



RECHTSPOSITIE EN BRONCODE

Risicobeperking softwaregebruik

De voordelen van geautomatiseerde systemen en goede software hoeven we tegenwoordig niet meer uit te leggen. Gebruikers kunnen bij een juiste keuze en goed gebruik hun werk veel efficiënter en effectiever uitvoeren. Dat er aan software ook negatieve kanten zitten en soms zelfs risico's kleven, is bij IT-auditors bekend. Om een van de haken en ogen te noemen: sommige software is (erg) onderhoudsgevoelig waardoor organisaties in meer of mindere mate afhankelijk zijn van de leverancier die vaak auteursrechthebbende is op de software. Dit artikel gaat in op de juridische aspecten van software en de vraag of deze afhankelijkheidsrisico's kunnen worden vermeden. Ook gaan we in op welke maatregelen je kan nemen en welke rol de IT-auditor daarin kan spelen.

HENRI HENSEN EN ERIK-JAN KREUZE

Het is wellicht een vreemde invalshoek om te beginnen met een pleidooi om anders naar software te kijken. Toch is dat wel nodig anno 2011. Of misschien wel juist in 2011, het jaar waar de economische crisis nog zo'n groot stempel op drukt. Die andere manier van kijken betreft dan onder meer de aandacht voor de juridische aspecten van software, software als vermogensbestanddeel¹ en de beeldvorming rond de inhoud van de relaties van bij software betrokkenen.

Een voorbeeld hiervan is de relatie licentiegever-licentienemer. Dit is geen gewone leverancier-klantrelatie. Door de langdurige band tussen softwareproducent en zijn afnemers, de volledige afhankelijkheid van de softwareproducent, het langdurige proces van vervanging van software en de onmisbaarheid van de gegevens uit het informatiesysteem (die vaak alleen leesbaar zijn, als de software werkt waarmee ze zijn vastgelegd) valt de softwareproducent niet te vergelijken met de leverancier van

levensmiddelen. De ontstane 'lotsverbondenheid' is een risico voor licentienemers en licentiegever.

Tegelijkertijd zijn de beschikbaarheid en continuïteit van het informatiesysteem erg belangrijk. Dit betekent dus dat de software steeds beschikbaar moet zijn in operationele staat. En om dat zo te houden moet de broncode met toebehoren onder alle omstandigheden beschikbaar zijn. Om dat goed te regelen is er een combinatie nodig van juridische zekerheid en technische continuïteit. Vooral met de juridische maatregelen wordt de basis gelegd onder de informatiebeveiliging en het beheersen van risico's die voortkomen uit de ontstane lotsverbondenheid.

JURIDISCH KADER

Hoewel het nooit zo wordt geformuleerd, is de handel in software feitelijk een handel in rechten. Dat heeft natuurlijk alles te maken met het auteursrecht waaronder ook software valt². Softwareproducenten maken daarbij handig gebruik van de



Auteurswet. Zij hebben namelijk het alleenrecht op openbaarmaking van hun producten. In de praktijk betekent dit, dat ze de zogenaamde objectcode (dat is de versie in digitale vorm) openbaar maken. Dat doen ze door een gebruiksrecht te verstrekken op de objectcode. Alle overige componenten van een compleet softwareproduct houden ze geheim. Dat is onder meer het materiaal dat ontwikkeld is voorafgaand aan het feitelijke programmeerwerk, en alle gebruikte hulpsoftware en de broncode zelf. Dit materiaal is wel nodig bij het onderhouden en doorontwikkelen van de programmatuur. Om deze reden zijn gebruikers aangewezen op een onderhoudscontract met de auteursrechthebbende van de software. Op zichzelf is dat aspect niet per se nadelig voor de licentienemers omdat op deze wijze kennis en kosten kunnen worden gedeeld, maar dit terzijde.

Het gaat te ver in het kader van dit artikel om alle op software en/of informatiesystemen zijnde wet- en regelgeving te bespreken. Denkt u bijvoorbeeld aan de Wet Bescherming Persoonsgegevens en de Data-bankwet. Het dient wel een punt van aandacht te zijn bij het treffen van beheersingsmaatregelen. Het kan een extra argument ervoor zijn of tot aanpassing van maatregelen leiden.

