

COMPACT

TIJDSCHRIFT EDP-AUDITING

**FORMELE ASPECTEN
VAN Y2K**

1998 / 6

INHOUDSOPGAVE

Compact ©
 Jaargang 25, nummer 6
 Een uitgave van KPMG EDP
 Auditors NV en ten Hagen &
 Stam BV.
 Het blad verschijnt 6 x per jaar.
Redactie
 Prof. A.W. Neisingh RE RA
 (hoofdredacteur)
 Drs. P.P.M.G.G. Brouwers RE RA
 Ir. J.A.M. Donkers RE
 W. de Korte RE RA
 J.C. van Praat RE RA
 Ir. Drs. J. van der Vlugt
Adviesraad
 Mr. P. van Dijken
 G. van Essen RA
 Prof. mr. H. Franken
 Dr. K.I.J. Mollema RA
 Prof. H.B. Moonen RE RA
 Prof. dr. ir. R. Paans RE
Bureau redactie
 Drs. Q.C.H.J. Hünteler,
 ten Hagen & Stam,
 Postbus 34,
 2501 AG Den Haag
 Tel.: 070 - 304 57 74
 Fax: 070 - 304 58 17
 e-mail: q.hunteler@wkhhs.nl
Basisvoormgeving
 Bureau Karakter, Delft
Opmaak
 AlphaZet bv, Waaldivoeren
Abonnementen
 f 165,- per jaar incl. BTW.
 Losse nummers f 45,- incl. BTW.
 Studentenabonnement f 95,-
 incl. BTW. Abonnementen kunnen
 schriftelijk tot uiterlijk één maand
 voor de aanvang van een nieuw
 abonnementsjaar worden opgezegd.
 Bij niet tijdige opzegging wordt het
 abonnement automatisch met een
 jaar verlengd.
Abonnementsadministratie
 Sansom Bedrijfsinformatie,
 Postbus 4,
 2400 MA Alphen aan den Rijn
 Tel.: 0172 - 466 800
 Fax: 0172 - 475 933
 Adreswijzigingen - ook tijdelijke -
 moeten minstens 8 weken voor de
 verschijningsdatum bekend zijn.
Overname artikelen
 Het overnemen en vermenigvuldigen
 van artikelen en berichten is
 slechts geoorloofd na schriftelijke
 toestemming van de uitgever.
Overdrukken artikelen
 Oeverdrukken van artikelen kunnen
 worden aangevraagd bij de bureau-
 redactie. Prijs per overdruk per
 artikel (inclusief omslag) f 5,-.
Uitgever
 I.J. van Haren

3
Millenniumprobleem onder controle, ook als het toch mis gaat?
Ir. M.B.J. van Goethem en drs. K.H.G.J.M. Ho RA
 Het opstellen en uitvoeren van een specifiek contingencyplan voor de overgang naar het nieuwe millennium is hard nodig om de continuïteit van de organisatie te waarborgen. Dit artikel beschrijft Millennium Contingency Planning en de rol van het (ICT-)management bij de realisering van een dergelijk plan.

11
Aansprakelijkheid van de softwareleverancier voor de millenniumbug
Mr. P.P.J.L. Enneking en mr. M. Seelt
 Eerst het probleem oplossen, dan pas strijden over de vraag wie moet betalen, aldus premier Kok. Toch kan men niet vroeg genoeg beginnen met het voorbereiden van een eventuele claim. Dit artikel behandelt de vraag wanneer de softwareleverancier aansprakelijk te stellen is voor het niet nakomen van de leveringsovereenkomst.

34
Y2Kkosten, baten
Drs. T.G. Kloosterman
 De millenniumbug stelt de accountant voor diverse problemen. Kosten en baten uit hoofde van het millenniumprobleem moeten worden ingeschat en vervolgens worden verwerkt in de jaarrekening. Dit artikel reikt handvatten aan om te komen tot een verantwoorde verwerking van Y2K in de jaarrekening.

43
Y2K voor de registeraccountant
J.C. van Praat RE RA
 Accountants spelen in toenemende mate een rol bij het toetsen of organisaties wel voldoende maatregelen treffen om het millenniumprobleem op te lossen. Dit artikel gaat in op de inhoud van die rol en op de consequenties voor de toekomstige beroepsuitoefening en de verdere ontwikkeling van het beroep.

48
Cumulatief

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:

- beoordeling automatiseringsorganisaties en -systemen
- risicobeheersing
- telecommunicatie-adviezen
- beveiligingsonderzoeken
- quality assurance
- opleidingen en trainingen
- privacywetgeving
- computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteurs persoonlijk, noch uitgeverij ten Hagen & Stam BV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers.

Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij de bureau-redactie verkrijgbaar is.

Dit nummer van Compact is geheel gewijd aan de problematiek rondom het jaar 2000. Helaas moet worden geconstateerd dat nog steeds niet alle organisaties zich bewust zijn van het feit dat het niet tijdig oplossen van het Jaar 2000-probleem niet slechts in informatie- en communicatietechnologie, doch ook in zogenoemde non-ICT-objecten een continuïteitsbedreiging is van de eerste orde. Veel organisaties hebben voor wat betreft ICT een groot onderhoudsproject opgetuigd en managen ook als zodanig. Dat wil zeggen een projectorganisatie is ingericht, projectplannen zijn uitgewerkt en prioriteitstelling gedefinieerd en voorzover dat nog niet in voldoende mate was geschied, is een zogenaamd awareness-programma gestart. Daarmee zijn wij er echter niet. Ten minste dient te worden gewaarborgd dat nieuw aan te schaffen hardware, besturingsprogrammatuur, toepassingsprogrammatuur en dergelijke in ieder geval Jaar 2000-compliant is. Een belangrijke actie betreft vanzelfsprekend het inventariseren van alle ICT- en non-ICT-objecten. Een heck of a job, omdat de volledigheid van zo'n overzicht nooit kan worden gegarandeerd; gebleken is dan ook dat dergelijke overzichten bij voortduring aan wijziging onderhevig zijn geweest. Wanneer aldus sprake is van een zorgvuldige voorbereiding van het complexe onderhoudsproject zal met het aanpassen van de programmatuur begonnen zijn. De Nederlandsche Bank heeft in haar memorandum van september 1997 realistische tijdlijnen weergegeven met betrekking tot de oplossing van het Jaar 2000-probleem bij banken en financiële instellingen die onder haar toezicht vallen. De tijdlijnen die onder meer betrekking hebben op het Jaar 2000-compliant maken van kritieke toepassingen (uiterlijk eind 1998) en overige toepassingen (medio 1999) leken op het moment van uitvaardiging van het memorandum haalbaar, doch blijken thans in veel gevallen zeer ambitieus te zijn. Dat is overigens een groot probleem, want 'the time is running away'. Begin 1999, aan de vooravond van de 21ste eeuw, hebben wij nog circa tweehonderd werkdagen om de laatste hand te leggen aan de oplossing van het probleem.

Wij bevinden ons thans op een moment dat het testen van kritieke toepassingen dient te zijn afgerond en met het testen van de overige toepassingen inclusief hardware-/software-infrastructuur ten minste dient te zijn begonnen. Testen van 2000-compliance betreft niet slechts testen op twee of vier posities voor het jaartal, doch eveneens tijdreizen, dat wil zeggen het verzetten van de computerklok en in ieder geval het testen van de ketens waarin de organisatie is opgenomen. Immers, één niet-compliant onderdeel in een elektronische keten kan de continuïteit van de gehele keten verstoren. Dit is overigens geen sinecure. Een bijzonder beheersprobleem betreft overigens, en dat terzijde, het feit dat thans

een drietal soorten programmatuurbibliotheken beschikbaar dient te zijn en wel:

- de operationele programmatuur, die op dit moment voor de gegevensverwerking wordt gebruikt;
- de inmiddels Jaar 2000-compliant-programmatuur
- de inmiddels eurocompliant gemaakte programmatuur.

Want één probleem tijdens de eeuwwisseling bleek helaas niet genoeg te zijn.

Na het testen van de programmatuur volgt uiteraard de invoering ervan, hetgeen na zorgvuldige voorbereiding en correct bibliotheekbeheer niet echt een groot probleem behoeft te zijn. Wel dienen organisaties zich te realiseren dat nog een tweetal zaken goed geregeld moet zijn, en dat zijn:

- de juridische aspecten rondom de aansprakelijkheid ten aanzien van het jaar 2000-probleem;
- het ontwikkelen van noodvoorzieningsplannen ingeval de continuïteitsdreiging zich omzet in een feit.

In dit nummer van Compact wordt uitgebreid aandacht besteed aan beide onderwerpen, waarna vervolgens de kosten-batenproblematiek met betrekking tot het Jaar 2000-probleem wordt besproken.

Vanzelfsprekend is afzonderlijk ingegaan op Y2K voor de registeraccountant.

Opnieuw een nummer van Compact dat op de problematiek van het gebruik van ICT ingaat en de actualiteit niet schuwt.

Prof. A.W. Neisingh RE RA

Millenniumprobleem onder controle, ook als het toch mis gaat?

Ir. M.B.J. van Goethem en drs. K.H.G.J.M. Ho RA

Millennium Contingency Planning is de specifieke vorm van contingencyplanning waarvan de stappen concreet zijn gericht op de millenniumovergang. Deze stappen worden helder beschreven om het (ICT-)management handvatten te geven om de organisatie optimaal over de inmiddels beruchte drempel te helpen.

INLEIDING

Stelt u zich de volgende situatie eens voor: het is zeven uur 's avonds en door een stroomstoring is er geen elektriciteit beschikbaar in de stad. Dit incident heeft de volgende gevolgen:

- mensen moeten uit liften en treinen worden gered;
- verkeerslichten en benzinepompen werken niet meer;
- reddingswerkers gebruiken satelliettelefoons om te communiceren.

Na enkele dagen is de stroomvoorziening nog steeds niet hersteld waardoor:

- banken gesloten zijn;
- problemen met watervoorziening en afvalwater tot massa-evacuaties leiden;
- apothekers geen medicijnen kunnen klaarmaken en leveren omdat hun computers niet werken.

Omdat de problemen enige weken aanhouden worden de gevolgen groter:

- het stadscentrum zit vol met politie om criminaliteit te voorkomen;
- inspecteurs van de volksgezondheid gaan naar restaurants om voedselvergiftiging te voorkomen die het gevolg is van een gebrek aan koeling;
- branden ontstaan als gevolg van oververhitte noodaggregaten (doordat ze slecht zijn onderhouden of doordat ze te veel worden belast);
- schepen worden weggestuurd van de haven omdat aan- en afvoer niet kan worden afgehandeld; er is geen elektriciteit om de computers waarop de systemen draaien te laten werken;
- het Bruto Binnenlands Product zal 0,35 procent lager zijn als gevolg van de crisis in deze stad;
- advocaten staan in de rij om iemand te vervolgen; iedereen die ze de schuld kunnen geven voor de huidige chaos komt in aanmerking;
- de handel stopt; klanten van buiten de stad gaan naar andere steden;
- de toekomst ziet er somber uit.

