE). Assurance-rapporten worden vervolgens gebruikt om verantwoording af te leggen over de interne beheersing in een bepaalde periode. Bekende vormen van assurance-rapporten zijn ISAE 3000, ISAE 3402, SOC 1 en SOC 2. Veel grote clouddienstverleners beschikken over dergelijke rapporten. Assurance-rapporten bevatten gedetailleerde informatie over het gehanteerde normenkader (de criteria), de wijze van toetsen en de geconstateerde bevindingen. De rapporten zijn bestemd voor een beperkte doelgroep en mogen niet verder worden verspreid.

In de praktijk wordt de assurance-audit ook wel aangeduid als ‘third party onderzoek’.

ISO-certificering

Een andere manier om zekerheid te verschaffen aan gebruikers is door middel van een ISO-certificaat. ISO is de Internationale Organisatie voor Standaardisatie, die wereldwijd normen en standaarden vaststelt voor bedrijven en organisaties. In Nederland beheert het Nederlands Normalisatie Instituut NEN de wereldwijde standaarden. ISO omvat een zeer groot aantal standaarden voor een zeer breed scala aan managementsystemen, producten, processen en diensten. Op dit moment zijn er meer dan 23.000 standaarden. Dat maakt ISO wel erg onoverzichtelijk. De meest bekende ISO standaard, is ISO 9001 voor kwaliteitsmanagement. Maar ook voor clouddiensten zijn er relevante standaarden, zoals

ISO 27001, 27002, 27017 en 27018 (Informatiebeveiliging), ISO 27701 (privacy informatiemanagement) en ISO 19086 (Informatietechnologie, cloudcomputing en SLA-raamwerk). Deze standaarden hebben overigens alleen betrekking op het managementsysteem van de cloudleverancier en niet op de clouddienst zelf.

ISO is een vorm van certificering wat betekent dat door middel van een certificaat tot uitdrukking wordt gebracht dat de clouddienst of de aanbieder van de dienst (afhankelijk van het type certificaat) voldoet aan de relevante (openbare) standaard. De gebruiker krijgt verder geen detailinformatie over de geconstateerde bevindingen. In de praktijk wordt de ISO-audit ook wel aangeduid als 'third party onderzoek'.

Zelf-evaluatie (self-assessment)

Onderzoek door derden heeft voor- en nadelen. Belangrijkste voordeel is, dat door de onafhankelijkheid en deskundigheid van de auditor er in de regel meer vertrouwen ontleend wordt aan bijvoorbeeld een certificaat. Belangrijkste nadeel zijn de doorgaans hoge kosten en lange doorlooptijden. Met name voor eenvoudige en niet kritische diensten wordt er daarom vaak getracht door middel van zelf-evaluatie invulling te geven aan de vraag naar zekerheid. Dit heeft echter alleen zin als de leverancier gebruikmaakt van geaccepteerde methoden om de conformiteit vast te stellen, en volledige transparantie geeft over de bevindingen. Ook in juridische procedures zal een zelf-evaluatie minder waarde hebben dan een door derden uitgevoerde assurance-audit. Na een zelf-evaluatie verklaart de leverancier van clouddiensten dat deze voldoen aan bepaalde criteria, met behulp van een 'Statement of Conformity'.

Onderzoek door gebruikers

Sommige wet- en regelgeving en toezichthouders eisen dat gebruikers van clouddiensten in bepaalde sectoren zelf onderzoek doen bij hun leverancier naar de betrouwbaarheid van de aangeboden diensten. Een voorbeeld hiervan is De Nederlandsche Bank. Dit kan een grote belasting vormen voor zowel de gebruiker als de leverancier. Daarom wordt door banken in de regel samengewerkt en door middel van een gezamenlijke audit invulling gegeven aan deze eis.