Als laatste in het juridische kader noemen wij hier een voor RA's en RE's relevant artikel uit het Burgerlijk Wetboek: 'De accountant brengt omtrent zijn onderzoek verslag uit aan de Raad van Commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.'³

Naast wet- en regelgeving kan er ook een juridische werking uitgaan van normen en *best practices* zoals bijvoorbeeld de Code voor Informatiebeveiliging en ITIL.

DE RECHTSPOSITIE VAN DE LICENTIENEMER

Zoals hierboven blijkt, is het standaardpraktijk dat de licentienemer uitsluitend een gebruiksrecht op de software krijgt.⁴ Het betreft dan uitsluitend de objectcode. Dat is op zichzelf al een zeer zwakke rechtspositie. Zowel tegenover de eigenaar van het auteursrecht als ook zijn eventuele rechtsopvolgers, waaronder hier voor het gemak overnemende partijen én een eventuele curator worden begrepen.

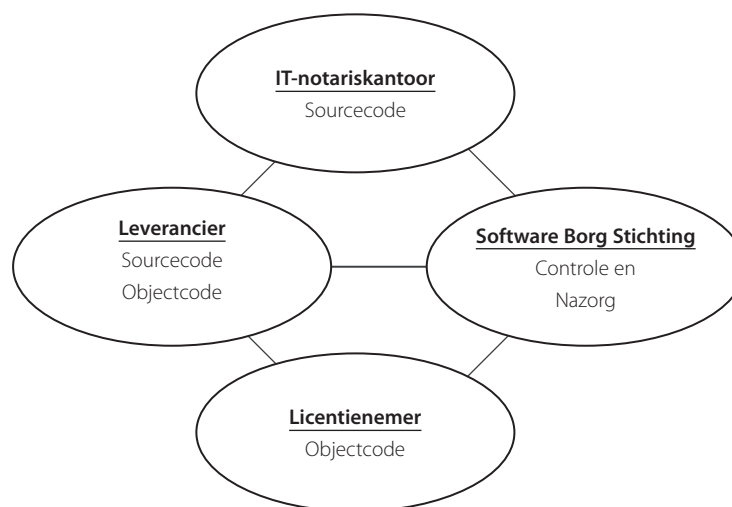
Deze rechtspositie wordt er meestal niet sterker op als gekeken wordt naar het eigendom van het auteursrecht. De meest eenvoudige en duidelijke vorm van eigendom is er, als de eigenaar van het auteursrecht een natuurlijke persoon is, die zelf de software heeft vervaardigd. Deze eenvoudige vorm van eigendom komt nog steeds voor. Maar in de praktijk werken de meeste softwareproducenten in de vorm van een rechtspersoon. Het auteursrecht houdt daar rekening mee. Het auteursrecht op het werk van een programmeur in loondienst gaat over op de werkgever.⁵ Maar hier houdt dit zeer beknopte verhaal over auteursrecht nog niet op. Steeds

meer softwareproducenten werken in een holdingstructuur. Daardoor wordt het voor de buitenwacht lastig om te weten wie de eigenaar van de software is. Daarbij gevoegd de mogelijkheden van het auteursrecht, dat er gedeeld eigendom bestaat, en er ook nog de mogelijkheid is pandrecht op software te vestigen.⁶ Dan wordt de vraag met wie een licentienemer eigenlijk zaken doet wel heel belangrijk.

De hele eigendomsvraag van software wordt nog eens ingewikkelder gemaakt door *open source software*. Bij deze software wordt juridisch gezien al snel gedacht aan vrijheid en blijheid, maar op open source software zijn ook licenties van toepassing. Daarvan zijn er heel veel in omloop en sommige daarvan bevatten verplichtingen met ingrijpende gevolgen.⁷ Er is een risico dat afgifte van een broncode kan worden geblokkeerd als niet aan de licentievoorwaarden is voldaan.

