WAARBORGEN CONTINUÏTEIT SAAS-INFORMATIESYSTEMEN

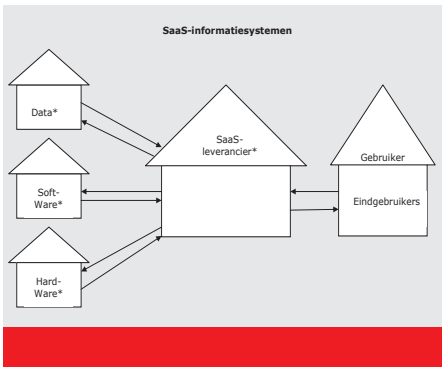
BRONCODE-ESCROW ALLEEN IS NIET VOLDOENDE

J.W. Oordt, IT-jurist bij Software Borg – info@softwareborg.nl

Onlangs is in dit blad vanuit Software Borg een publicatie verschenen waarin wordt gepleit voor een multidisciplinaire aanpak bij het verzorgen van de continuïteit van softwaregebruikers[1]. In dat artikel wordt mede gewezen op het belang van een sterke rechtspositie: de softwaregebruiker moet naast technische, ook de juridische middelen hebben om zijn continuïteit af te dwingen. Betoogd wordt, dat zulks met name geldt voor een broncode-escrowregeling. In dit artikel wordt aan de bespreking van het onderwerp broncode-escrow een vervolg gegeven. De nadruk ligt daarbij op de bespreking van de continuïteitsrisico's van de gebruiker van Software as a Service (SaaS) en met name op de manier waarop die risico's kunnen worden beperkt.

De karakteristieken van SaaS: complexer en meer divers dan on premises oplossingen

Net als dat bij on premises oplossingen het geval is, krijgt de gebruiker van SaaS tegen betaling een recht op het gebruik van de software. Verschil met 'traditionele' licenties is echter, dat de softwaregebruiker ook de toestemming moet hebben om gebruik te maken van de hardware en infrastructuur op afstand, waarmee de toegang tot de software feitelijk aan hem geleverd wordt. De SaaS-gebruiker krijgt geen objectcode-exemplaar, maar met de inloggegevens die zijn leverancier hem heeft verstrekt, kan hij zich via het internet toegang tot de software en de daarmee verwerkte gegevens verschaffen. Het toegankelijk en beschikbaar houden van die toegang gebeurt onder de verantwoordelijkheid van de leverancier, die daarbij vaak derde-partijen inschakelt.



De leverancier stuurt als hoofdaannemer de door hem ingehuurde derde-partijen aan. Een (eenvoudig en bekend) voorbeeld: de leverancier ontwikkelt en onderhoudt de software, maar een hostingprovider verzorgt de beschikbaarheid van de programmatuur en data. De gebruiker heeft niet in beeld door wie en hoe het totale SaaS-systeem functionerend wordt gehouden. De taken rondom het verzorgen van het beheer en de bereikbaarheid van de software en de gegevens kunnen dus onder meerdere, in een keten verbonden, partijen zijn verdeeld. Het wegvallen van één van die partijen kan het gebruik van de software en de toegang tot de data al frustreren. Omwille van de omvang, wordt in dit artikel uitgegaan van de situatie waarin de SaaS-leverancier wegvalt.

> De SaaS-gebruiker is eerstverantwoordelijke voor de continuïteit van zijn eigen bedrijfsvoering

De SaaS-gebruiker: wel verantwoordelijk, maar geen beschikkingsmacht

Van tijd tot tijd is er in de literatuur aandacht voor de risico's die de gebruiker van SaaS loopt. Dan gaat het bijvoorbeeld om vragen als: hoe zit het bijvoorbeeld met de af- en bescherming van de data (risico van onvoldoende informatiebeveiliging)? Worden de gegevens in een overdraagbaar formaat opgeslagen (risico van vendor lock-in)? Welke (overheids)instanties kunnen de op afstand verwerkte persoonsgegevens inzien (risico van niet voldoen aan wettelijke plichten)?