Is dit fictie, of zou deze situatie zich ook in uw omgeving kunnen voordoen?

De hierboven beschreven gebeurtenis vond afgelopen lente daadwerkelijk plaats in het commerciële centrum van Auckland te Nieuw-Zeeland en duurde bijna twee maanden. Soortgelijke incidenten kunnen zich rond de millenniumovergang¹ op wereldwijde schaal herhalen; vrijwel alle maatschappelijke voorzieningen zijn immers afhankelijk van computergestuurde systemen. Dit voorbeeld toont aan dat een beperkte benadering van het millenniumprobleem niet volstaat. U zult er terdege rekening mee moeten houden dat er zich, ondanks alle reeds gedane millenniumspanningen, problemen zullen voordoen met bedrijfsondersteunende systemen of dat partijen waarvan uw organisatie in meerdere of mindere mate afhankelijk van is, zullen worden getroffen door millenniumproblemen.

Dit artikel wil het management ervan bewust maken dat er, naast eventuele lopende projecten voor het millenniumbestendig maken systemen voor Infor-

matie- en Communicatie Technologie (ICT) en naast eventuele bestaande Business Contingency Planning-activiteiten, een noodzaak bestaat voor het opstellen en uitvoeren van een specifiek contingencyplan voor de overgang naar het nieuwe millennium. Centraal hierbij staat de vraag waarom u zich, als manager (eind)verantwoordelijk voor ICT, zou voorbereiden op de mogelijkheid dat het toch mis gaat bij de millenniumovergang en op welke wijze u dit zou kunnen doen. Experts zeggen over contingencyplanning in het kader van de millenniumovergang:

- '... the only surviving organizations will be those that have adopted a full-scale contingency plan' ([Your98]);
- 'Even if you're 110% sure your systems will be ready for the date change, ...it's a good idea to have backup plans' ([Anth98]).

In dit artikel zal allereerst worden toegelicht wat risicomangement en Business Contingency Planning (BCP) inhouden. Vervolgens wordt de noodzaak voor Millennium Contingency Planning (MCP) toegelicht en wordt MCP gepositioneerd ten opzichte van BCP. Verder wordt aangegeven hoe een Millennium Contingencyplan kan worden gerealiseerd. Ten slotte is in de bijlage als toelichting een matrix opgenomen van risico's en mogelijke tegenmaatregelen/noodscenario's² in het kader van de millenniumovergang.

RISICOMANAGEMENT EN BUSINESS CONTINGENCY PLANNING

In veel organisaties neemt risicomangement een vooraanstaande plaats in. Riscicomangement probeert op gestructureerde wijze passende antwoorden te vinden op vragen over interne en externe³ risico's die een organisatie loopt. Na het in kaart brengen van deze risico's wordt door het topmanagement afgewogen welke risico's aanvaardbaar zijn en welke moeten worden afgedekt. Het volledig afdekken van alle risico's die een organisatie loopt is niet realiseerbaar en het toepassen van alle beschikbare tegenmaatregelen/noodscenario's is niet doelmatig uit kosten-batenoogpunt. Hierdoor dienen bewust bepaalde risico's te worden genomen en te worden geaccepteerd. Centraal bij deze keuze staat de strategische vraag ten aanzien van de doelen en prioriteiten van de organisatie. Als dit duidelijk is dan kan aan de operationele uitwerking van de beperking van deze risico's worden gedacht. Deze operationele uitwerking wordt Business Contingency Planning (BCP) genoemd. Adequaat risicomangement is geen eenmalige activiteit; bedrijfsrisico's en getroffen tegenmaatregelen/noodscenario's dienen periodiek te worden geëvalueerd op basis van veranderde externe en interne omstandigheden.

In het algemeen kan worden gesteld dat BCP tot doel heeft om voortzetting van bedrijfsactiviteiten bij een calamiteit⁴ mogelijk te maken. Tot de scope behoren zowel de primaire en de ondersteunende bedrijfsprocessen als de resources en interne en externe organisaties die deze processen mogelijk maken (bijvoorbeeld management, personeel en leveranciers). De belangrijkste activiteiten bij BCP zijn het realiseren van tegenmaatregelen/noodscenario's op basis van kosten-batensanalyses, het toezicht

houden op de status van deze tegenmaatregelen/noodscenario's en het testen en actueel houden hiervan. Hierbij dient afstemming plaats te vinden tussen BCP en risicomangement omtrent de doelen, risico's en strategie met betrekking tot het beperken van deze risico's. BCP draagt zorg voor de bewerkstelling van een optimale mix van tegenmaatregelen/noodscenario's voor de af te dekken risico's.

De risico's kunnen globaal worden onderverdeeld in:

- risico's met betrekking tot leveranciers van producten/diensten⁵, inclusief leveranciers van ondersteunende producten/diensten;
- risico's met betrekking tot afnemers van producten/diensten, inclusief maatschappelijk verkeer, autoriteiten, aandeelhouders, etc.;
- risico's met betrekking tot ICT-dienstverlening;
- risico's met betrekking tot facilitaire dienstverlening.

Tegenmaatregelen/noodscenario's (preventief of repressief) kunnen worden onderverdeeld naar hun aandachtsgebied. Een veel gehanteerde indeling is:

- continuïteit van bedrijfsprocessen:
 - alternatieve werkwijzen voor getroffen bedrijfsactiviteiten (bijvoorbeeld handmatige procedures),
 - beperking van de afhankelijkheid van individuele leveranciers,
 - beperking van het aandeel van belangrijke klanten in de totale bedrijfsomzet,
 - verzekeringen tegen bedrijfsschade en aansprakelijkheid,
 - bescherming van key-personeel,
 - noodcommunicatieplannen/persberichten;
- ICT-dienstverlening:
 - fysieke en logische toegangsbeveiliging,
 - ononderbroken stroomvoorziening,
 - dubbele uitvoering van belangrijke apparatuur of datacommunicatieverbindingen,
 - interne en externe uitwijk van ICT-dienstverlening;
- facilitaire dienstverlening:
 - ontruimingsplannen,
 - oefeningen met noodhulpdiensten,
 - tijdelijke alternatieve huisvesting,
 - noodvoorzieningen voor telefonie,
 - alternatieve stroomvoorziening.

WAAROM NOG MILLENNIUM CONTINGENCY PLANNING?

Millennium Contingency Planning (MCP) is de specifieke vorm van contingencyplanning waarbij de risicoanalyse en de tegenmaatregelen/noodscenario's concreet zijn gericht op de millenniumovergang. Het is dus een verbijzondering van contingencyplanning voor een specifieke en eenmalige bedreiging; de overgang naar het jaar 2000. De eenmaligheid van de bedreiging is een kenmerk waarmee MCP afwijkt van 'normale' contingencyplanning: de tegenmaatregelen/noodscenario's die worden genomen en de bijbehorende investeringen die deze tegenmaatregelen/noodscenario's vergen, zijn gericht op deze eenmalige gebeurtenis en zijn hierna in principe afgeschreven⁶.

1 Daar waar wordt gesproken van millenniumovergang, eeuwwisseling of 1 januari 2000 als datum voor het optreden van millenniumproblemen worden ook andere datums bedoeld die voor problemen kunnen zorgen. Het gaat hierbij met name om de eerst mogelijke datum, de zogenaamde 'first fail date', een datum die kan liggen voor 1 januari 2000.

2 Tegenmaatregelen hebben vaak een preventief karakter (het voorkomen van schade) en noodscenario's hebben een repressief karakter (schadebeperkend). Noodscenario's zijn meer beschrijvend van aard, waarbij wordt aangegeven hoe het alternatief in de praktijk kan functioneren. Ten aanzien van de millenniumproblematiek zijn (combinaties van) beide soorten op te nemen in een MCP.

3 Hierbij dient niet alleen te worden gedacht aan leveranciers en afnemers, maar ook aan bijvoorbeeld economische risico's, conflictdreiging en politieke risico's (die slecht beïnvloedbaar en sterk aan verandering onderhevig zijn).

4 Een calamiteit is een gebeurtenis (of samenstel van gebeurtenissen) die een zodanige verstoring van de betreffende processen tot gevolg heeft, dat de continuïteit van de bedrijfsvoering in gevaar komt.

5 Bedrijfsmiddelen die reeds binnen de organisatie aanwezig zijn vallen ook hieronder.

6 Vergelijk met het afsluiten van een schadeverzekering voor een bepaalde periode.

De noodzaak voor Millennium Contingency Planning

Het millenniumprobleem is één van de grootste bedrijfsproblemen waarmee de mensheid ooit te maken heeft gehad. Wereldwijd worden enorme investeringen gepleegd om uitval van geautomatiseerde systemen (zoals computersystemen, communicatiesystemen, systemen voor toegangsbeveiliging, procesautomatiseringssystemen en andere systemen met embedded software) te voorkomen. Veel bedrijven zijn (te) laat begonnen met deze activiteiten, een aantal bedrijven onderkent het gevaar nog steeds niet of nog onvoldoende.

Waarschijnlijk heeft het millenniumprobleem ook binnen uw organisatie een hoge prioriteit. Projecten om datumgevoelige systemen millenniumbestendig te maken zijn enige tijd geleden gestart, uw ICT-leveranciers hebben de millenniumbestendigheid van de door hen geleverde systemen en systeemcomponenten gegarandeerd en misschien hebt u zelfs verzekeringen afgesloten om eventuele bedrijfsschade te compenseren.

