Stichting Continuïteit
internetdiensten

Continuïteit in de cloud

Clouddiensten zijn tegenwoordig niet meer weg te denken uit de online wereld. Van een simpele e-maildienst tot volledige facturatie- of accountantprogramma's, ondernemingen maken gebruik van allerlei clouddiensten. Hiermee ontstaat een grote afhankelijkheid en dat brengt risico's met zich mee. Steeds vaker zal de vraag gesteld worden 'Wat als mijn clouddienstverlener failliet gaat?' of 'Hoe kan ik er voor zorgen dat de dienst gecontinueerd wordt?'. Deze vragen leiden steeds vaker tot een risicoanalyse ten aanzien van de weerbaarheid van clouddiensten. Met back-up faciliteiten en exit-regelingen kunnen bepaalde zaken geregeld worden. Om écht continuïteit te waarborgen is een omvangrijkere oplossing nodig. Cloudrecht en de Stichting Continuïteit Internetdiensten (SCI) bieden die oplossing.

Continuïteit

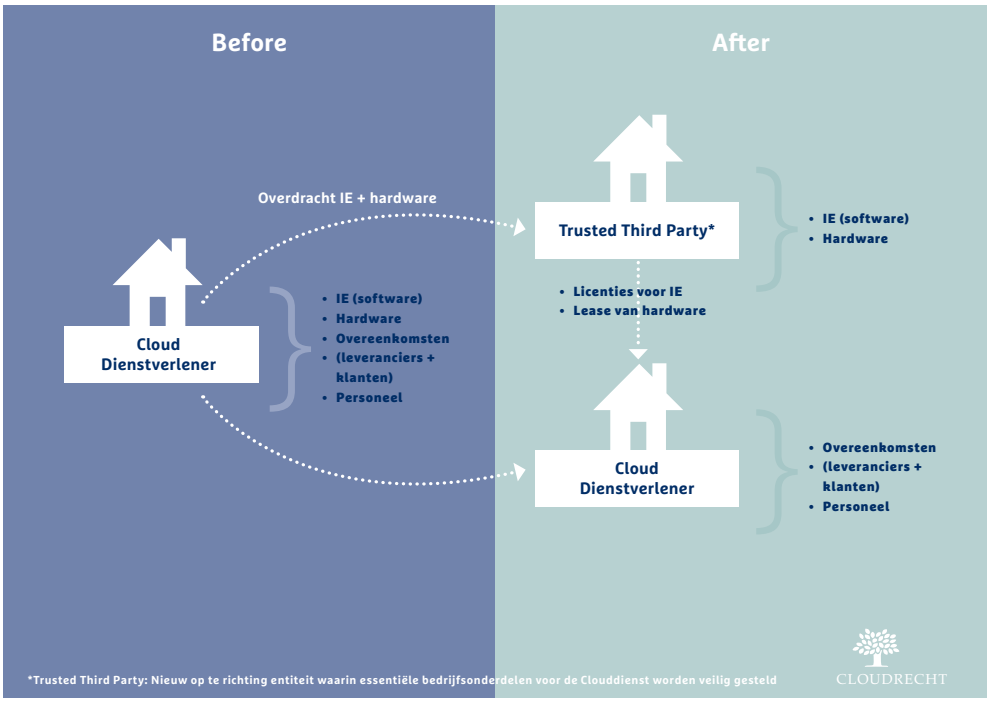
De beschikbaarheid van een clouddienst is essentieel. Voor zowel leverancier als afnemer is het van belang dat de continuïteit van de dienst gewaarborgd is. Verschillende bedreigingen kunnen ondervangen worden met een slimme en doortastende oplossing. Door technische, financiële en juridische maatregelen te nemen wordt zekerheid geboden voor alle partijen. Het doel is het bieden van een volledige oplossing die bestand is tegen bedreigingen zoals een faillissement of een overname van de leverancier. Of het nu gaat om een eenvoudige webapplicatie of een volledig IT-landschap, de oplossing is altijd binnen handbereik.

Voorheen werd de oplossing gevonden in escrow-regelingen. Deze hebben als doel de broncode van de software veilig te stellen voor de afnemer. De meeste escrow-overeenkomsten gaan uit van een afspraak tussen de leverancier, een onafhankelijke derde: de escrow-agent (soms een notaris) en de afnemer. Indien de leverancier dan failliet wordt verklaard, stelt de escrow-agent de broncode ter beschikking aan de afnemer. Deze regeling is om meerdere redenen niet toereikend. Allereerst is een clouddienst meer dan alleen de broncode. De hosting, de data en aanverwante service onderscheiden een clouddienst van reguliere software en die zaken worden niet veilig gesteld door een broncode-escrow. Daarbij kan uit het in 2006 gewezen Nebula-arrest van de Hoge Raad de conclusie getrokken worden dat de curator als rechthebbende van de software het gebruik daarvan niet hoeft te dulden.