De SaaS-gebruiker is eerstverantwoordelijke voor de continuïteit van zijn eigen bedrijfsvoering. Wanneer die continuïteit mede wordt bepaald door de continuïteit van het onderhoud en gebruik van een computerprogramma en de daarmee verwerkte gegevens, eist zijn verantwoordelijkheid dat hij dat onderhoud en gebruik veiligstelt. De middelen die daarvoor nodig zijn, vallen echter niet onder zijn beschikkingsmacht. Dat is bij on premises software het geval, maar des te meer bij SaaS. In het eerste geval kan de gebruiker immers terugvallen op een werkend objectcode-exemplaar dat hij op eigen hardware heeft geïnstalleerd, terwijl daar bij SaaS niet op kan worden gerekend. Bovendien geeft hij naast de controle over de hardware en de software, de beschikkingsmacht over de data die met de SaaS-applicatie worden verwerkt uit handen.

Dit alles klinkt negatief, maar uiteraard moet niet uit het oog worden verloren dat het buitenshuis laten beheren van

IT hem grote (kosten)voordelen kan bieden [2]. De SaaS-gebruiker geeft met andere woorden meer weg, maar hij mag er wel wat terug voor verwachten. SaaS is dan ook een succesvol businessmodel, al betekent dit dus niet dat de SaaS-gebruiker minder (eind) verantwoordelijkheid heeft voor de continuïteit van zijn informatiesysteem. Bovendien moet hij meer doen om die verantwoordelijkheid goed in te vullen: hij moet meer beschikkingsmacht (terug) zien te krijgen.

Broncode-escrow: oplossing voor continuïteitsrisico's SaaS-gebruiker?

Het voldoen aan de verantwoordelijkheid voor het verzorgen van de continuïteit van bedrijfskritische software, is voor de softwaregebruiker zonder medewerking van zijn leverancier niet eenvoudig. Die medewerking kan tot uiting komen doordat de leverancier kiest voor het opzetten van een broncode-escrowregeling, waarbij de softwaregebruiker in het geval van een calamiteit toegang krijgt tot de broncode van de software en de daarbij horende technische documentatie. Het doel van broncode-escrow is het loskoppelen van de software-continuïteit van het voortbestaan van de leverancier.

Broncode-escrow alleen is, mits technisch en juridisch goed geregeld, voor de gebruiker van een on premises informatiesysteem dat door hemzelf draaiend wordt gehouden, voldoende. Met de toegang tot de broncode kan hij op de lange termijn voorzien in het onderhoud en de doorontwikkeling van de software. Met de veiligstelling van een (curator-proof) gebruiksrecht op de software is hij ook op de korte termijn verzekerd van het onafgebroken gebruik van de software: hij heeft immers reeds een werkend objectcode-exemplaar ervan in huis. Ook de gegevens die met de software worden verwerkt, zijn intern en op eigen gegevensdragers vastgelegd.

Voor de gebruiker van SaaS is broncode-escrow onvoldoende. Dat komt met name omdat het onafgebroken gebruik van de software niet meer kan worden bewerkstelligd met een stevig gebruiksrecht en een werkend exemplaar van de objectcode. De gebruiker kan immers niet terugvallen op een draaiend informatiesysteem: daar is de inzet van de leverancier voor nodig. De leverancier zorgt voor het dagelijkse beheer van de door hem aangeboden SaaS-oplossing. Voorts is hij degene die de voor de levering van de software ingeschakelde derde-partijen aanstuurt en hen betaalt voor hun diensten. Deze derde-partijen hebben geen verplichtingen tegenover de SaaS-gebruiker, waardoor zij hun dienstverlening zouden kunnen staken op het moment dat de leverancier hen niet meer betaalt. Leveranciersonafhankelijke softwarecontinuïteit is bij SaaS daarom lastiger te bewerkstelligen dan bij on premises programmatuur.

Continuïteit SaaS-informatiesysteem bij faillissement leverancier?

Ook het verzorgen van de continuïteit van SaaS-oplossingen is een multidisciplinaire aangelegenheid. De gebruiker moet niet alleen over de technische middelen (broncode, documentatie, data etc.) beschikken die voor het verzorgen van zijn continuïteit noodzakelijk zijn (de technische beschikkingsmacht), hij moet ook het recht hebben om die zaken te gebruiken (de juridische beschikkingsmacht). Het is de vraag of de rechten die hem in de SaaS-overeenkomst zijn toegekend, voldoende zijn. Allereerst zit het gebruiksrecht alleen op een draaiend exemplaar van de objectcode van de applicatie dat niet op de apparatuur van de gebruiker is geïnstalleerd. De gebruiker kan met enkel de SaaS-overeenkomst in de hand geen aanspraak maken op de broncode. Datzelfde kan ook gelden voor de data, waarvan de gebruiker niet zonder meer eigenaar is op het moment dat daaromtrent geen afspraken gemaakt zijn.