Maar bent u nu echt klaar om het nieuwe millennium in te gaan? De ervaring tot op heden leert dat zo'n 95 procent van de automatiseringsprojecten niet binnen de initieel geplande doorlooptijd wordt afgerond. Experts ([Jone97]) verwachten dat 10 tot 35 procent van de mogelijke millenniumproblemen niet tijdig zal zijn opgelost. Resources voor millenniumprojecten zijn op dit moment uitermate schaars. Weet u zeker dat u op tijd klaar bent? En als de projecten op tijd zijn afgerond, hebt u dan een absolute garantie dat al deze projecten ook daadwerkelijk succesvol zijn en millenniumbestendige producten/diensten hebben opgeleverd? Wie garandeert u dat uw leveranciers inderdaad in staat zijn geweest om millenniumbestendige producten te leveren? Hoe weet u zeker dat uw businesspartners (leveranciers en afnemers in de bedrijfsketen waarin uw organisatie zich bevindt) niet dusdanige millenniumproblemen zullen hebben dat zij hun verplichtingen niet kunnen nakomen? Als u twijfels hebt bij één van deze vragen, dan kan het de moeite waard zijn eens nader stil te staan bij de mogelijkheid dat zich ondanks alle inspanningen toch millenniumproblemen gaan voordoen: Millennium Contingency Planning. Ook MCP vergt kostbare resources die waarschijnlijk voor een deel aan bestaande millenniumprojecten moeten worden onttrokken. Toch biedt de investering in een Millennium Contingencyplan een aantal belangrijke voordelen:

- De afhankelijkheid van het welslagen van het eigen millenniumproject en van millenniumprojecten van andere organisaties wordt sterk vermindert. Gezien de mogelijk grote gevolgen van millenniumproblemen (een rechtstreekse bedreiging van de continuïteit van uw organisatie) is een dergelijke risicospreiding sterk aan te bevelen. Bestaande millenniumprojecten kennen de volgende risico's die een streven naar vermindering van afhankelijkheid rechtvaardigen:
- alle millenniumactiviteiten dienen te zijn afgerond vóór de eeuwwisseling (er is dus een keiharde deadline; uitloop van millenniumprojecten is desastreus);

Een MCP is een verbijzondering van contingencyplanning voor een specifieke en eenmalige bedreiging: de overgang naar het jaar 2000.

- er is doorgaans niet voldoende tijd en/of geld om alle problemen op tijd op te lossen (veel niet-bedrijfskritieke systemen zullen helemaal niet meer millenniumbestendig worden gemaakt);
- een aantal systemen van middelgroot belang zal vanwege de tijd niet meer adequaat kunnen worden getest (millenniumbestendigheid van deze systemen blijft hier een onzekere factor);
- een aantal bedrijfskritieke systemen zal toch nog fouten kunnen bevatten, zelfs na grondig testen (u kunt altijd voor verrassingen komen te staan).

- Het vooraf treffen van tegenmaatregelen/noodscenario's is doorgaans aanzienlijk goedkoper dan het treffen van tegenmaatregelen/noodscenario's na het optreden van problemen. In het licht van de verwachte resourceschaarste na de millenniumovergang is het de vraag of het treffen van tegenmaatregelen/noodscenario's achteraf überhaupt nog haalbaar is.

- Een adequate invulling van MCP zal in sommige gevallen door verzekeringsmaatschappijen als noodzakelijke voorwaarde worden gesteld voor het afdekken van eventuele schade door millenniumverzekeringen.

- Bestuurders van organisaties kunnen aansprakelijk worden gesteld als ze geen adequate maatregelen (inclusief MCP) hebben getroffen⁷ (in Nederland bijvoorbeeld bij faillissement). Een goede invulling van MCP kan dit aansprakelijkheidsrisico beperken.

Hiernaast heeft de millenniumovergang een aantal specifieke kenmerken die nadere aandacht voor MCP rechtvaardigen naast een eventueel reeds bestaand BCP-proces:

- De kans op incidenten neemt rond de millenniumovergang tijdelijk sterk toe.

- Er bestaat een aanzienlijk verhoogde kans dat verschillende incidenten tegelijkertijd optreden (zowel binnen de eigen organisatie als bij andere organisaties), waardoor de schaars beschikbare resources moeten worden verdeeld over de verschillende herstelactiviteiten en tegenmaatregelen/noodscenario's.

- Bepaalde terugvalmogelijkheden of tegenmaatregelen/noodscenario's zijn niet langer beschikbaar (een uitwijksysteem heeft zeer waarschijnlijk dezelfde millenniumproblemen als het originele productiesysteem, omdat het uitwijksysteem vrijwel altijd een exacte kopie is van het originele productiesysteem⁸; overeenkomsten met branchegeenoten voor wederzijdse uitwijk kunnen onbruikbaar zijn, omdat de andere partij eveneens is getroffen door het millenniumprobleem).

⁷ In sommige landen, zoals de Verenigde Staten, is het management wettelijk verplicht beschikking te hebben over een adequaat Millennium Contingencyplan.

⁸ Bijvoorbeeld in geval van uitval van de computer zal moeten worden uitgeweken naar een ander type computer, maar de vraag is dan of de betrokken software hierop is te draaien

De millenniumovergang heeft dus ten aanzien van BCP een aantal additionele problemen, waardoor MCP aanvullend op BCP dient te worden uitgevoerd en niet aan de aandacht mag ontsnappen. Als gevolg van de aanzienlijk verhoogde kans op het gelijktijdig optreden van incidenten, zal extra aandacht moeten worden gegeven aan het bestuurlijke traject van MCP, te weten coördinatie, besluitvormingstrajecten, verdeling van schaarse resources, testen en up-to-date houden van contingencyplannen en het inrichten van een crisiscentrum.

De keuze van geaccepteerde risico's dient onder de rechtstreekse verantwoordelijkheid van het topmanagement te vallen.

Gezien de beschikbare resources en de noodzaak om snel en adequaat te kunnen reageren zal de diepgang van het op te stellen Millennium Contingencyplan aanzienlijk dienen te zijn. Er zal immers weinig tijd zijn om uitgebreid na te denken over wat te doen in bepaalde situaties⁹, zeker gezien de verwachte gelijktijdigheid van de millenniumproblemen. Diverse alternatieve situaties dienen daarom met een grote diepgang te worden uitgewerkt in scenario's.

Alhoewel MCP-activiteiten en -tegenmaatregelen/noodscenario's in principe eenmalig zijn en louter zijn gericht op de millenniumovergang, kunnen de inzichten die tijdens de MCP-risicoanalyses zijn opgedaan en de tegenmaatregelen/noodscenario's die in het kader van MCP zijn genomen (voorzover nog bruikbaar) ook na de millenniumovergang nog een bijdrage leveren aan een verdere verbetering van het Business Contingencyplan.

Verantwoordelijkheid voor Millennium Contingency Planning

Bestaande millenniumprojecten zijn doorgaans technisch gefocust en veelal belegd binnen de ICT-organisatie. Wat nu als een millenniumproject faalt? Stel dat enkele van uw bedrijfskritieke informatiesystemen uitvallen, ondanks alle maatregelen die binnen de millenniumprojecten zijn genomen. Heeft u dan alternatieve ICT-leveranciers achter de hand en zijn deze daadwerkelijk beschikbaar in geval van calamiteiten? Heeft u handmatige noodprocedures opgesteld en extra personeel achter de hand, zodat u toch enige tijd door kunt werken zonder uw ICT-systemen? Heeft u overeenkomsten met externe dienstverleners of branchegeenoten voor het overnemen van (delen van) uitgevallen bedrijfsprocessen? Bovenstaande vragen in het kader van millenniumrisico's geven aan dat beslissingen rondom MCP dienen te worden genomen op het niveau van het topmanagement. De keuze van geaccepteerde risico's moet in overeenstemming zijn met de doelstellingen en het beleid van de organisatie en dient daarom onder de rechtstreekse verantwoordelijkheid van het topmanagement te vallen. MCP kan van een zodanig belang zijn voor het overleven van

uw organisatie na het jaar 2000 dat de verantwoordelijkheid hiervoor niet kan worden gedelegeerd.

STAPPENPLAN OM TE KOMEN TOT EEN MILLENNIUM CONTINGENCYPLAN

Het is moeilijk aan te geven welke incidenten of problemen zullen optreden in het kader van de millenniumproblematiek. In de bijlage is een aantal risico's opgenomen, waarbij zeker niet is gestreefd naar volledigheid. Doel van deze bijlage is de lezer bewust te maken van de diverse gebieden waar millenniumrisico's aanwezig en tegenmaatregelen/noodscenario's mogelijk zijn.

Gezien het feit dat elke organisatie in een andere situatie verkeert (verschillende en anders ingerichte en ondersteunde processen, andere risico-inschattingen, andere beschikbare budgetten, andere leveranciers en afnemers, ander personeel, ander gebouw en faciliteiten, etc.) is het onmogelijk een standaardplan te maken dat voor iedere organisatie direct toepasbaar is. Wel is het mogelijk via onderstaand stappenplan op een gestructureerde wijze te komen tot een evenwichtig Millennium Contingencyplan.

Elke organisatie dient voor zichzelf een specifiek plan op te stellen, aangezien elk bedrijf zijn specifieke kwetsbaarheden heeft. Deze paragraaf beschrijft globaal hoe een Millennium Contingencyplan tot stand kan worden gebracht, waarbij de volgende stappen worden onderscheiden:

- projectopzet;
- millennium-risicoanalyse;
- realisatie Millennium Contingencyplan;
- testen Millennium Contingencyplan.

Projectopzet

Nadat iemand van het topmanagement verantwoordelijk is gesteld voor het realiseren van het Millennium Contingencyplan kan formeel worden gestart met contingencyplanningsactiviteiten, te beginnen met de projectopzet. Activiteiten in deze stap zijn bijvoorbeeld:

- Stel per bedrijfsproces en ondersteunend proces de eigenaar vast die verantwoordelijk is voor de continuïteit van het proces. De proceseigenaar dient tevens zitting te nemen of zich te laten vertegenwoordigen in de op te zetten projectgroep.

- Zet een MCP-project op, benoem de projectgroepleden en stel de rollen en verantwoordelijkheden vast. De projectgroep dient een MCP-strategie te ontwikkelen, die vervolgens dient te worden vastgelegd, te worden gevalideerd door het topmanagement en te worden gecommuniceerd aan alle betrokkenen. Hierbij dient antwoord te worden gegeven op vragen als 'Wat is de verwachte omvang en het karakter van de calamiteiten?', 'Waarop dienen de schattingen te worden gebaseerd?' en 'Welke aannames en veronderstellingen worden gehanteerd, bijvoorbeeld ten aanzien van de overheid¹⁰, leveranciers, afnemers en de voortgang van het eigen millenniumproject?'

⁹ Haast je als je tijd hebt, dan heb je tijd als je haast hebt.

¹⁰ Men kan zich bijvoorbeeld afvragen of de regering alle noodaggregaten zal gaan vorderen voor gebruik voor algemeen nut.

– Stel alle processen vast waarvoor een continuïteitsoplossing noodzakelijk is, inclusief een score die aangeeft hoe lang het desbetreffende proces 'uit de lucht' mag zijn. Ontwikkel vervolgens in overleg met de verantwoordelijke topmanager en de diverse proceseigenaren een MCP-projectplan, inclusief mijlpalen en budgetten voor realisatie en het testen van de contingencyplannen.

– Analyseer de reeds bestaande (business) contingencyplannen. Hierbij dient rekening te worden gehouden met het feit dat enerzijds de veronderstellingen en aannames¹¹ over de kans op en de omvang en het karakter van de calamiteiten anders (kunnen) zijn en dat anderzijds een aanzienlijk aantal tegenmaatregelen/noodscenario's die in het Business Contingencyplan worden genoemd ook een millenniumprobleem hebben en dus niet (zonder) meer werken; alleen de bruikbare delen van het Business Contingencyplan kunnen in het Millennium Contingencyplan worden opgenomen. Indien mogelijk dienen de functionarissen die betrokken zijn geweest bij de opzet en actualisering van het Business Contingencyplan in de MCP-projectgroep te worden opgenomen.