Het zal duidelijk zijn dat er in de vele factoren die van invloed zijn op de eigendomssituatie van software, wijzigingen kunnen optreden tijdens de gebruiksduur. Een regelmatige controle op de eigendomssituatie is dan ook noodzakelijk.

Schematische weergave:



Figuur 1: Software Borg Systeem 3: continuïteitsregeling

RECHTSZEKERHEID VOOR LICENTIENEMERS

De vraag is nu hoe de rechtspositie van licentienemers structureel kan worden verbeterd. Daarvoor is kennis en ervaring nodig op het grensvlak van de vakgebieden IT en Recht. Op dit grensvlak doen zich vele ontwikkelingen voor, denkt u aan jurisprudentie en opkomst ASP/SAAS-systemen. Er ontstaan nieuwe specialismen, producten en diensten. Langer bestaande diensten worden geprofessionaliseerd. Dat geldt bijvoorbeeld voor het 'product' broncode-escrow. Sinds het notariaat zich serieus met de ontwikkeling heeft beziggehouden, is de kwaliteit van de escrow-diensten sterk verbeterd.

Broncode deponering gebeurt vooral in het belang van de softwaregebruiker. Minder bekend is, dat ook de eigenaar van het auteursrecht (softwareontwikkelaar) op een broncode een belang heeft. Dat is gelegen in het feit dat het auteursrecht op broncodes niet wordt geregistreerd. Dat vindt zijn oorzaak in het auteursrecht. Het auteursrecht ontstaat namelijk spontaan en het belangrijkste vereiste voor auteursrechtelijke bescherming is dat het werk 'een eigen, oorspronkelijk karakter bezit en het persoonlijk stempel van de maker draagt'.⁸ Het registreren van auteursrecht hoeft bij veel producten vaak niet, omdat door openbaarmaking (dit is één van de rechten van de maker) controle op namaak (plagiat, vervalsing) vrij gemakkelijk plaatsvindt. Voor software ligt dit natuurlijk heel anders en zeker voor de broncode, die met opzet geheim wordt gehouden.

Er is een praktische oplossing voor dit gebrek aan rechtszekerheid. Dat is het deponeren van een broncode bij de notaris door middel van een notariële akte, nadat een zogenaamd titelonderzoek is verricht. Dit titelonderzoek heeft tot doel een duidelijke eigenaar te identifi-

ceren. Uiteraard speelt kennis van auteursrecht en van softwareontwikkeling hierbij een belangrijke rol. De voordelen zijn evident: er is nu een duidelijke en geregistreerde eigenaar en doordat de broncode is gedeponerd bij de notaris zijn inbreuken op het auteursrecht veel beter te bestrijden. Daarbij helpt, dat de notariële akte dwingende rechtskracht heeft.

Broncodedeponering, mits deskundig en zorgvuldig uitgevoerd, kan er voor zorgen, dat er duidelijkheid bestaat over de vraag of de licentienemer wel een overeenkomst heeft afgesloten met de juridische eigenaar van de software waar hij alleen een gebruiksrecht van heeft. Dit wordt tegenwoordig ook bij elke herdeponering opnieuw door de notaris gecontroleerd.

RECHT OP DE BRONCODE

Als de software op een juridisch correcte wijze gedeponerd is, dan is het nog een kleine stap, om de licentienemer het recht te verlenen op de broncode onder zgn. opschortende voorwaarde. Ook daarvoor moeten wel eisen gesteld worden aan de wijze waarop de broncode is gedeponerd. De belangrijkste eis is, dat er een deskundige controle heeft plaatsgevonden van de broncode met alle toebehoren. Daarbij is het belangrijk, dat men zich realiseert, dat broncodedeponering ook bedoeld is om schade te beperken, die het gevolg kan zijn van (langdurige) uitval van informatiesystemen. Met het te deponeren materiaal moet onderhoud en doorontwikkeling kunnen plaatsvinden. Daarom trent kan alleen zekerheid worden geboden na een reconstructie van de software door vanuit een broncode en alle gebruikte hulpsoftware een werkende objectcode te generen. Daarnaast moet er tevens nog een test worden uitgevoerd of wijzigingen in de objectcode kunnen worden doorgevoerd. Nadat vastgesteld is, dat het te deponeren materiaal vol-