Die vraag wordt extra relevant op het moment dat de leverancier wegvalt, omdat hij in staat van faillissement is gesteld, vooral vanwege het door de Hoge Raad gewezen Nebula-arrest[3]. Een curator kan beslissen om SaaS- en continuïteitsregelingen die niet tegen die beslissing bestand zijn gemaakt, te wanpresteren. De curator heeft dus goede mogelijkheden om de continuïteit van een SaaS-oplossing en de beschikbaarheid van de daarmee verwerkte data, te frustreren.

De curator dient immers niet het belang van de SaaS-gebruiker, maar zijn handelen is erop gericht om de vorderingen van de schuldeisers op de failliete boedel zoveel mogelijk te voldoen. Hij heeft daarbij veel vrijheid. Hij kan ervoor kiezen om mee te werken aan een continuïteitsregeling of om de SaaS-dienstverlening onder dezelfde

Een té beperkt begrip

Escrow is een begrip dat in beginsel moet worden gebruikt voor het verschijnsel waarin een partij ten behoeve van zijn wederpartij een goed in bewaring geeft aan een betrouwbare derde. Bij broncode-escrow betreft dat goed een softwarebroncode. Zoals in deze publicatie wordt betoogd, is broncode-escrow slechts een klein onderdeel van het verzorgen van de continuïteit van SaaS-informatiesystemen. De escrowdienstverlener is niet meer de partij die slechts een DVD in bewaring neemt en aan de gebruikers overhandigt in het geval van een calamiteit. Hij moet daarentegen de middelen en know how hebben om onder andere SaaS-ketens en de omvang van de continuïteitsrisico's voor de SaaS-gebruiker in kaart te brengen, de contractuele huishouding van een continuïteitsregeling samen te stellen en de taken van een weggevallen SaaS-dienstverlener of ketendienstverlener over te nemen.

SaaS-escrow

voorwaarden voort te zetten. Denkbaar is daarentegen dat de curator de uitvoering van de continuïteitsregeling stil legt en de gebruikers laat bieden voor de toegang tot de software en/of de data. Dat een curator in het ene faillissement niet tegenwerkt, zegt niets over zijn rol in een ander geval.

De gebruiker is niet zonder meer eigenaar van de data

Kortom de curator is een onvoorspelbare factor die in een continuïteitsregeling voor SaaS-informatiesystemen moet worden geneutraliseerd. De exclusieve technische en juridische beschikkingsmacht over de middelen waarmee de continuïteit van de softwaregebruiker kan worden verzorgd, moet in de regeling aan een potentiële curator worden ontrokken. De SaaS-gebruiker moet in het geval van een calamiteit bij zijn leverancier, met de continuïteitsregeling er zeker van zijn dat ook hij die beschikkingsmacht krijgt.

Verzorgen continuïteit SaaS-informatiesysteem: algemene aandachtspunten

Die beschikkingsmacht ziet op de componenten van het SaaS-informatiesysteem die door de gebruiker uit handen zijn gegeven. Het gaat in de hoofdzaak om de software, hardware, data en het operationele beheer. In een continuïteitsregeling zal dus in ieder geval aan deze specifieke zaken aandacht moeten worden besteed. In de komende paragrafen zal hierop worden ingegaan, naast het feit dat ook de volgende algemene aandachtspunten een rol spelen bij het verzorgen van de continuïteit van SaaS.

Allereerst moet rekening worden gehouden met het feit dat de regeling, zowel op de korte als op de lange termijn, continuïteit moet bieden. Bij het wegvallen van de SaaS-leverancier betekent dat ten aanzien van de korte termijn dat het onafgebroken gebruik van de applicatie en de onafgebroken beschikbaarheid van de data worden veiliggesteld. Voor de lange termijn betekent dit onder andere dat de oplossing moet kunnen worden onderhouden en doorontwikkeld. De gebruiker moet dus de middelen krijgen die hem in staat stellen om de SaaS-oplossing te laten aanpassen en beheren door een partij of partijen die de weggevallen leverancier op dat punt vervangt respectievelijk vervangen. Een (kostbare) migratie van het SaaS-informatiesysteem en/of de overstap naar nieuwe programmatuur moeten liefst niet noodzakelijk zijn voor continuïteit.