– Implementeer kwaliteitborgingsmaatregelen, zoals wijze van vastlegging, rapportage, definities, richtlijnen, methoden, technieken en interne en externe audits op projectopzet en -resultaten.

Millennium risicoanalyse

In deze stap worden voornamelijk analyses uitgevoerd. Hierbij kan veelal gebruik worden gemaakt van reeds bestaand materiaal, zoals bestaande Business Contingencyplannen, door anderen onderkende risico's, service level agreements en vastleggingen van risico's ten aanzien van de ICT-infrastructuur. Activiteiten in deze stap zijn:

– Stel met de desbetreffende proceseigenaar voor ieder bedrijfsproces en ondersteunend proces het minimumniveau van productie en dienstverlening vast dat nog acceptabel is. Vervolgens kunnen de kritieke functies en resources voor de missie van de organisatie worden vastgesteld, inclusief de tijdsduur dat deze functies/resources kunnen worden gemist zonder dat de continuïteit van het desbetreffende proces wordt beïnvloed.

– Stel voor ieder onderkend proces vast welke millenniumincidenten er mogelijk zijn¹². Daarna dient voor ieder onderkend millenniumincident een risico- en impactanalyse¹³ te worden uitgevoerd, zonder rekening te houden met andere alternatieve werkwijzen¹⁴. Hierbij dient tevens per 'fail date' de waarschijnlijkheid te worden vastgesteld dat een functie/resource faalt als gevolg van millenniumproblemen.

– Stel per millenniumincident mogelijke tegenmaatregelen/noodscenario's vast. Hierbij dient minimaal aandacht te worden besteed aan de 'single points of failure'¹⁵ in de processen, de benodigde resources voor tegenmaatregelen/noodscenario's, kosten-batenanalyse van de tegenmaatregelen/noodscenario's, de benodigde tijd voor de ontwikkelingen ervan en de onderlinge afhankelijkheid¹⁶ ertussen.

Realisatie Millennium Contingencyplan

Nadat de mogelijke tegenmaatregelen/noodscenario's zijn vastgesteld, dienen in deze stap keuzen te worden gemaakt door de betrokken proceseigenaren ten aanzien van de opname van de tegenmaatregelen/noodscenario's in het Millennium Contingencyplan. De gemaakte keuzen dienen te worden goedgekeurd door het topmanagement. Naast het daadwerkelijk voorbereiden en realiseren van tegenmaatregelen/noodscenario's dient nog een aantal belangrijke activiteiten te worden uitgevoerd:

– Zet een crisiscentrum op dat zorg draagt voor onder andere de coördinatie, resourceplanning en samenstelling van teams, besluitvormingsprocedures, communicatie omtrent het probleem (zowel binnen de eigen organisatie als naar derden daarbuiten), ondersteuning van personeel, helpdeskactiviteiten en het registreren van gebeurtenissen, het monitoren van acties en het bewaken van de voortgang van contingencyactiviteiten.

– Stel procedures en verantwoordelijkheden op voor het monitoren van specifieke risico's, het detecteren¹⁷ van millenniumincidenten en het analyseren en identificeren van millenniumincidenten door de analyseteams, inclusief het beoordelen van de intensiteit¹⁸.

– Stel procedures¹⁹ en criteria op voor het afkondigen en activeren van contingencyplannen, inclusief de voorafgaande besluitvorming.

– Stel de rollen, verantwoordelijkheden en autorisaties van de gebruikersorganisatie²⁰ op, rekening houdend met de vaardigheden van het personeel.

– Stel een overzicht op van procedures voor het inlichten van personeel, businesspartners, autoriteiten en andere doelgroepen in geval van ernstige millenniumproblemen en voor de overgang naar contingencysituaties.

– Stel procedures en criteria op voor het terugkeren van de contingencysituatie naar de normale situatie, inclusief de maximale duur van de contingencysituatie (vóór welk moment dient een permanente oplossing te zijn geïmplementeerd), de wijze van testen van de terugkeer naar de normale situatie en beoordeling van de testresultaten, de wijze van herstarten/restoren van systemen (inclusief besluitvorming) en de wijze van corrigeren/restoren van corrupte/verloren gegevens.

Testen Millennium Contingencyplan

Nadat het Millennium Contingencyplan is opgesteld, dient te worden getest of de uitgewerkte tegenmaatregelen/noodscenario's daadwerkelijk in de praktijk werken. Activiteiten in deze stap zijn onder andere:

– Stel een testplan op om de verschillende contingencyplannen individueel en in samenhang te testen (niet alleen om de werking vast te stellen, maar ook om medewerkers te trainen in het overgaan op en werken in contingencysituaties).

– Bereid het testen van de noodscenario's goed voor, waarbij tijdig testteams dienen te worden aan-

11 Welke aannames doe je? Waar baseer je je schattingen op?

12 Zie de bijlage voor een aantal voorbeelden van risico's en de tegenmaatregelen/noodscenario's die mogelijk zijn.

13 Inclusief effecten als levensbedreigingen, bedreigingen van bezit, milieuvervuiling, missie niet gehaald, explosie, brand, vrijkomen van gif, mechanische problemen, externe verplichtingen, etc.

14 Immers, de alternatieve werkwijzen kunnen ook weer afhankelijk zijn van het millenniumprobleem. In deze stap is het zaak om in risico's te denken, niet in oplossingen.

15 Dit zijn componenten/systemen die bij storing/uitval leiden tot discontinuïteit van het te ondersteunen bedrijfsproces en waarvoor tegenmaatregelen/noodscenario's absoluut noodzakelijk zijn om binnen de toegestane tijd de beschikbaarheid van het bedrijfsproces te herstellen.

16 Met name voor wat betreft het gemeenschappelijk gebruik van bepaalde resources.

17 Hierbij wordt geconstateerd of er daadwerkelijk problemen zijn ontstaan.

18 Gericht op de analyse van de aard en omvang van het probleem en de vaststelling wat verantwoordelijk is voor de oorzaak.

19 Inclusief wijze van besluitvorming, triggers, benodigde gegevens en verantwoordelijkheden.

20 Met name indien deze anders zijn dan normaal.

Ir. M.B.J. van Goethem
Is werkzaam bij Pink Elephant
Finance als IT Management
Consultant en IT Auditor.
Zijn aandachtsgebied ligt momenteel hoofdzakelijk op het gebied van advisering en auditing met betrekking tot de inrichting van beheerprocessen binnen ICT-organisaties in de bank- en verzekeringssector.

Drs. K.H.G.J.M. Ho RA
Is bij KPMG EDP Auditors werkzaam als EDP Audit Manager. Zijn aandachtsgebied ligt momenteel primair op het gebied van advisering en auditing met betrekking tot de millenniumproblematiek, waarbij hij tevens verantwoordelijk is voor de productontwikkeling voor de millenniumdienstverlening van KPMG. Daarnaast heeft hij zich binnen de business unit Technical Auditing gespecialiseerd in advisering en auditing op het gebied van planning en beheersing van automatiseringsprojecten.

gesteld en tijdig afspraken dienen te worden gemaakt met betrokkenen. De tests dienen zich met name te richten op de effectiviteit van de tegenmaatregelen/noodsenario's. Tijdens de uitvoering van de tests dienen de gebeurtenissen, besluiten en acties nauwkeurig te worden geregistreerd.

– Pas het Millennium Contingencyplan aan naar aanleiding van nieuwe inzichten en de testresultaten (eventueel hertesten). Nadat alle tests succesvol zijn afgerond, dient het Millennium Contingencyplan te worden gevalideerd door het topmanagement.

– (Laat) audits uitvoeren op de projectopzet en -resultaten en de actualiteit van het Millennium Contingencyplan.

CONCLUSIE

Nu de millenniumovergang nadert en organisaties sterk in beslag worden genomen door hun 'normale' millenniumprojecten wordt het steeds belangrijker om stil te staan bij het risico dat uw millenniumprojectorganisatie of andere interne of externe partijen niet tijdig slagen in het millenniumbestendig maken van de producten of diensten in kwestie. De

tijd dringt; tijdens de millenniumovergang zelf is het te laat om hierover na te denken. Het verdient aanbeveling om niet alle kaarten in te zetten op het millenniumbestendig maken van uw bedrijf, toeleveranciers en afnemers, maar om tevens terdege rekening te houden met het 'falen' van de desbetreffende activiteiten.

Een goede opzet van MCP is essentieel om te kunnen overleven bij het daadwerkelijk optreden van millenniumproblemen, zowel binnen de organisatie zelf als binnen de keten waarin de organisatie opereert.

LITERATUUR

[Chaa97] M. Chaabouni, *A Framework for Testing Year 2000 Application Conversions*, juli 1997, <http://www.year2000.com>.

[Your98] E. Yourdon, *Computer World Special Report Year 2000 'When disaster strikes'*, 1998.

[Anth98] G.H. Anthes, *Computer World Special Report Year 2000 'When disaster strikes'*, 1998.

[Jone97] C. Jones, *Contingency planning for the Year 2000 software problem*, 5 December 1997.

BIJLAGE

In deze bijlage is een aantal risico's aangegeven, aangevuld met mogelijke tegenmaatregelen/noodsenario's die in het Millennium Contingencyplan kunnen worden opgenomen. Het doel hiervan is de lezer attent te maken op mogelijke 'gaten' in zijn/haar risicoanalyses en tegenmaatregelen/noodsenario's; volledigheid is dus niet nagestreefd.