Om écht continuïteit te kunnen bieden is er een completere oplossing nodig. Die oplossing heeft betrekking op alle onderdelen van de clouddienst. De meeste clouddiensten bestaan grofweg uit (i) intellectueel eigendom, zowel eigen software als licenties van derden, (ii) hardware, zoals eigen of gehuurde servers, (iii) personeel, voor onderhoud aan de software en een helpdesk en (iv) overige overeenkomsten met leveranciers en klanten. Om een clouddienst weerbaar te maken tegen bedreigingen zoals een faillissement dient er gekeken te worden naar al deze 'assets'.

De oplossing

De crux van de oplossing is gelegen in het buiten de macht van de curator brengen van de assets. De bovengenoemde bedrijfsonderdelen worden daarvoor in een aparte constructie ondergebracht. Daarbij wordt gebruik gemaakt van een 'trusted third party' (TTP) in de vorm van een stichting of een besloten vennootschap. Hiervoor kan een nieuwe rechtspersoon worden opgericht maar er kan ook gebruikgemaakt worden van reeds bestaande entiteiten zoals de holding. De intellectuele eigendomsrechten en de benodigde hardware wordt door de werkmaatschappij van de clouddienstverlener overgedragen aan de TTP. Het personeel en de overeenkomsten met leveranciers en klanten zullen in eerste instantie bij de werkmaatschappij blijven. Er zal dus een splitsing plaatsvinden tussen de assets vanuit de werkmaatschappij.

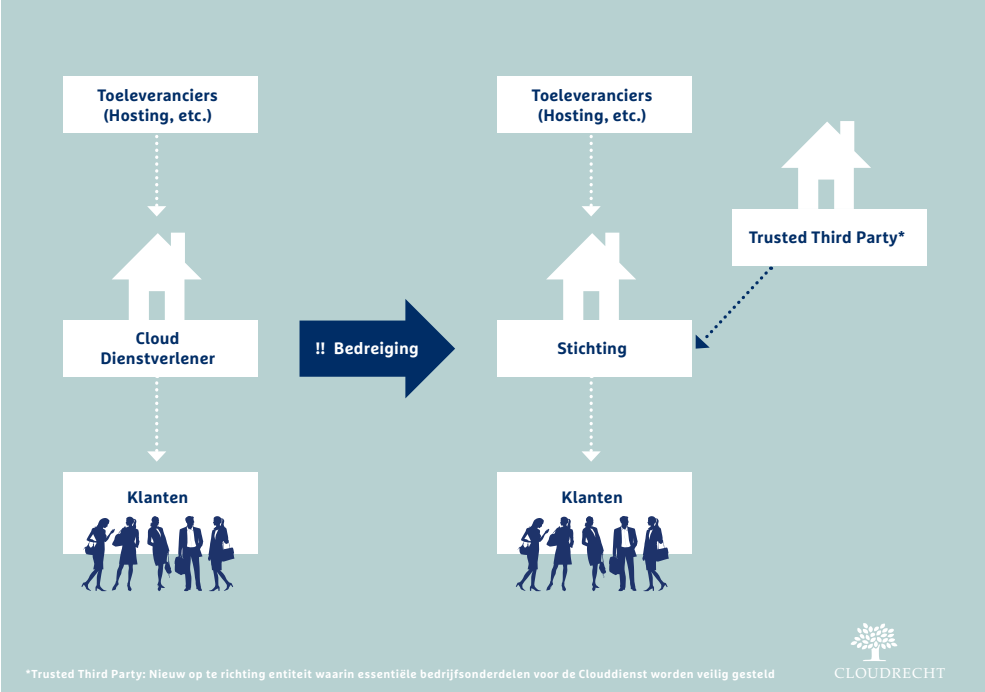


De TTP fungeert in de nieuwe constructie als een veilige haven die zolang er geen bedreigingen van de continuïteit optreden niet per se een actieve functie heeft. De daar geplaatste assets worden via licenties en eventuele lease van hardware aan de werkmaatschappij ter beschikking gesteld. Zodoende verandert er feitelijk weinig in de bedrijfsvoering van de clouddienstverlener en zijn de assets beschermd tegen bedreigingen van de werkmaatschappij.

Naast de TTP moet er een partij zijn die de clouddienst kan leveren in het geval dat er een bedreiging intreedt. De afnemers van de clouddienst kunnen dan bij deze partij aankloppen ten behoeve van de continuïteit van de dienst. Deze partij dient onafhankelijk van de werkmaatschappij te zijn, bij voorkeur een niet commerciële entiteit zoals een stichting. Hiervoor is ook de Stichting Continuïteit Internetdiensten (SCI) in het leven geroepen. Lees meer onder het kopje “Over de Stichting Continuïteit Internetdiensten”.