Een algemeen aandachtspunt is tevens het feit dat het opzetten van een continuïteitsregeling maatwerk betreft, omdat SaaS-informatiesystemen en de daarachter liggende ketenstructuren van geval tot geval verschillen. Dit betekent dat het pas duidelijk is welke continuïteitsmaatregelen moeten worden genomen, op het moment dat deze zaken in kaart zijn gebracht. Bovendien is dit een multidisciplinaire aangelegenheid. Een gedegen technisch en juridisch vooronderzoek is dus noodzakelijk.

Bij het opzetten van de regeling spelen voorts de kosten van continuïteit een rol. Er mag geen afbreuk worden gedaan aan de economische voordelen die voor de gebruiker juist de beweegreden zijn geweest om op SaaS over te stappen. Dat betekent dat er altijd een afweging is tussen de kosten van een continuïteitsmaatregel enerzijds en de omvang van het af te dekken risico anderzijds.

De SaaS-gebruiker moet de beschikkingsmacht over de applicatie en de gegevens behouden

In het algemeen kan ten slotte gesteld worden dat het verloop van een calamiteit bij de leverancier en de afwikkeling daarvan van te voren moeilijk te voorspellen is. Een faillissement bijvoorbeeld, kan het einde van de leverancier betekenen, maar een curator kan ook bijvoorbeeld proberen om een doorstart te organiseren. En een curator is niet de enige onzekere factor. Ook van de noodzakelijke medewerking van de partijen die onderdeel zijn van de SaaS-keten, mag niet vanzelfsprekend worden uitgegaan. Een escrowdienstverlener dient dus in het belang van de gebruiker zoveel mogelijk uit te gaan van een worst case scenario.

Verzorgen continuïteit SaaS-informatiesysteem: software en hardware

Bij het verzorgen van de continuïteit van een SaaS-informatiesysteem moet allereerst de component software worden veiliggesteld. Voor de continuïteit op de korte termijn is nodig dat de software onafgebroken kan worden blijven gebruikt. Hiervoor zal het allereerst zo moeten zijn dat de software te gebruiken is wanneer de SaaS-leverancier wegvalt. De gebruiker moet gerechtigd zijn om de applicatie in het geval van een calamiteit bij zijn leverancier te blijven gebruiken: zijn softwarelicentie moet in stand blijven. Voorts moet bij een calamiteit de feitelijke beschikbaarheid van de software en dus de beschikbaarheid van de hardware waarop de software draait, worden verzorgd. De partijen die binnen een SaaS-keten daarvoor verantwoordelijk zijn, moeten daartoe dus technisch en juridisch in staat zijn. Bovendien moeten zij zich tegenover de gebruiker met zekerheid committeren, maar er ook op kunnen vertrouwen dat zij voor hun dienstverlening worden betaald.

Voor continuïteit van de software op de lange termijn, dient gebruik te worden gemaakt van solide broncode-escrow. Uitgangspunt is dat alle broncode, technische documentatie, beheersinformatie, hulpsoftware en de overige zaken die noodzakelijk zijn voor het kunnen beheren, reconstrueren en onderhouden van het SaaS-informatiesysteem, gedeponeerd zijn bij de escrowdienstverlener.

Dit depotobject moet werkzaam en actueel zijn, iets waarbij de specifieke kenmerken van SaaS een belangrijke

rol spelen. Zo moet rekening worden gehouden met het feit dat veel SaaS-oplossingen zeer frequent worden geupdate, en de broncode ervan dus snel veroudert. Een mogelijke oplossing voor dit probleem is om met behulp van een koppeling aan het versie managementsysteem van de leverancier, ervoor te zorgen dat de escrowdienstverlener bij totstandkoming van een nieuwe versie van de broncode daarover meteen de beschikking krijgt.

In het geval van een calamiteit bij de SaaS-leverancier, wordt het depotobject aan de gebruiker afgegeven. Hij moet daarbij kunnen rekenen op ondersteuning bij het aanwenden van het depotobject voor continuïteit. Zo moet de escrowdienstverlener in staat zijn om het dagelijkse beheer van het SaaS-informatiesysteem over te nemen.