Kiezen van de geschikte methode

De genoemde methoden om zekerheid te krijgen over de betrouwbaarheid van een dienst verschillen op een aantal punten:

1. **Wie doet het onderzoek:** een onafhankelijke deskundige (assurance, ISO-certificering) of de aanbieder zelf (zelf-evaluatie), of de gebruiker? Gezien de complexiteit van clouddiensten vergt onderzoek vaak de samenwerking van onderzoekers met uiteenlopende kennis en ervaring. Inzage in de samenstelling en ervaring van het onderzoeksteam is daarom belangrijk om de onderzoeksresultaten op waarde te kunnen schatten.
2. **Wat wordt onderzocht:** is het de organisatie van de dienstverlener die wordt onderzocht (ISO-certificering) of de aangeboden dienst (Assurance). Bij een dienst zijn vaak verschillende dienstverleners en daarmee organisaties betrokken.
3. Wat is het **normenkader** (de criteria) waar de dienstverlener of dienst aan is getoetst? Neemt dat normenkader de wensen en eisen van de gebruiker en afnemer van de dienst mee of is er sprake van een generiek normenkader of een normenkader dat de aanbieder zelf heeft opgesteld? Wordt in het normenkader wet- en regelgeving meegenomen? Zijn algemene kwaliteitscriteria goed meegenomen?
4. Wordt **de effectiviteit (werking)** onderzocht van de technische en organisatorische maatregelen of wordt alleen het bestaan onderzocht?
5. Hebben de **conclusies** van het onderzoek alleen betrekking op het verleden of doet het ook uitspraken over de toekomst?

6. Is er een rapportage die inzage geeft in de **risicoafwegingen** van een aanbieder bij het voldoen aan het normenkader (assurance) of is er sprake van een oordeel (bijvoorbeeld ja of nee) over betrouwbaarheid (certificering).

Eén van de actiepunten van de OTC is dat afnemers van diensten veel meer handreiking moeten krijgen welke zekerheden ze aan de verschillende conformity assessments kunnen ontlenen.

Een complicerende factor is, dat gebruikers van clouddiensten, maar ook andere belanghebbenden zoals toezichthouders, moeilijk op een uniforme manier aan kunnen geven welk bewijs zij nodig hebben om te kunnen vaststellen of een de clouddienst voldoende betrouwbaar is. Eén van de voorgenomen acties van de OTC is de methoden om zekerheid te bieden te harmoniseren en een handreiking te bieden.

Voor particuliere gebruikers is het vaak voldoende om algemene informatie te ontvangen van de leverancier van clouddiensten over betrouwbaarheid en de zekerheid die wordt geboden. In combinatie met publiekelijk beschikbare informatie over de reputatie van de leverancier is dat afdoende. Zakelijke gebruikers hebben behoefte aan informatie over de kwaliteit van de processen en systemen van de leverancier, gedetailleerde verantwoordingsinformatie en een door een derde partij verstrekte zekerheidsgarantie zoals een keurmerk.

Zakelijke gebruikers willen vaak specifieke informatie hebben volgens een door hen gekozen methode, waardoor de leverancier zekerheid op maat moet leveren. Gevolg daarvan is dat de leverancier ook op maat moet communiceren, gericht op die ene gebruiker met specifieke eisen aangaande de betrouwbaarheid van zijn clouddienst.

Een van de actiepunten van de OTC is dat leveranciers in staat moeten zijn om hun rapportages en communicatie over betrouwbaarheid op een schaalbare manier in te richten. Dat sluit aan bij hun corebusiness: een keer inrichten en vervolgens aan iedereen leveren. Standaardisatie biedt uitkomst. Aan de hand van standaarden kan op voorhand op verschillende niveaus zekerheid worden geboden en kan hierop de communicatie worden ingericht. Hiermee kan het bieden van zekerheid door een leverancier net zo standaard worden als het leveren van de clouddienst zelf. Voor de gebruikers wordt het krijgen van zekerheid net zo eenvoudig als het afnemen van de clouddienst.