Risico's	Tegenmaatregelen/noodsenario's op het vlak van continuïteit van bedrijfsprocessen	Tegenmaatregelen/noodsenario's op het vlak van ICT-dienstverlening	Tegenmaatregelen/noodsenario's op het vlak van facilitaire dienstverlening
Leveranciers van producten/diensten²¹:			
– leverancier kan geen of alleen met vertraging grondstoffen/halffabrikaten leveren	– afhankelijkheid van individuele leveranciers verminderen – extra voorraden aanleggen (inclusief financiering en effecten op de jaarrekening) – voorkeur geven aan betrouwbare leveranciers (op basis van het vragen en krijgen van een garantie of millenniumcertificaat)	n.v.t.	– opslagruimte voor extra voorraden regelen
– leverancier kan geen millenniumbestendige ICT-producten meer leveren	n.v.t.	– afhankelijkheid van individuele leveranciers verminderen – alleen millenniumbestendige componenten/systemen aanschaffen van andere leveranciers	n.v.t.
– wegvallen milieubeheersingsmaatregelen	– treed in overleg met de autoriteiten – zet het productieproces stil – sla afval op in plaats van lozen	n.v.t.	n.v.t.
– tekort aan human resources na millenniumovergang: • doordat binnen de eigen organisatie meerdere millenniumproblemen tegelijkertijd optreden en voor het oplossen van de problemen en het uitvoeren van contingencymaatregelen	– capaciteit reserveren bij uitzendbureau (met leveringsgarantie) – tijdelijk extra personeel aannemen – overwerkregeling maken – beschikbaarheid personeel rondom millenniumovergang regelen tijdens normale werktijden – nieuwjaarsfeestje organiseren op	– capaciteit reserveren bij softwarewarehouse (met leveringsgarantie) – tijdelijk extra ICT-personeel aannemen – overwerkregeling maken – beschikbaarheid ICT-personeel rondom millenniumover-	– extra werkplekken regelen, inclusief faciliteiten

<i>Risico's</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van continuïteit van bedrijfsprocessen</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van ICT-dienstverlening</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van facilitaire dienstverlening</i>
<p>gelen beroep wordt gedaan op dezelfde human resources</p> <ul style="list-style-type: none"> • doordat vele organisaties millenniumproblemen krijgen en een beroep doen op dezelfde externe human resources 	<p>het bedrijfsterrein en aanwezigheid verplicht stellen</p>	<p>gang regelen (stand-by)</p>	
<p>– vervoersdiensten vallen uit</p>	<p>– voorraden aanleggen</p>		<p>– extra opslagcapaciteit regelen (met leveringsgarantie)</p> <p>– alternatief vervoer regelen:</p> <ul style="list-style-type: none"> – personeel – aanvoer grondstoffen
<p>– geleverde machines vallen uit (embedded software)</p>	<p>– betrouwbare millenniumbestendige leveranciers selecteren</p> <p>– garanties vragen</p> <p>– overwegen van het vervangen van niet-gegarandeerde apparatuur</p> <p>– extra voorraden eindproduct aanleggen</p> <p>– alternatieve productiemethoden ontwikkelen</p>	<p>n.v.t.</p>	<p>– extra opslagcapaciteit regelen (met leveringsgarantie)</p> <p>– betrouwbare millenniumbestendige leveranciers selecteren</p> <p>– garanties vragen</p> <p>– overwegen van het vervangen van niet-gegarandeerde apparatuur</p>
<p>– leverancier eist schadevergoeding indien niet wordt afgenomen conform contract</p>	<p>– contractueel afdichten</p> <p>– afsluiten verzekering</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
Afneemers²²			
<p>– afnemer kan niet of slechts gedeeltelijk afnemen</p>	<p>– afhankelijkheid van individuele afnemers verminderen</p> <p>– betrouwbare millenniumbestendige afnemers bevoordelen</p> <p>– afsluiten verzekering</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– afnemer krijgt liquiditeitsproblemen of gaat failliet</p>	<p>– bankgaranties vragen</p> <p>– kredietverzekering afsluiten</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– niet nakomen van wettelijke verplichtingen ten aanzien van milieu</p>	<p>– in overleg treden met autoriteiten</p> <p>– zuiveringsinstallaties aanbrengen</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– niet nakomen van wettelijke verplichtingen ten aanzien van arbeidsomstandigheden</p>	<p>– in overleg treden met betrokken instanties als autoriteiten en ondernemingsraad</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– vervoersdiensten vallen uit</p>	<p>– afnemer ertoe bewegen extra voorraden aan te leggen</p>	<p>n.v.t.</p>	<p>– alternatief vervoer regelen</p>
<p>– eigen producten/diensten zijn niet millenniumbestendig</p>	<p>– aansprakelijkheid uitsluiten</p> <p>– dossier opbouwen dat al het mogelijke is gedaan om de millenniumbestendigheid te waarborgen</p> <p>– afsluiten van aansprakelijkheidsverzekering</p> <p>– alternatieve producten/ diensten leveren</p> <p>– fusie²³ overwegen met millenniumbestendige partner</p> <p>– afstoten bedrijfsactiviteiten</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– afnemer eist schadevergoeding</p>	<p>– contractueel afdichten</p> <p>– afsluiten verzekering</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
<p>– afbreuk imago</p>	<p>– opstellen communicatieplan rekening houdend met verschillende doelgroepen als aandeelhouders, werknemers, autoriteiten, leveranciers en afnemers</p>	<p>n.v.t.</p>	<p>n.v.t.</p>
ICT-producten en -diensten			
<p>– kritiek systeem valt uit (zowel interne als externe provider) of belangrijke gegevens gaan verloren</p>	<p>– kritieke runs draaien vóór de fail date</p> <p>– handmatige procedures opzetten</p> <p>– alternatieve ICT-organisatie inschakelen</p>	<p>– alternatief systeem inschakelen</p> <p>– datumgevoelige functionaliteit uitschakelen</p>	<p>– extra personeel inzetten</p> <p>– extra papier regelen</p> <p>– extra werkplekken regelen, inclusief faciliteiten</p>

<i>Risico's</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van continuïteit van bedrijfsprocessen</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van ICT-dienstverlening</i>	<i>Tegenmaatregelen/noodscenario's op het vlak van facilitaire dienstverlening</i>
	– fusie overwegen met millenniumbestendige partner	– van belangrijke gegevens vooraf een hardcopy maken	
– performance van een kritiek systeem is te laag	– handmatige procedures opzetten – alternatieve ICT-organisatie inschakelen	– uitbreiden ICT-capaciteit (capaciteit zelf kopen of huren bij een derde (in het laatste geval met leveringsgarantie))	n.v.t.
– het telefoonverkeer is niet meer mogelijk		– realiseer Internet-aansluiting	– realiseer radiografische verbindingen
– het Internet is niet meer beschikbaar	– communiceer alternatieve bereikbaarheid	– n.v.t.	– breid de telefooncentrale uit om communicatie in stand te houden
– millenniumproject dreigt uit te lopen	– continue analyse van voortgang en haalbaarheid projecten – functionaliteit beperken – bedrijfsprocessen minder afhankelijk maken van functionaliteit van het desbetreffende systeem – identificatiemechanisme regelen voor mislukkende projecten	– extra capaciteit inhuren – alternatief scenario inzetten (bijvoorbeeld fixing van oude programmatuur)	– faciliteiten minder afhankelijk maken van functionaliteit van het desbetreffende systeem
– gegevensverwerking is onbetrouwbaar	– detectiemechanisme in werking stellen – bepalen welke gegevens welke mate van onbetrouwbaarheid toelaten	n.v.t.	n.v.t.
– logische toegangsbeveiliging functioneert niet meer	n.v.t.	– overwegen logische toegangsbeveiliging uit te zetten – fysieke toegang tot werkstations beperken en bewaken	– extra beveiligingspersoneel inschakelen
– storing van interne/externe telecommunicatie	n.v.t.	– alternatieve communicatiekanalen regelen	n.v.t.
Facilities			
– eigen vervoer valt uit	– alternatieve vervoersorganisatie inschakelen	n.v.t.	– alternatief vervoer regelen
– kantine valt uit	n.v.t.	n.v.t.	– werknemers vragen lunchpakketten mee te nemen – alternatieve kantinefaciliteiten regelen
– lift loopt vast		n.v.t.	– inhuur kranen regelen om goederen te takelen
– schaarste aan voedingsmiddelen	n.v.t.	n.v.t.	– extra voorraden aanleggen, inclusief faciliteiten voor gekoelde opslag
– stroomvoorziening valt uit	n.v.t.	n.v.t.	– zorgen voor noodaggregaatvoorziening – uitwijken naar een locatie met stroom – noodverwarming/koeling regelen
– gasvoorziening valt uit	n.v.t.	n.v.t.	– noodvoorziening regelen – noodverwarming/koeling regelen
– toegangsbeveiliging en/of brandalarm functioneert niet meer	n.v.t.	n.v.t.	– bewakingsdienst inhuren – extra personeel inzetten – inbraak- en brandalarm preventief uitschakelen

- 21 Niet alleen directe leveranciers vallen in deze categorie, maar ook werknemers en de bedrijfsactiva die tijdens de millenniumovergang in gebruik of op voorraad zijn.
22 Niet alleen klanten worden als afnemers beschouwd, maar bijvoorbeeld ook het maatschappelijk verkeer, consumenten, autoriteiten, aandeelhouders en werknemers.
23 De mate waarin het millenniumprobleem adequaat is/wordt opgelost, kan van invloed zijn op de prijs/waarde van een organisatie.

Aansprakelijkheid van de softwareleverancier voor de millenniumbug

Mr P.P.J.L. Enneking en mr M. Seelt

Wanneer kan een afnemer, geconfronteerd met een millenniumbug in zijn software, zijn leverancier aansprakelijk stellen voor het niet nakomen van de leveringsovereenkomst? Dit artikel behandelt in drie delen de aansprakelijkstelling op grond van wanprestatie, waarbij wordt uitgegaan van de professionele afnemer.

INLEIDING

Op de vraag: 'De millenniumbug, wat is dat voor beest?', luidt het antwoord: 'De millenniumbug is een computerprobleem'. Programmeurs hebben vroeger, vooral om geheugenruimte te besparen, in veel programma's jaartallen alleen in de laatste twee cijfers genoteerd. Bij het bereiken van de 21ste eeuw¹ gaat dat mis. Het jaartal 00 wordt dan gezien als 1900. Dat kan gevolgen hebben variërend van het printen van verkeerde datums² tot het vastlopen van systemen.

Doordat vele processen met informatietechnologie (IT) werken, is het een probleem van iedereen. Overheidsinstellingen en bedrijven zijn voor hun bedrijfsvoering sterk afhankelijk van computers. Maar ook thuis kan bijvoorbeeld de telefoon, het gas of de elektriciteit uitvallen. Op straat kunnen de verlichting en stoplichten weigeren. Misschien stoppen zelfs auto's en treinen, want ook daarin zitten vaak datumgevoelige programma's.

Het is dan ook van belang dat het publieke en private management zich met dit grote probleem bezighouden. Volgens velen zijn eerst de technici aan de beurt en moeten juristen nog op de achtergrond blijven. 'We moeten voorrang geven aan de technici', zo zei minister-president Kok bij de oprichting van het Millennium Platform: 'Het Jaar 2000-probleem is geen project voor juristen.' Pas als de problemen zijn opgelost, is er tijd om te strijden over de vraag wie betalen moet.