ledig is, moet vervolgens nog aandacht worden besteed aan de overdraagbaarheid. Zoals bekend zal zijn bij IT-auditors wordt het belang van documentatie door softwareontwikkelaars nogal eens onderschat. Het is daarom nodig dat de informatie die nodig is voor de overdraagbaarheid, wordt vastgelegd en toegevoegd aan de te deponeren broncode. Dit kan gebeuren tijdens de controle van de broncode.

AFGIFTEREGELING

Onder welke voorwaarden kan de licentienemer een beroep doen op afgifte van de broncode? In de praktijk komen doorgaans de volgende afgiftegronden voor:

- Overeenstemming tussen de leverancier en broncode-escrow agent, dat het afgifte-recht mag worden uitgeoefend.
- Het vervallen van de inschrijving van de leverancier bij de Kamer van Koophandel.
- Het faillissement van de leverancier.
- Overdracht van de programmatuur door de leverancier aan derden, zonder dat rechten en plichten uit de overeenkomst met de broncode-escrow agent zijn overgedragen.
- Een rechterlijke uitspraak waarbij vastgesteld is dat:
 - de leverancier de met de broncode-escrow agent gesloten overeenkomst niet volledig nakomt;
 - de leverancier zijn verplichtingen uit overeenkomsten met een licentienemer niet behoorlijk vervult;
 - de leverancier het onderhoud van de betreffende programmatuur heeft gestaakt.

Een voorwaarde voor afgifte is natuurlijk ook, dat de licentienemer in aanvulling op zijn licentieovereenkomst, met de organisatie die broncode-escrow verzorgt, een overeenkomst heeft afgesloten. Bijkomende voorwaarden zijn dan natuurlijk, dat er op het moment van afgifte sprake moet zijn van een geldige licentie- en onderhoudsovereenkomst. ▣



CONTROLEMOGELIJKHEID DOOR LICENTIENEMERS

Voor veel licentienemers zijn begrippen als 'automatisering' en 'software' al behoorlijk abstracte begrippen. Broncodedeponering wordt dan al gauw ervaren als een complex vraagstuk. Dat wordt nog eens in de hand gewerkt door de vele broncoderegelingen die kwalitatief niet aan redelijkerwijs te stellen eisen voldoen. Dat wordt vaak verhuld met een gebrek aan voorlichting en controleerbaarheid. Het is belangrijk, dat aan licentienemers de mogelijkheid wordt geboden, te controleren of de broncode van de door hun gebruikte software is gecontroleerd én gedeponerd. Dit moet onder meer duidelijk gemaakt kunnen worden door middel van een controleverslag aan de licentienemer. Dit controleverslag moet gegevens bevatten over de partijen, en hun contactpersonen die bij deponering zijn betrokken. Ook gegevens over de frequentie van deponering zijn van belang. En tenslotte moet er een hardcopy van het inlogscherf van de gebruiksversie van de software worden opgenomen met extra gegevens die de verificatie van de software door de licentienemer mogelijk maken. Het kan een belangrijk onderdeel van het werk van een IT-auditor zijn, toe te zien op de aanwezigheid van een controleverslag van de broncode-escrow regeling.

CONTROLEMOGELIJKHEDEN DOOR IT-AUDITORS

Als informatiebeveiliging een belangrijk aandachtspunt is voor IT-auditors, dan hoort daar zeker aandacht voor de rechtspositie van de softwaregebruiker bij. Als er iets in de relatie softwareproducent – licentienemer dreigt mis te gaan, of misgaat, dan hangt de vraag of de schade beperkt kan worden voor een groot deel af van de rechtspositie van de softwaregebruiker. En de licentieovereenkomst geeft doorgaans uitsluitend het recht op het

gebruik van een verzameling nullen en enen (objectcode).