Het bieden van zekerheid op meerdere niveaus wordt op deze manier onderdeel van de basisdienstverlening. Leveranciers kunnen de kosten dan ook opnemen in de vergoeding die zij vragen voor een clouddienst. Hoe meer zekerheid, hoe hoger de vergoeding is. Iedere gebruiker betaalt mee aan de zekerheid dat de clouddienst betrouwbaar is. Door dit collectief te regelen, blijft de kostenvergoeding per gebruiker beperkt.

De vraag naar betrouwbaarheid en zekerheid van een clouddienst kan niet beantwoord worden zonder ook naar de verantwoordelijkheden te kijken die afnemers hebben als zij gebruikmaken van clouddiensten. Ook daarover is communicatie nodig en wellicht moet ook de afnemer van de dienst onafhankelijk onderzoek laten uitvoeren of zij die verantwoordelijkheid op de juiste manier nemen; of de techniek en eigen organisatie op de juiste manier zijn ingericht.

4. Praktijkcasus ziekenhuis

Een ziekenhuis wil haar patiëntgegevens opslaan in de cloud. Daar gelden stringente beveiligingseisen voor. Zo geeft NEN 7510 richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening.

Een leverancier van clouddiensten moet voor veel klanten aantoonbaar voldoen aan ISO 27001 en ISO 27002. Leveranciers beschikken vaak al over diverse certificeringen zoals NEN 7510.

Dit ziekenhuis verkeert echter in bijzondere omstandigheden: het behandelt kwetsbare groepen en bijzondere individuele gevallen.

Het probleem is dat het ziekenhuis in de huidige situatie zelf moet vaststellen of de certificeringen van de leverancier afdoende zijn in deze bijzondere situatie. Het vergt veel kennis om vast te stellen in hoeverre die certificeringen zekerheid geven over de algehele betrouwbaarheid van de clouddienst en over de effectiviteit van de extra genomen maatregelen.

In deze casus ontdekt het ziekenhuis dat deze eisen niet in voldoende mate worden afgedekt door de generieke kwaliteitseisen en wet- en regelgeving voor de zorg.

Het ziekenhuis moet vervolgens aan de leverancier duidelijk maken welke extra eisen er aan de clouddienst gesteld worden. De (potentiële) leverancier moet een analyse maken en aantonen hoe de dienst aan deze extra eisen voldoet, en het ziekenhuis moet op zijn beurt deze analyse interpreteren en concluderen of de clouddienst wel of niet voldoet. Het is bovendien de vraag of de extra maatregelen die de leverancier treft effectief zijn. Waar het hier om gaat, is dat het ziekenhuis wil weten of het vertrouwen kan hebben in de betreffende clouddienst.

De OTC is van plan ondersteunende middelen te ontwikkelen die de gebruiker helpen bij het formuleren van eisen aan de clouddienst en bij het analyseren van de door de leverancier aangeleverde verantwoordingsinformatie. De OTC is bovendien van plan ondersteunende middelen te ontwikkelen op het gebied van zekerheid, zodat leveranciers zekerheid aan gebruikers kunnen geven.

5. Acties voor betrouwbare en veilige clouddiensten

Clouddiensten staan niet op zichzelf. Zij bestaan uit ketens van diensten die vaak door verschillende aanbieders worden geleverd. Een aanbieder van een SaaS-dienst (software die in de cloud beschikbaar is), zal bijna altijd gebruikmaken van hosting- en platformdiensten van derde partijen. Dit wordt vaak nog aangevuld met managed services (uitbesteding van onderhoud aan Saas-oplossingen). Deze diensten moeten op een goede manier met elkaar samenwerken om uiteindelijk een betrouwbare en veilige SaaS-dienst te kunnen leveren. Hiervoor is het nodig dat de componenten van de clouddienstverlening grotendeels gestandaardiseerd en geharmoniseerd zijn. Dat geldt ook voor de betrouwbaarheidseisen die aan een clouddienst gesteld worden en het te leveren bewijs dat de clouddienst betrouwbaar is.

In dit kader is de ambitie van de OTC: “het verkennen, ontwikkelen en beschikbaar maken van meer eenduidige, efficiëntere en laagdrempelige methoden waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn en dat die het validatieproces van de gebruikers ondersteunen”[2].