Dat lijkt verstandig. Toch moet de jurist nu al veel werk doen. Hij moet nagaan of noodzakelijke aanpassingen van de systemen niet onder lopende onderhoudscontracten vallen. Verder kunnen auteursrechten in het geding zijn. Mag de afnemer wel aan de software (laten) sleutelen als de leverancier dat weigert, en kan hij daartoe de broncode opeisen? Ook een aansprakelijkheidsonderzoek is al nodig. In ieder geval moet de jurist bekijken of een vordering op de soft- of hardwareleverancier kan verjaren en hoe dat te voorkomen is. Als de leverancier hulp weigert, is er bovendien geen reden om met hardere acties te wachten. Los daarvan is kennis over de slaagkans van een aansprakelijkstelling van de leverancier wezenlijk voor de financiële planning van de afnemer en de leverancier. Bewijsmateriaal moet bovendien zo snel mogelijk worden veiliggesteld. Men kan dus niet vroeg genoeg beginnen een eventuele claim voor te bereiden.

Dit artikel spitst zich toe op de vraag wanneer de softwareleverancier aansprakelijk te stellen is voor het niet nakomen van de leveringsovereenkomst.

1 Eigenlijk wordt de 21ste eeuw pas bereikt in 2001. Dit komt doordat onze jaartelling is begonnen met het jaar 1 en niet met het jaar 0. Maar het feit dat de feesten voor het inluiden van het nieuwe millennium gepland zijn voor de overgang van 1999 naar het jaar 2000, geeft aan dat de meerderheid van de wereldbevolking ervan uit gaat dat het nieuwe millennium in het jaar 2000 start.

2 Het woord data wordt veel gebruikt voor gegevens. Om duidelijk aan te geven dat het meervoud van datum wordt bedoeld, zal daarvoor het Nederlandse woord datums worden gebruikt.

3 De gegevens waarmee een computer op een bepaald moment aan het werk is, worden opgeslagen in het werkgeheugen van de computer (ook wel RAM, random access memory, genoemd). Gegevens die niet direct worden gebruikt, worden vastgelegd op de harde schijf (hard-disk) van de computer, en als ze langere tijd niet nodig zijn kunnen ze ook worden opgeslagen op een tape of diskette.

4 Zo kostte een Megabyte harddiskruimte in 1996 10 dollarcent per maand om te leasen tegen 163 dollar in 1963 (met inflatiecorrectie komt dat op 10.600 dollar per jaar); Leon Kappleman en Phil Scott, 'Accrued savings of the Year 2000 Computer Date Problem', <http://www-lan.unt.edu/cobabak/www/bcis/faculty/kappelma/accrued.htm>.

5 Afkomstig van de website van Intel, [Http://intel.com](http://intel.com).

6 In de meeste PC's zit een real-time clock die tijd en datum bijhoudt, ook als de computer uit staat. Bij het opstarten geeft deze chip de datum en tijd door aan de BIOS, die het vervolgens weer doorgeeft aan de systeemsoftware. Met systeemdatum wordt meestal de datum bedoeld die de systeemsoftware weergeeft.

7 De meeste systeemklokken van oudere personal computers die in menige studentenkamer of gezinshuishouding nog te vinden zijn, zullen terugspringen naar 1980 of 1984. Nieuwere versies real-time clocks en BIOS'en springen naar 00, maar geven daarbij een eeuwwisselingsbit mee, waardoor aangepaste (systeem)programmatuur (o.a. DOS 6.2 of Windows 95) deze datums als horende bij de volgende eeuw beschouwt. Ed Baars, 'Tijd', *Computer Totaal* 1998, 1.

Figuur 1.
Elke anderhalf jaar verdubbelde het aantal schakelingen op een Intel-chip.

PROBLEMEN VAN DE BUG

In deze introducerende paragraaf komen aspecten van oorzaak, gevolgen en oplossingen aan de orde.

Hoe konden die programmeurs zo stom zijn?

Ze konden toch zien aankomen dat het fout zou gaan? Stom was het vroeger allerminst dat ze jaartallen in twee cijfers noteerden, want de pioniers moesten zich in het begin in allerlei bochten wringen om met hun programma's zo min mogelijk werkgeheugen en opslagcapaciteit³ te gebruiken. De prijzen waren daar namelijk naar.⁴ Door bij een datum steeds twee geheugenposities te sparen won de programmeur 25 procent ruimte per opgeslagen datum. ('ddmmjj' in plaats van 'ddmmjjjj')

Het leek onwaarschijnlijk dat men bij de eeuwwisseling nog programma's uit de beginjaren zou gebruiken want door de snelle ontwikkelingen in de computerindustrie hadden computers, programma's en zelfs programmeertalen maar een korte (economische) levensduur. Het aantal schakelingen op een chip verdubbelde iedere twee jaar. Figuur 1 geeft de processorontwikkeling van Intel-chips weer.⁵ Dat dwingt bedrijven om hun computers na een paar jaar te vervangen. Vaak stappen ze daarbij over op nieuwe (versies van) programma's.

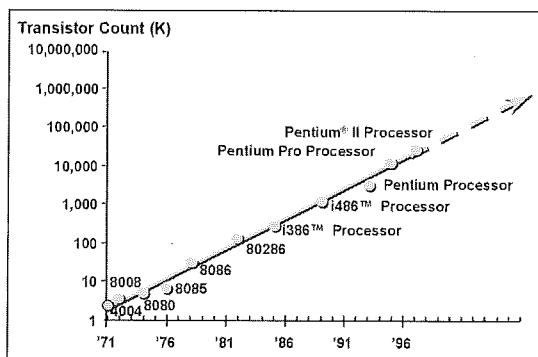
Andere argumenten voor het weglaten van de eeuwaanduiding waren:

- de tweecijferige jaaraanduiding sluit aan bij het spraakgebruik;
- met twee cijfers passen meer gegevens tegelijk op een beeldscherm, en bij het printen wordt papier bespaard;
- het scheelt twee toetsaanslagen per datum;
- computers kunnen onderling sneller gegevens uitwisselen.

In de volgende decennia werd het gebruik van twee posities voor de jaaraanduiding daarom standaard, vaak ook in nieuwe programmeertalen en in hardware. Zo hielden (en houden soms nog steeds) de real-time clocks⁶ van computers de datum bij zonder eeuwaanduiding.⁷ De reden was vooral dat modernere programma's rekening moesten houden met de standaard omdat ze anders niet met oude software en gegevens overweg konden.

Wat gaat er door de bug mis in de software?

Het grootste probleem is dat de gegevens niet meer kloppen. Dat is nog gevaarlijker dan wanneer de



software helemaal niet meer werkt, want in dat geval merkt men dat meteen.

Voorbeelden

Bij berekeningen met tweecijferige jaartallen kunnen nog méér fouten worden gegeneerd. Bijvoorbeeld als een leeftijd berekend wordt volgens:

Huidig jaar – Geboortjaar = Leeftijd

Als de beide jaren in deze eeuw liggen, is er geen probleem:

$$98 - 71 = 27$$

Maar na de millenniumwisseling gaat het met een notering in twee cijfers fout:

$$00 - 71 = -71$$

Het kan voorkomen dat het programma het minteken negeert en dan uitkomt op 71.

Bij het sorteren van gegevens zullen ook fouten optreden. Het jaartal 00 wordt dan gezien als 1900 en niet als 2000 en zal bij oplopend sorteren helemaal vooraan worden gezet.

Ook bij andere bewerkingen gaat het mis. Als de gebruiker in het jaar 2000 bijvoorbeeld opdracht geeft om alle bestanden van voor '98 te wissen, worden ook de bestanden van 2000 meegenomen want het jaar 00 ligt volgens de computer vóór het jaar '98.

Computergestuurde processen kunnen in de war raken. Bekend is het voorbeeld van een ingebouwde chip die bijhoudt wanneer het apparaat de laatste servicebeurt kreeg. Soms is de chip zo geprogrammeerd dat die het apparaat blokkeert als te veel tijd is verstreken sinds de laatste servicebeurt. Bij notering in twee cijfers is dan onvoorspelbaar wat er na de eeuwwisseling gebeurt.

Dan is er nog het schrikkeljaarprobleem. Voor schrikkeljaren gelden drie regels. De eerste is dat ieder jaar dat deelbaar is door 4 een schrikkeljaar is. De tweede is dat jaren deelbaar door 100 geen schrikkeljaar zijn, waarbij de eerste regel wordt genegeerd. De derde stelt dat een jaartal deelbaar door 400 toch een schrikkeljaar is. 1900 is dus geen schrikkeljaar, maar 2000 wel. Het kan zijn dat programmeurs deze regels niet correct toepasten. Bij het bepalen van de dag, week en het aantal dagen in een bepaald jaar gaat het dan na 29 februari 2000 mis.⁸

De bepaling van de dag van de week en de week van het jaar kan ook mislopen zonder schrikkeljaarprobleem. 1 januari was in 1900 een maandag en is in 2000 een zaterdag. Als de computer het jaar 00 behandelt als 1900 zal hij een verkeerde dag van de week kiezen. Programma's die in het weekend andere routines uitvoeren dan door de week raken dan van slag.

Deze fouten kunnen zich al voor 2000 voordoen want programma's kunnen nu al te maken krijgen met datums in het volgende millennium, bijvoorbeeld bij financiële planningen en bij het verwerken van houdbaarheids- en geldigheidsdatums. Een andere reden waarom het al vóór 2000 fout kan gaan, is dat veel programmeurs aan het jaartal 99 of de datum 9/9/99 een bijzondere betekenis toekenden, bijvoorbeeld dat het jaartal onbekend is. Dit kan betekenen dat gegevens met die datum niet correct worden behandeld. De programma's zouden dus eigenlijk op 1 januari 1999 al moeten zijn aangepast.

De gevolgen van de bug in de software

De mogelijke impact van de bug op de samenleving is zonder overdrijving enorm. Enkele voorbeelden. In de financiële sector gaat de administratie en communicatie van gegevens zoals banksaldi, aandelen-transacties, het elektronisch overboeken van tegoeden, renteberekeningen, etc. via computers. Bijna iedere transactie wordt voorzien van een datum en een tijd. Daar komt bij dat de financiële sector veel met nieuwe versies van oude programma's werkt, die het jaar nog steeds in twee cijfers aangeven.⁹ De eerste problemen deden zich al voor. Betaalautomaten herkennen bankpassen en creditcards met een geldigheidsdatum van 2000 of later niet, of namen die in omdat de kaarten verlopen zouden zijn.

Ook veel productieprocessen werken met chips die op vaste tijdstippen meetgegevens doorgeven en met computers die het productieproces sturen. Wat er gebeurt als zo'n systeem zich in een datum verslijkt bleek eind 1996 bij twee aluminiumsmelterijen in Nieuw-Zeeland en Australië. Dat jaar was een schrikkeljaar en telde dus 366 dagen. Maar de computer, die het smeltproces stuurde, hield daar geen rekening mee en liep vast. Het smeltproces stopte en het aluminium stelde in de buizen. Schade circa 1,5 miljoen gulden.¹⁰

Er staan ook mensenlevens op het spel. In ziekenhuizen is veel apparatuur die datum en tijd bijhoudt. Patiënten zijn daarvan afhankelijk. Dat kan fataal zijn.