Nu is de IT-auditor vaak geen jurist. En bovendien is het aan ICT gerelateerde recht net als het vakgebied van de IT-auditor sterk in ontwikkeling. De logische vraag is dan ook hoe je hier als IT-auditor praktisch mee om moet gaan.

Een antwoord kan zijn het kiezen voor een zorgvuldig uitgevoerde en op wetenschappelijke basis onderbouwde broncodedeponering. Broncodedeponering is een activiteit op het grensvlak van IT en Recht en heeft slechts zin als de vele juridische details allemaal en in samenhang een sluitend geheel opleveren. Daarnaast moet er natuurlijk ook een broncode met toebehoren worden bewaard, die geschikt is voor het doel: schade beperken.

Het is goed om te weten dat het notariaat hier een voortrekkersrol vervult. Zo is in 1998 de Vereniging voor Notariaat en Informatietechnologie opgericht. En bestaat er een samenwerkingsverband van enkele tientallen gespecialiseerde notariskantoren met een centrale organisatie: de Software Borg Stichting. Deze Stichting houdt het Centraal Auteursrecht Register Software bij.

Vanwaar de belangstelling van het notariaat voor software? Dat heeft alles te maken met de bijzondere positie van de notaris in ons rechtsbestel. Zo is er een notariswet (die zelfs iets zegt over broncodedeponering)⁹, kan de standplaats van de notaris niet failliet gaan (van belang voor continuïteitsaspecten) en heeft zijn akte dwingende rechtskracht (van belang voor bescherming auteursrecht). Ook heeft de beroepsgroep een sterke wetenschappelijke basis. Deze aspecten zijn voor een onderwerp als broncodedeponering van cruciaal belang onder meer in ver-

band met het volgen van de juridische ontwikkelingen. Denkt u in dit verband vooral aan de jurisprudentie.

De belangrijkste functie van het notariaat is het bevorderen van de rechtszekerheid. Op dat gebied ligt er nog een groot terrein braak in de softwarewereld. Hiervoor is het belang van een goede rechtspositie van een licentienemer van software al beschreven in het kader van het beperken van de risico's van softwaregebruik. Maar er zijn veel meer redenen voor broncodedeponering die in dit artikel nog aan de orde komen.

Belangrijke vragen die de IT-auditor kan stellen om zicht te krijgen op de kwaliteit van een broncoderegeling (broncode-escrow) zijn, onder meer, welke continuïteitsgaranties de bewaarder van de broncode verstrekt over zijn eigen voortbestaan, of er een serieuze onafhankelijke controle plaatsvindt door technici die zelf ook verantwoordelijk zijn voor de nazorg en in hoeverre de betreffende regeling de nazorg geregeld heeft in het geval van een beroep op de broncode. Als hier twijfel over is, dan is het mogelijk een second opinion te vragen aan een gespecialiseerde IT-auditor of notaris. Daarvoor is alle kennis in hun netwerk aanwezig.¹⁰

BIJZONDERE REDENEN VOOR BRONCODEDEPONERING

In de praktijk ontstaan naast de bekende reden van informatiebeveiliging nog steeds nieuwe redenen om de broncode van nieuwe of reeds bestaande software op juridisch correcte wijze te deponeren: wij noemen hier de meest voorkomende:

- Overdracht van auteursrecht op software. Dit vindt plaats bij de verkoop van *softwarehouses* en bij overdracht van broncodes. Het gaat er daarbij vooral om een exact beeld van de over te dragen software te krijgen op het moment van overdracht. Dit is van belang voor de vraag of fouten voor of na de

eigendomsoverdracht in de broncode zijn ontstaan. Te meer omdat de overnamesom vaak afhangt van het aantal licentienemers, die van de software gebruik (blijven) maken.