De OTC wil op de belangrijkste knelpunten actie ondernemen. Hieronder worden de knelpunten en de bijbehorende acties vermeld.

Actiepunt 1: vergelijkbaarheid van certificeringen en normenkaders voor betrouwbaarheid en het geven van zekerheid

In de hoofdstukken over betrouwbaarheid en zekerheid blijkt dat een belangrijk knelpunt met betrekking tot de betrouwbaarheid van clouddiensten de veelheid aan eisen is, die gesteld worden ten aan zien van bijvoorbeeld informatietechnologie, cybersecurity en privacy. Bij het formuleren van deze eisen wordt nauwelijks samengewerkt tussen partijen, maar toch blijkt uit een vergelijking van normenkaders van verschillende certificeringsschema’s dat de gehanteerde normen voor een groot deel overlappen.

De Online Trust Coalitie is daarom van plan een analyse uit te voeren van bestaande certificeringen en normenkaders voor betrouwbare clouddiensten. We willen een algemeen toepasbaar normenkader vaststellen, zodat standaardisatie en harmonisatie van clouddiensten mogelijk wordt. Vervolgens zijn gestandaardiseerde aanvullingen mogelijk met extra eisen voor specifieke toepassing in bepaalde bedrijfssectoren.

De bedoeling is de zekerheidsniveaus voor clouddiensten modulair op te bouwen, zodat per niveau snel een eenvoudig aan de hand van gestandaardiseerde modules aangetoond kan worden hoe betrouwbaar en veilig de clouddienst is. Hierdoor hoeven leveranciers van clouddiensten niet meer voor iedere gebruiker afzonderlijk op maat betrouwbaarheid en zekerheid te bieden. De betrouwbaarheid van clouddiensten wordt op deze manier inzichtelijk, waardoor gebruikers bewust kunnen afwegen voor welke clouddienst zij kiezen. Bijkomend voordeel is dat aan deze werkwijze minder kosten zijn verbonden.

Actiepunt 2: Keuzehulp voor gebruikers

Gebruikers van clouddiensten worden afhankelijk van hun leverancier. Vaak is het voor gebruikers onduidelijk welke eisen zij moeten stellen en aan welke eisen een clouddienst voldoet. Zie het hoofdstuk over betrouwbaarheid. Een duidelijk voorbeeld hiervan doet zich voor bij beëindiging van de clouddienst. Als een IT-toepassing in eigen beheer wordt beheerd, zullen na beëindiging van de levenscyclus de toepassing en de daarbinnen verwerkte en opgeslagen gegevens in de regel nog voor de gebruiker beschikbaar zijn. Bij beëindiging van een clouddienst is dat geen vanzelfsprekendheid.

2 https://ecp.nl/wp-content/uploads/2020/09/Online-Trust-Coalitie-Manifest.pdf

Er zullen met de leverancier afspraken gemaakt moeten worden over de voorwaarden waaronder gegevens beschikbaar blijven. Veel leveranciers hebben hier standaardoplossingen voor. Een ander voorbeeld van afhankelijkheid doet zich voor als een van de leveranciers in de keten van clouddiensten stopt met zijn dienstverlening. De maatregelen die de gebruiker dan moet nemen, zijn wezenlijk anders dan bij IT-middelen die in eigen beheer zijn. Een laatste voorbeeld van afhankelijkheid is de benodigde medewerking van de leverancier bij het overstappen naar een andere clouddienst. Als hij niet wil meewerken, dan is het risico op een 'vendor lock-in' aanwezig.

De Online Trust Coalitie gaat in samenspraak met leveranciers, gebruikers en brancheorganisaties een toelichting opstellen waarin wordt aangegeven welke zaken van belang zijn bij de keuze voor een clouddienst en -leverancier.