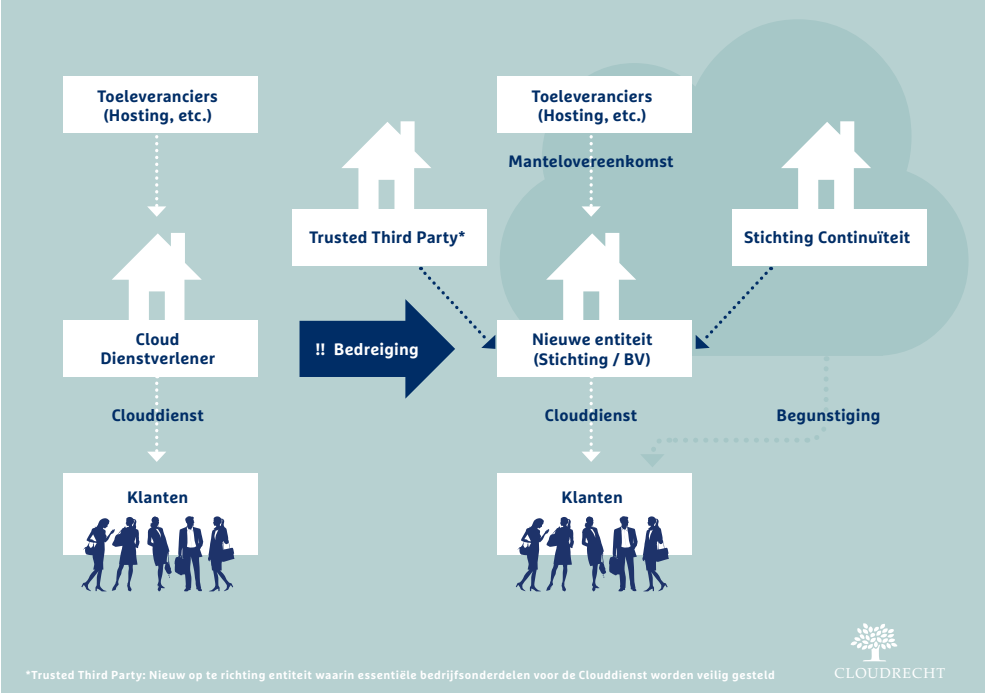
De toeleveranciers (hoster/datacenter/softwareleverancier) moeten hun diensten na het intreden van een bedreiging gaan leveren aan de dan actief wordende stichting. Om dit te bewerkstelligen dienen er overeenkomsten te worden gesloten met de toeleveranciers door de stichting.

Eenvoudig weergegeven ziet de situatie voor en na de bedreiging er als volgt uit:



Over de Stichting Continuïteit Internetdiensten

Uiteraard komt er meer bij kijken dan hierboven weergegeven. Afhankelijk van de soort clouddienst en de wensen van de afnemer kan de constructie complexer of simpeler worden. Vaak is er behoefte aan een onafhankelijke partij die de bedreigingen monitort en kan ingrijpen wanneer nodig. Hiervoor is de Stichting Continuïteit Internetdiensten (SCI) in het leven geroepen. Deze door ICTRecht opgerichte stichting zal in samenspraak met de clouddienstverlener contractuele afspraken maken met de werkmaatschappij die de dienst levert en de toeleveranciers in de vorm van een mantelovereenkomst. Hierin worden de precieze omvang van de dienst, de bedreigingen van de continuïteit, financiële afspraken en de periode waarvoor continuïteit gewenst is vastgesteld. Om de afnemers deelgenoot van de constructie te maken wordt er een begunstiging afgegeven. Dit zal in de vorm van een certificaat gebeuren waardoor afnemers hun recht op continuïteit kunnen inroepen. De SCI zal middels een jaarlijkse audit en continue monitoring van de bedreigingen voor afnemers de zekerheid bieden die gewenst is. Indien gewenst kan de SCI ook fungeren als TTP.



Werkwijze

De hierboven beschreven oplossing kan voor allerlei soorten clouddiensten worden ontwikkeld. Of het nou gaat om IaaS, PaaS, SaaS of on premise software: door een doortastende en slimme werkwijze is er een manier te vinden om klanten zekerheid te verschaffen. De juristen van Cloudrecht hebben ruime ervaring met verschillende soorten bedrijfsstructuren en houden tevens rekening met fiscale en financiële obstakels. Omdat geen enkele clouddienstverlener hetzelfde is zal het altijd maatwerk zijn. De werkwijze valt in vier fases uiteen:

1. Allereerst nodigen wij de clouddienstverlener of afnemer graag uit voor een oriënterend intakegesprek. Tijdens dit gesprek zal de dienst besproken worden en zal er verdere uitleg gegeven worden over de specifieke mogelijkheden.

2. Dan vindt er een uitgebreide inventarisatie plaats van de voor de dienst essentiële bedrijfsonderdelen. Aan de hand daarvan worden de mogelijke constructies besproken met de clouddienstverlener.

3. Vervolgens zal er een advies opgesteld worden waarin de specifieke constructie wordt beschreven.

4. Tenslotte moet de constructie daadwerkelijk uitgerold worden. Dit zal met name bestaan uit het opstellen van contracten en andere juridische documentatie. Denk hierbij aan de overdracht van IE en hardware en het opstellen van verschillende overeenkomst waaronder de mantelovereenkomst en de oprichtingsakte van de stichting(-en).

Zoals u ziet zullen er om continuïteit te kunnen waarborgen een aantal ingrijpende maatregelen worden genomen. Daarom is het noodzakelijk dat er gedurende het hele proces open en helder gecommuniceerd wordt met de verschillende belanghebbende.