- ♦ Fiscale redenen. De belangrijkste daarvan is de fiscale bewaarplicht. De fiscus baseert zich voor de regelgeving op dit punt op de Algemene Wet Rijksbelastingen uit 1965.¹¹ De verantwoordelijkheid om te voldoen aan de fiscale bewaarplicht van geautomatiseerde administratieve systemen wordt geheel bij de belastingplichtige organisatie gelegd. De fiscus ziet het recht op de broncode wel als een belangrijke beheersingsmaatregel.
- ♦ Pandrecht op software. Software is doorgaans het enige bezit van een softwarehouse. Geldschietters zijn misschien bereid geld te lenen maar willen daartegenover natuurlijk zekerheid. Een bij de IT-notaris gedeponeerde broncode biedt die zekerheid voor de geldschietter. Dit kan ook goed gecombineerd worden met een continuïteitsregeling voor de licentienemers.
- ♦ Zeer langlopende licentieovereenkomsten zoals in Publiek Private Samenwerkingen (PPS) De in dit soort projecten gebruikte software moet soms 30 of 40 jaar beschikbaar blijven.
- ♦ Samenwerkingsovereenkomsten tussen softwareontwikkelaars. Na jaren kan de vraag opkomen: wie heeft wat, wanneer ingebracht?
- ♦ De kwetsbaarheid van apparaten en productielijnen door uitval van software: PLC (*Programmable logic controller*), FPGA (*Field-programmable gate array software*).
- ♦ De nieuwe Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT), versie 2010.¹² Artikel 47 inzake escrow bepaalt dat de leverancier altijd een escrowregeling moet hebben. Deze moet voldoen aan hetgeen ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is.

Actief broncodebeheer in de praktijk

Broncode en fiscus

Op alcoholhoudende dranken zit zoals bekend accijns én uiteraard BTW. De kostprijs van sterke drank en de consumentenprijs heeft ruwweg een verhouding van 1 op 5. Oftewel 80% van de consumentenprijs bestaat uit belasting. Deze bedrijfstak wordt daarom buitengewoon scherp in de gaten gehouden door de fiscus. Een softwareproducent in deze branche besloot het onderhoud op zijn programma te stoppen. Hij ging na deze aankondiging nog twee jaar door met het onderhoud. De belastingplichtige bedrijven moeten hun gegevens nog zeven jaar bewaren én toegankelijk houden. Nadat het onderhoud was gestopt, heeft de notaris waar de broncode was gedeponeerd volgens het Software Borg Systeem deze afgegeven. Software Borg heeft volgens een zorgvuldige afgifteprocedure de broncode met toebehoren gedistribueerd. Zoals uit dit praktijkgeval blijkt, zijn er veel meer redenen voor broncode-deponering dan alleen het faillissement. De notarissen die met het Software Borg Systeem werken, hebben overeenkomsten waarin veel in de praktijk ontstane afgiftegronden zijn verwerkt.

ACTIEF BRONCODEBEHEER IS DE BASIS VAN UW INFORMATIEBEVEILIGING

ACCEPTATIEBELEID

De essentie van de werkzaamheden van een organisatie die zich bezighoudt met broncode-escrow is schade beperken. Dat begint al in de preventieve sfeer, maar komt het meest pregnant naar voren op het moment dat zich een calamiteit voordoet. Dan moet een belofte worden waargemaakt. Er moet dus worden gewaakt tegen schijnzekerheid. Daarvoor dient het acceptatiebeleid.

Hoewel het basisprincipe van broncode-escrow eenvoudig is, vergt een serieuze uitvoering daarvan veel kennis en ervaring. En omdat het een activiteit is op het grensvlak van IT en Recht moeten op deze vakgebieden de risico's die de uitvoering van de belofte kunnen bedreigen, in een acceptatiebeleid worden opgenomen. Naast juridische en technische risico's

zijn er ook algemene risico's die de kwaliteit van een broncoderegeling kunnen bedreigen of deze zelfs zinloos kunnen maken.

De juridische risico's kunnen grofweg verdeeld worden in de risicovolle aspecten die aan de betreffende broncode kunnen zijn gerelateerd en risico's die voortvloeien uit ontwikkelingen op juridisch gebied zoals jurisprudentie. Een goed voorbeeld daarvan is het Nebula arrest, dat de bodem heeft weggeslagen onder alle broncode-escrowregelingen die gebaseerd zijn op obligatoire overeenkomsten.¹³ In de praktijk is dat de meest voorkomende soort.