Actiepunt 3: Spelregels voor de cloud

Voor potentiële gebruikers van clouddiensten is het van belang dat leveranciers toezeggen dat hun dienstverlening betrouwbaar is, dat de communicatie daarover correct is en dat zij meewerken aan het verschaffen van de gewenste mate van zekerheid hierover. Tegelijkertijd moeten de leveranciers ervan uit kunnen gaan dat gebruikers de dienst gebruiken op een manier die geen afbreuk doet aan de inspanningen van de leverancier om een betrouwbare dienstverlening te waarborgen. De vorige hoofdstukken belichtten een handreiking voor het samenspel tussen de aanbieder en afnemer van clouddiensten op dit moment ontbreekt.

De Online Trust Coalitie zal in samenspraak met leveranciers, brancheorganisaties en vertegenwoordigers van gebruikers werken aan de totstandkoming van 'spelregels voor de cloud'. Hierbij zal nadrukkelijk aansluiting worden gezocht bij de gedragscode (Cloud Rule Book) voor GAIA-X.

Actiepunt 4: Monitoring

Er is een grote diversiteit aan oplossingen die zekerheid bieden over de betrouwbaarheid en veiligheid van een clouddienst. Kenmerk van al deze oplossingen is dat naar het verleden wordt gekeken. Bovendien wordt er wel naar de organisatie en de interne beheersprocedures rondom technologie gekeken, maar slechts beperkt naar de technologie zelf.

Een aantal OTC-deelnemers zal onderzoek doen naar mogelijke innovatieve methoden voor het aantonen van betrouwbaarheid en veiligheid van clouddiensten. Denk bijvoorbeeld aan het inzetten van technologie voor het uitvoeren van beoordelingen en audits, en het real-time monitoren van de betrouwbare werking van clouddiensten.

Actiepunt 5: Standaardisatie van verantwoordingsinformatie

Zoals in het hoofdstuk over zekerheid werd geconcludeerd is een van de belangrijkste knelpunten rond het geven van zekerheid door de aanbieder van een clouddienst aan de gebruiker, het ontbreken van geharmoniseerde communicatie over de betrouwbaarheid van clouddiensten en het geven van zekerheid. Verschillende vormen van wet- en regelgeving vergen verschillende vormen van conformiteitsonderzoeken, verantwoordingsrapporten, certificaten en dergelijke. Iedere vorm heeft zijn eigen protocollen en manier van uitwerken. Voor leveranciers – en met name voor het MKB – is het zeer tijdrovend en kostbaar om verantwoording af te leggen via al deze verschillende vormen. Harmonisatie is dan ook gewenst.

De Online Trust Coalitie wil de diversiteit in rapportagevormen over betrouwbaarheid en veiligheid van clouddiensten terugbrengen tot gestandaardiseerde verantwoordingsinformatie voor gebruikers en auditors van toezichthouders. De standaarden voor deze rapportages worden gebaseerd bestaande wet- en regelgeving, en zullen worden afgestemd met toezichthouders en andere relevante betrokkenen

Actiepunt 6: GAIA-X

Een Duits-Frans initiatief wil binnen Europa een Europese cloud tot stand brengen: een federatieve cloud, waarin aanbieders samenwerken, die gebaseerd is op Europese wet- en regelgeving en die wat functionaliteit betreft kan concurreren met de grote wereldwijde cloud-aanbieders. Dit initiatief heet GAIA-X en een van de belangrijke doelen van GAIA-X is het regelen van de governance van deze federatieve Europese cloud. In Brussel is de GAIA-X Foundation opgericht. Partijenkunnen hieraan deelnemen om vorm te geven aan de governance van de toekomstige Europese cloud.

De Online Trust Coalitie is van plan deel te nemen aan de GAIA-X Foundation, en specifiek zitting te nemen in de werkgroep die de ‘assurance’ (betrouwbaarheid en zekerheid) van clouddiensten gaat regelen.


MAX ST BILITY
VALL TTA

WILT U CONTACT OF MEER INFORMATIE?

info@onlinetrustcoalitie.nl
www.onlinetrustcoalitie.nl