Verzorgen continuïteit SaaS-informatiesysteem: data en operationeel beheer

Bij het opzetten van een continuïteitsregeling verdienen de data specifieke aandacht. Ten eerste moeten zij beschikbaar blijven bij het wegvallen van de leverancier, iets wat net als bij de beschikbaarheid van de software gekoppeld is aan de beschikbaarheid van de hardware. De hosting van de data moet kortom gegarandeerd zijn, omdat de gebruiker niet de feitelijke beschikkingsmacht heeft over de gegevens, althans in verwerkbare vorm. Daarbij komt echter, dat de SaaS-gebruiker zonder nadere afspraken niet zonder meer eigenaar van de data is. In het kader van de continuïteitsregeling zullen daarom de (intellectuele) eigendomsrechten die op de data rusten, moeten worden overgedragen aan de gebruiker. De data moeten ten slotte in een voldoende overdraagbaar formaat zijn opgeslagen. Dit opdat de gebruiker, indien hij gewenst, over kan stappen naar een andere applicatie op het moment dat zijn SaaS-leverancier wegvalt.

Daarnaast dient de escrowdienstverlener bij het opzetten van de continuïteitsregeling vast te stellen welke organisatorische maatregelen moeten worden genomen: welke partijen moeten wat doen in het geval van een calamiteit bij de leverancier? Moeten werknemers van de weggevallen leverancier betrokken worden bij de voortzetting van het beheer van het informatiesysteem? De afspraken die worden gemaakt, zullen in een contract moeten worden gegoten, zodat de verplichtingen afdwingbaar zijn. De escrowdienstverlener zorgt ervoor dat de rol van de weggevallen SaaS-leverancier wordt uitgevoerd en dat op operationeel niveau het roer wordt overgenomen. Hij kan dat zelf doen, maar deze taak kan (op termijn) tevens worden uitgevoerd door een andere partij die daartoe bekwaam is. De escrowdienstverlener heeft ten slotte de functie van coördinator: hij verzorgt de aansturing van de ketendienstverleners die de SaaS-applicatie draaiend moeten houden. ●

> Een escrowdienstverlener dient uit te gaan van een worst case scenario

Links

[1] *H.J.J. Hensen en J.W. Oordt, 'Recht en Informatiebeveiliging: samen sterk', Informatiebeveiliging 2013/1.*

[2] *W.S. Chung, 'Informatiebeveiliging versus SaaS, Compact 2008/4.*

[3] *Zie voor een meer uitvoerige bespreking van dit arrest ook link [1].*

[4] *Software Borg Stichting: http://www.softwareborg.nl*

Software Borg Stichting en IT-notaris

De SaaS-continuiteitsregeling van Software Borg [4] gaat voor een belangrijk deel uit van de noodzaak van gedegen vooronderzoek en maatwerkoplossingen. Dat komt uiteraard doordat de techniek en organisatie van de dienstverleners-keten achter een SaaS-oplossing van geval tot geval verschilt. Zo kan het inschakelen van een hostingback-up noodzakelijk zijn, wanneer de software-leverancier zelf de applicatie en de data host. Een andere oorzaak is de contractenketen die de basis vormt voor de verplichtingen van de partijen die bij de SaaS-oplossingen betrokken zijn. De softwareleverancier hoeft bijvoorbeeld niet de houder van de auteursrechten op de applicatie te zijn.

Software Borg inventariseert en verzamelt de middelen en kennis die noodzakelijk zijn voor het voortzetten van de SaaS-oplossing bij het wegvallen van de leverancier. Deze worden gecontroleerd op werkzaamheid en actualiteit. Vervolgens worden deze zaken in een (digitale) kluis van de IT-notaris opgeslagen.

Voorts voorziet de continuïteitsregeling in de doorbetaling van de partijen die de SaaS-oplossing in stand moeten houden op het moment dat de softwareleverancier is weggevallen. Daartoe wordt gebruik gemaakt van een derdengeldenrekening. De gebruikers maken naar die rekening een bedrag over op het moment dat een calamiteit zich voordoet. De IT-notaris verzorgt aansluitend de doorbetaling.

Als tegenprestatie voor de zekerheid van de doorbetaling van hun dienstverlening, verplichten de ketendienstverleners zich tot het in de lucht houden van de SaaS-oplossing gedurende een bepaalde periode. Zo kan de SaaS-applicatie ook bij een calamiteit voor een bepaalde periode onafgebroken worden gebruikt en is het mogelijk om voor de lange termijn een oplossing te vinden met de broncode en de andere technische middelen die aan de IT-notaris zijn toevertrouwd.