Bij technische risico's die schadelijk kunnen zijn voor een optimaal effect van de regeling behoren vooral factoren die de overdraagbaarheid betreffen. Daaronder vallen onder meer exotische programmeertalen, bedrijfseigen ontwikkelomgevingen en onnavolgbare systeemontwerpen. En natuurlijk moet de softwareontwikkelaar zijn medewerking verlenen aan de controlewerkzaamheden. Een overdreven zorg voor geheimhouding zoals beschreven in het boek *De Broncode*¹⁴ maakt broncode-deponering onmogelijk.

En dan zijn er nog de algemene risico's die de werking van broncode-escrowregelingen kunnen bedreigen. Zo beschermt een solide broncoderegeling vooral tegen zakelijke risico's die de relatie tussen softwareproducent en softwaregebruiker (onherstelbaar) kunnen beschadigen. Het beschermt dus niet (afdoende) tegen bijvoorbeeld gezondheidsrisico's waaraan eenmansbedrijven zijn blootgesteld. Overigens kan dit risico zich in verschillende vormen ook bij grotere softwareproducenten voordoen.

Het is om deze redenen van belang te kijken naar de ethiek en moraal van de organisatie die dit soort diensten aanbiedt. Uiterlijke en ▣



gemakkelijk te herkennen kenmerken op dit gebied zijn onder meer het lidmaatschap van een relevante beroepsvereniging van de verantwoordelijken binnen een organisatie voor deze activiteit¹⁵ en een beroepsaansprakelijkheidsverzekering die de activiteit broncode-escrow dekt.

KWALITEITSLABEL VOOR PROCES VAN BRONCODEDEPONERING SAS 70

Bij broncodeponering is er sprake van samenwerking tussen de auteursrechthebbende en de broncode-escrow agent. Aan deze samenwerking kan goed vorm worden gegeven door procesbeschrijving, formuleren en instructies. En er kunnen veel controle mogelijkheden worden ingebouwd voor bewaking van de kwaliteit onder meer door inschakeling van de notaris. Maar alleen al door het tijdsverloop tussen twee controles valt er geen 100 procent zekerheid te bereiken. Dat is de reden dat de werkzaamheden van elke escrow agent gebaseerd moeten zijn op een inspanningsverplichting. Maar hoe weten de niet deskundige betrokkenen nu, dat die vereiste inspanningen ook echt geleverd worden? De uitkomst op deze belangrijke vraag kan voor een deel geleverd worden door het gereedschap van de IT-auditor, te weten de SAS 70-methode.

Het betreft dan het softwaretechnische deel. Die beperking wordt veroorzaakt doordat de IT-auditor geen diepgaande kennis heeft van juridische aspecten van software.



In het enige bekende geval dat de SAS 70 methodiek is toegepast¹⁶, is voorafgaand aan het onderzoek een team samengesteld, waarin de IT-auditor kon samenwerken met een in IT-recht gespecialiseerde wetenschapper, een oud notaris en een advocaat die ervaring heeft als curator in faillissementen van IT-bedrijven.

In overleg is een gestructureerde aanpak ontwikkeld om zo efficiënt mogelijk naar een SAS 70-rapportage te komen.

Belangrijk kenmerk van de SAS 70 is dat er geen sprake is van een vastomlijnd normenkader. De *assertions* (controle doelstellingen) worden vaak afgeleid van de jaarrekeningcontrole. Voor uitbesteding van IT-diensten is dat minder toepasselijk of hoogstens op metaniveau. Binnen SAS wordt dat opgelost door alle risico's en controls te beschrijven en vervolgens te toetsen. Voor wat betreft de softwaretechnische aspecten is dat natuurlijk een vertrouwd werkkterrein voor de IT-auditor.