Wat is eraan te doen?

Op zich verschilt de millenniumbug niet veel van andere bugs in maatwerkprogramma's en standaardpakketten. Voor grotere (maatwerk)pakketten worden doorgaans onderhoudscontracten overeengekomen om de software van eventuele bugs te ontdoen. Voor kleine pakketsoftware stellen leveranciers regelmatig zogenaamde patches, updates of fixes beschikbaar: kleine programma's die eerder geleverde software ontdoen van bugs en soms kleine verbeteringen aanbrengen. Ze worden vaak gratis verspreid via Internet of naar geregistreerde gebruikers gestuurd.

De millenniumbug is ook relatief gemakkelijk te vinden en op te lossen. Het gaat om plaatsen met datumvelden. Verder bevatten veel computertalen standaardprocedures om datums te bewerken. Voor het vinden van de bug zijn speciale softwaretools ontwikkeld.¹¹

Het oplossen van de bug is geen 'rocket-science'. De twee meest genoemde manieren zijn 'windowing' en 'date-expansion'. Het laatste ligt het meest voor de hand, namelijk het alsnog toevoegen van twee velden. Daarmee is het probleem compleet opgelost zonder het systeem te vertragen.

Bij windowing blijven de tweecijferige verwerking en opslag van het jaartal bestaan. Maar zodra datums worden verwerkt bepaalt de software de eeuw van het jaartal door te kijken of de desbetreffende dag vóór of ná een bepaald breekjaar valt. Als bijvoorbeeld geen datums van vóór 1960 zijn verwerkt kunnen jaren onder de 60 aan de volgende eeuw worden toegekend, en jaartallen daarboven aan

De millenniumbug verschilt op zich niet veel van andere bugs in maatwerkprogramma's en standaardpakketten.

déze eeuw. Zolang de te verwerken datums binnen de honderdjarige 'window' tussen 1960 en 2060 liggen is er geen probleem. Toekomstige complicaties kan de programmeur voorkomen door elk jaar het raam, en dus het breekjaar, een jaar op te schuiven. Oude datums moeten dan wel op tijd uit het systeem worden verwijderd om geen problemen te krijgen met het begin van de 'window'.

Windowing wordt waarschijnlijk het meest toegepast, want bij date expansion moeten aanwezige gegevens worden omgezet en dat is extra werk. Bovendien moet een al aangepast programma kunnen werken met programma's die nog niet verbeterd zijn, want vaak kan niet alles tegelijk worden aangepakt. Het bedrijf zou dan te lang stilliggen. Daarom moeten brugprogramma's worden geschreven tussen aangepaste en nog niet aangepaste programma's en gegevens, zodat goede communicatie mogelijk blijft. Deze brugprogramma's moeten na de operatie weer worden verwijderd. Voor al die stappen ontbreekt het aan de cruciale factor: tijd.

Een millenniumproject is een race tegen de klok met als inzet de continuïteit van het bedrijf:

- De komst van de volgende eeuw kan niet worden uitgesteld. Het is een deadline waar niet met een boete, lagere prijs of excuses aan te ontkomen valt.
- Het is een mondiaal probleem waardoor IT-diensten en -personeel steeds schaarser en duurder worden, met name voor oudere programmeertalen en het aanpassen en testen van programma's.
- Alles moet worden gecontroleerd, maar omdat de bedrijfsvoering doorgaans niet toelaat dat alles tegelijk wordt gedaan, moet het millenniumproject gefaseerd worden aangepakt.

Ook los van het tijdsaspect is de millenniumbug moeilijker op te lossen en duurder dan een gemiddelde 'bug'.

- Deze verhoogde moeilijkheidsgraad komt door het feit dat het programma met de bug al op de werkvloer wordt gebruikt, wat aanpassen bemoeilijkt.
- Verder komen datum-routines vaak voor in programma's. Bijna iedere code moet worden nagezien.
- De bug komt vooral in oudere programma's voor, wat de volgende problemen oplevert:
 - weinig beheersen nog de oude programmeertalen;
 - de kennis over wat de programma's doen en hoe ze werken, is niet meer aanwezig;
 - documentatie is zoek, verouderd of nooit gemaakt;
 - de broncode¹² van het programma is niet (compleet) aanwezig¹³,

8 Een voorproefje hiervan kreeg de Belgische beurs die in 1996 enige tijd stillag omdat de software 1996 niet als schrikkeljaar herkende; zie <http://www.fenit.nl/2000/probleem.html#Wat> is het probleem.

9 Zie bijvoorbeeld het artikel 'ING worstelt met Jaar 2000-project', *Computable*, 16 januari 1998, p. 1, waarin wordt beschreven hoeveel moeite het ING kost om de millenniumbugs uit zijn systemen te krijgen die in de oude delen van zijn programmatuur zitten verstoort.

10 A. van Deursen en P. Klint, 'Het jaar-2000-probleem', *Computerecht* 1997/6, p. 266-271.

11 Maar echt volautomatisch zal het zoeken nooit kunnen gaan. Sommige programmeurs gebruiken namelijk voor hun variabelen fantasienamen, zoals die van hun kinderen of van favoriete popsterren.

12 De broncode (ofwel source code) is de vorm waarin programma's worden geschreven. Mensen kunnen die nog direct lezen doordat begrijpelijke commando's worden gebruikt. Deze code moet worden omgezet in objectcode (een serie nullen en enen) waarmee de computer kan werken.

13 Soms kan men nog het programma decompileren (de source code reconstrueren uitgaande van het gecompileerde programma). Maar dat is moeilijk. Van worst is ook geen varken meer te maken, aldus Pagrach in 1991. H. van Steenis, *Sybox Interactief Woordenboek Informatica* (CD-Rom), Soest 1995.

De kosten van het oplossen van de bug zijn maar een fractie van de schade die de bug kan aanrichten.

- compilers¹⁴ voor het programma zijn niet meer aanwezig;
- oudere programma's worden in de loop der jaren onderhouden door er telkens stukjes aan te plakken. Dat noemt men wel 'spaghetti programming', omdat een schema van de handelingen die het programma uitvoert er uitziet als spaghetti en onhandelbaar wordt.

14 Een compiler compileert de broncode tot objectcode (zie ook noot 12).

15 Als ze het al onderkennen. Uit onderzoek van Moret Ernst & Young en de VU in Amsterdam naar de effectiviteit en efficiency van de financieel-economische functie van industriële bedrijven in Nederland blijkt dat begin 1998 20 procent van de Nederlandse bedrijven nog niet gestart is met een millenniumproject (nieuwsbericht 20 mei 1998 op de site van het Millennium Platform, <http://www.mp2000.nl>).

16 Het nieuw BW spreekt van 'tekortkoming in de nakoming' (art. 6:74 lid 1 BW). De term wanprestatie is echter nog steeds courant in het juridische taalgebruik en voor veel niet-juristen een bekende term. In dit artikel zullen beide termen naast elkaar gebruikt worden.

17 Zie voor andere gronden waarop de leverancier aansprakelijk gesteld kan worden W.F.R. Rinzema, 'Is het Nederlandse recht millenniumproof?', *Computerrecht* 1997/6, p. 289-298.

18 Rb Den Haag 26 maart 1986, *Computerrecht* 1986/3, p. 185.

19 Zie over dit en andere typen automatiseringscontracten nader C. Stuurman, 'Computercontracten', in: H. Franken, H.W.K. Kasperen en A.H. de Wild (red.), *Recht en Computer*, serie recht en praktijk nr. 36, Deventer 1997, pp. 74-102.

20 Op dit onderscheid gaat de subparagraaf 'Wat mag de afnemer van software in het algemeen verwachten?' van deze paragraaf nader in.

Ogenschijnlijk is de millenniumbug een gewone bug, maar het verwijderen ervan kost veel meer tijd en geld. En doordat de hele wereld dezelfde deadline heeft zijn de kosten extra hoog.

Wie moet dat betalen?

De meeste bedrijven zijn vooral bezig het probleem tijdig op te lossen en niet met wie het betalen moet.¹⁵ De kosten van het oplossen zijn ook maar een fractie van de schade die de bug kan aanrichten. Daarom praten bedrijven met hun leveranciers nu over oplossingen en niet over schuld. De leverancier kan de bug vaak het best repareren. Hij weet het meeste over de programma's en is vaak de enige die de broncode heeft. Toch is onderzoek naar de mogelijkheden om de leverancier aansprakelijk te stellen nu al geboden.

Er zijn in ons rechtsstelsel diverse juridische gronden waarop de leverancier kan worden aangesproken: wanprestatie¹⁶, onrechtmatige daad en (soms) productaansprakelijkheid. Verder kan met de leverancier een onderhoudsovereenkomst zijn aangegaan die hem misschien verplicht de millenniumbug te verwijderen. Dit artikel behandelt alleen de mogelijkheid de softwareleverancier aansprakelijk te stellen op grond van wanprestatie.¹⁷ Daarbij wordt uitgegaan van een professionele afnemer en niet ingegaan op het consumentenrecht.

In het volgende zal een mogelijke claim op grond van wanprestatie in drie delen behandeld worden. Het eerste deel gaat over vragen die bij ieder onderzoek naar mogelijke wanprestatie van een softwareleverancier kunnen spelen. Het tweede over de invloed op de claim van het feit dat de millenniumbug pas na enige tijd na de levering van de software de functionaliteit ervan aantast. Wanneer is er dan sprake van een wanprestatie? En in het derde deel wordt behandeld hoe haalbaar een millenniumclaim op grond van wanprestatie is.

WANPRESTATIE BIJ SOFTWARE-LEVERING: ALGEMENE VRAGEN

Voordat goede studie van de aansprakelijkheid van de softwareleverancier voor de millenniumbug door wanprestatie mogelijk is, moet eerst het feitelijk en juridische kader helder zijn waarin leverancier en afnemer opereren. Logisch is dat de juridische kwalificatie van softwareleveranties en de bepaling

van de rechten en plichten van partijen in dit verband vastliggen in de wet en jurisprudentie. Maar zo ver is het nog niet.

Eén van de oorzaken daarvan is dat software niet goed past in het huidige juridische begrippenkader. Het algemene vermogensrecht kent alleen zaken en vermogensrechten. Ook regelingen in het BW, zoals de productaansprakelijkheid bij een koopovereenkomst, gebruiken het zaakbegrip voor de afbakening van hun werkingsterrein. Maar niet duidelijk is of software een zaak is in de zin van het wettelijk gedefinieerde begrip. Men kan zich afvragen of sommige regelingen, los van de vraag of software al of niet een zaak is, toch (naar analogie) van toepassing (dienen te) zijn op softwareleveringen.

Een ander probleem is dat software op totaal verschillende manieren geleverd kan worden. Belangrijk is het onderscheid tussen maatwerksoftware en standaardsoftware.