De samenwerking tussen de IT-auditor en de juristen heeft uiteindelijk geleid tot een goedkeurende SAS 70-verklaring type 1. Het was een nuttige exercitie omdat daarmee drie vliegen in één klap werden geslagen: de werkwijze met betrekking tot de controle werkzaamheden en de verslaglegging daarvan zijn kritisch beoordeeld, de juridische aspecten op zichzelf zijn kritisch tegen het licht gehouden en tenslotte is ook de nauwe onderlinge samenhang van de juridische en softwaretechnische aspecten beoordeeld door de onderzoekers.

Dit laatste onderdeel van het totale onderzoek is natuurlijk het meest unieke resultaat. Er is immers nooit eerder zo'n onderzoek door zo een team verricht.

Anno 2011 weten we natuurlijk dat SAS-70 achterhaald dreigt te worden door ISAE 3402 en de richtlijn 3000 voor assurance-rapportages. Doorontwikkeling in de toekomst zal dan ook nodig zijn. Dit neemt niet weg dat de Software Borg Stichting de



H.J.J. Hensen (Henri) is vanaf 1972 tot op heden actief in de automatiseringsbranche. In 1992 richtte hij samen met een notaris de Software Borg Stichting op. Hij geeft gastcolleges onder meer voor de vakgroep Recht en ICT van de Rijksuniversiteit Groningen.



Drs. J.H. Kreuze RE RA (Erik-Jan) is registeraccountant en IT-auditor bij Afier Accountants en Bedrijfsadviseurs, een door de Autoriteit Financiële Markten gecertificeerd accountantskantoor.

SAS 70 in 2009 heeft gebruikt om haar kwaliteit aan derden zichtbaar te maken.

CONCLUSIE

Uit het oogpunt van informatiebeveiliging is aandacht voor de juridische aspecten van software noodzakelijk. Een licentieovereenkomst alleen geeft de licentienemer (gebruiker) een zwakke rechtspositie. Bovendien is er een aanzienlijk risico dat de licentieovereenkomst met de verkeerde partij wordt aangegaan. Namelijk een partij die het auteursrecht zelf niet bezit. Dit heeft vanzelfsprekend de nodige impact op de rechtspositie van de licentienemer. Ook het feit dat gebruikers geen enkel recht hebben op de broncode van software maakt hen onnodig kwetsbaar, omdat het voortbestaan van de softwareproducent en de gebruiker daardoor praktisch aan elkaar gekoppeld zijn. Dat heeft te maken met de onderhoudsgevoeligheid van software, het langdurige vervangingstraject en grote (financiële) schade aan de bedrijfsvoering bij uitval van software. Een solide broncode-escrowregeling is dan ook een logische aanvulling op de licentieovereenkomst. Hier ligt een mooie taak voor IT-auditors op een nog braakliggend terrein als controleur en adviseur. ■

Noten

1. Software, een novum in het vermogensrecht, E.P.M. Thole.
2. Ex artikel 10 lid 1 sub 12 Auteurswet.
3. Ex artikel 393 lid 4 Burgerlijk Wetboek boek 2.
4. Zie ook de Algemene Voorwaarden van ICT-office.
5. Ex artikel 7 Auteurswet.
6. Pandrecht in de notariële praktijk, *Ars Notariatus*, deel 136, mr. J.G. Gräler, hoofdstuk Pandrecht op ICT-producten.
7. Zie: <http://gpl-violations.org/news/20041024-linux-totom.html>.
8. HR 4 januari 1991, NJ 1991, 608, AMI 1991, p. 177; van Dale/Romme.
9. Zie memorie van toelichting op art. 48 Notariswet.
10. Zie www.softwareborg.nl.
11. Ex artikel 52 Algemene Wet inzake Rijksbelastingen.
12. Zie Staatscourant nr. 11138, Regeling van de minister-president, minister van Algemene Zaken, van 7 juli 2010, nr. 3093917.
13. HR 3 november 2006, RvdW 2006, 1033.
14. *De Broncode*, auteur: Eric Smit.
15. Zie www.nvbi.nl.
16. Zie www.softwareborg.nl.