Deze paragraaf schetst het algemene juridische kader voor softwareleveranties, met name die aspecten die van belang kunnen zijn om de aansprakelijkheid te bepalen voor de millenniumbug door een wanprestatie van de leverancier. Aan de orde komen:

- hoe software feitelijk en juridisch geleverd wordt;
- wat de afnemer doorgaans van de software mag verwachten en of bij de bepaling daarvan het conformiteitsbeginsel van artikel 7:17 BW een rol speelt;
- of een softwareleverantieovereenkomst een inspannings- of een resultaatverbintenis is.

De feitelijke verhouding tussen afnemer en softwareleverancier

Om de relatie tussen afnemer en leverancier te bepalen is het belangrijk de levering van maatwerksoftware te onderscheiden van die standaardsoftware. Leveranciers ontwikkelen op eigen initiatief standaardpakketten die ze vaak aan meerdere afnemers verkopen, bijvoorbeeld tekstverwerkingspakketten als Word en WordPerfect. Bij maatwerksoftware krijgt de afnemer speciaal gemaakte programma's. Vaak zijn daartoe bestaande softwarepakketten aangepast voor de afnemer, maar soms ontwikkelt de leverancier in nauw contact en in samenwerking met de afnemer nieuwe software. Van ontwerp tot ingebruikname van de software moet de afnemer duidelijk maken wat hij wil en de leverancier helpen een goede prestatie te leveren. Als de afnemer niet genoeg meewerkt, bijvoorbeeld door niet op tijd te zorgen voor voldoende geschoold personeel, dan is de schade die daardoor ontstaat voor zijn rekening, aldus de rechtbank van Den Haag in de zaak ICL/Blommestein.¹⁸ De overeenkomst die de levering van maatwerksoftware regelt heet ook wel een softwareontwikkelingsovereenkomst.¹⁹ Het lijkt dan meer op aanneming van werk of een opdracht, dan bij de aanschaf van een standaardpakket, wat meer gelijkenis met koopovereenkomst heeft.²⁰

Sommige softwareleveranties onderscheiden zich doordat daarbij ook andere automatiseringsproducten worden verkocht, bijvoorbeeld computers waarop de programmatuur moet draaien en machines

die aangestuurd worden. Een bijzondere vorm hiervan is de zogenaamde 'turnkey'-overeenkomst waarbij de afnemer de realisatie van het op te leveren systeem uitbesteedt en als het ware alleen maar de sleutel hoeft om te draaien om over het automatiseringssysteem te beschikken.

Daarnaast komt het vaak voor dat de softwareleverancier ook de automatiseringsadviseur is. Hij kan dan stappen voorstellen om de bedrijfsvoering te automatiseren, waarna hij die adviezen al dan niet, of ten dele, zelf uitvoert.

De relatie tussen afnemer en leverancier kan dus sterk verschillen en variëren van zeer nauw tot zeer los. Bij maatwerksoftware is de relatie veel nauwer dan bij standaardpakketten. Als de leverancier adviseert over software is de relatie ook nauwer. Als de leverancier naast de software ook andere automatiseringsproducten levert, dan is de relatie eveneens nauwer. Deze nauwheid van de relatie, dit wil zeggen de mate waarin de leverancier bekend is met de bedoeling van de afnemer met de software, beïnvloedt de aansprakelijkheid van de leverancier. Enkele uitspraken in conflicten over automatiseringsprojecten illustreren dat.

Voor de softwareleverancier annex adviseur is het arrest RBC/Brinkers²¹ wezenlijk. RBC was een automatiseringsadviseur die onder tijdsdruk een verkeerd advies gaf, waardoor de automatisering bij Brinkers mislukte en er veel schade ontstond. Hoewel de tijdsdruk was ontstaan doordat Brinkers spoed eiste en RBC bovendien erop had gewezen dat diepgaander onderzoek eigenlijk nodig was, ontlastte dat RBC niet. Als deskundig adviseur was het juist een hoofdverplichting van RBC om goed na te gaan aan welke eisen het automatiseringssysteem van Brinkers moest voldoen.²² Een softwareleverancier die ook als adviseur optreedt, is dus sneller aansprakelijk voor tekortkomingen van software in relatie tot de eisen van de bedrijfsvoering van de afnemer. Hij moet de eisen kennen, en daar rekening mee houden. Verder mogen afnemers sneller van hem verwachten dat hij meedeelt dat de geleverde software niet aan de eisen voldoet. De volgende paragraaf gaat dieper in op de mededelingsplicht.

Als de softwareleverancier ook hardware levert of bepaalde hardware voorschrijft dan kan het zijn dat hij door de onderlinge afhankelijkheid tussen software en hardware moet instaan voor de compatibiliteit. Hij weet immers dat de afnemer beide componenten met elkaar wil gebruiken. Een voorbeeld is een arrest van het Hof van Den Bosch²³ waarin wanprestatie van een softwareleverancier werd aangenomen omdat die een programma had geleverd voor een bepaald type computer zonder te melden dat het programma niet goed samenwerkt met het standaardbesturingssysteem van die computer.

Als de softwareleverancier ook hardware levert of voorschrijft is een ander aansprakelijkheidsrisico dat bij gebrekkige levering van één van beide sprake kan zijn van een wanprestatie voor de hele overeenkomst. In de zaak Bazuin en Glimmerveen tegen XTEC²⁴ bijvoorbeeld werd voor f 351.500 hardware geleverd en voor f 248.500 software ontwikkeld. De softwareontwikkeling liep mis onder andere doordat een onderaannemer failliet ging. Omdat het om een essentieel onderdeel van de overeenkomst ging

werd die helemaal en niet alleen voor de softwareontwikkeling ontbonden wegens wanprestatie.

Dit verband tussen enerzijds de mate waarin de softwareleverancier betrokken en bekend is met de automatiseringseisen van het bedrijf van de afnemer en anderzijds met de aansprakelijkheid van de leverancier kan belangrijk zijn bij millenniaansprakelijkheid. Argumenten als 'de fout zit niet in mijn software, maar in de manier waarop de hardware of andere programma's met de datums omgaan' verliezen aan waarde als er sprake is van een nauwe relatie. De afnemer kan dan namelijk stellen dat de leverancier op de hoogte was van de hard- en softwareomgeving waarin de geleverde software moest functioneren en dat hij daarmee rekening houdt.

De nauwheid van de relatie speelt ook een rol bij de vraag of de leverancier een mededelingsplicht heeft geschonden door de afnemer niet te wijzen op de aanwezige millenniumbug. Hij kan bij een nauwe relatie bijvoorbeeld constateren dat de afnemer de programmatuur nog zal gebruiken als de te verwerken jaartallen problematisch worden.

De mate waarin leverancier en afnemer met elkaar samenwerken, kan belangrijk zijn voor het bepalen van de millenniaansprakelijkheid.

Voorals als de leverancier ook de adviseur is, kan de nauwe relatie hem verplichten om de afnemer op millenniumbugs te wijzen in de hard- en software van andere leveranciers waarmee programmatuur die hij zelf levert moet samenwerken. Dit verzaken van een mededelingsplicht kan leiden tot gerechtvaardigde grotere verwachtingen van de afnemer. Hij mag er sneller van uitgaan dat het programma ook datums van na de eeuwwisseling kan verwerken als de leverancier wist dat dit de planning was en niet waarschuwde voor de millenniumbug. De volgende paragraaf gaat dieper in op de mededelings- en waarschuwingsplicht.

Overigens leidt een nauwere band tussen afnemer en leverancier niet altijd tot meer aansprakelijkheid van de leverancier. De afnemer kan onder omstandigheden grote invloed hebben op het succesvol ontwikkelen van software. Als hij dat bijvoorbeeld zelf coördineert en daar een softwareleverancier bij trekt, dan ligt de verantwoordelijkheid voor het juist omgaan met datums meer bij de afnemer, want hij bepaalt de manier van programmeren, houdt toezicht en draagt daarvoor de verantwoordelijkheid.

De juridische classificatie van software

Om het juridische kader waarin software wordt geleverd te schetsen, moet duidelijk zijn hoe software juridisch moet worden gekwalificeerd. De definitie van software van de World Intellectual Property Organization (WIPO) luidt:

Software may be either:

- 'a computer program' (set of instructions capable of causing a machine having information-

21 HR 11 april 1986, *Computerrecht* 1986/3, p. 174 e.v. met een bespreking door C. Stuurman.

22 Het Hof formuleerde het aldus (r.o. 26): 'onafhankelijk van de vraag of hem een dergelijk onderzoek door (de opdrachtgever) werd opgedragen, had (de adviseur), wanneer dit om een verantwoord advies uit te brengen nodig was, de benodigde tijd voor een diepgaand onderzoek naar de bedrijfsstructuur moeten verlangen.'

23 Hof Den Bosch 9 juni 1992, *Computerrecht* 1993/1 p. 30.

24 Rb Den Bosch 4 februari 1994 *Computerrecht* 1994/4 p. 174.

- processing capabilities to indicate, perform or achieve a particular function, task or result),
- 'a program description' (underlying information determining the instructions to be incorporated in the program),
- 'supporting material' (documentation, user instructions etc.),
- or a set of several of these elements.²⁵

Deze definitie geeft goed aan dat software weliswaar primair op computerprogramma's slaat, maar dat de begeleidende materialen ook onder de definitie vallen.

De meeste programma's worden tegenwoordig geschreven in programmeertalen die getrainde mensen makkelijk schrijven en lezen. Voorbeelden zijn Delphi, C, C++ en Java. Maar computers kunnen deze programma's niet direct lezen omdat ze nog in de zogenaamde broncode staan. Ze moeten eerst worden omgezet in een elektronische vorm die de computer wel kan lezen (compileren). Eenmaal gecompileerd in zogenaamde objectcode kan het programma worden geladen in het computergeheugen en de computer aansturen.

Een bron van discussie is de vraag of software door het recht als een stoffelijke zaak behandeld moet worden. Het wordt wel vastgelegd op een stoffelijk object, bijvoorbeeld op papier of diskette²⁶, maar in essentie is software een niet-lichamelijke zaak, namelijk een complex van ideeën, vondsten en gegevens in de vorm van computerinstructies. Het feit dat het eerst naar het geheugen van een computer gekopieerd moet worden om te kunnen functioneren, toont ook het onstoffelijke karakter ervan aan.

In zijn proefschrift²⁷ over productaansprakelijkheid voor software besteedt Westerdijk veel aandacht aan de juridische classificatie van software. De vraag of de regeling voor productaansprakelijkheid van toepassing is, hangt mede af van de vraag of software een product is. Hij stelt voorop dat software als zodanig geen stoffelijk object is.²⁸ Maar het stoffelijk zijn is niet het enige criterium voor het zaakbegrip. Andere criteria zijn onderwerping aan de macht van de mens, mechanische beheersbaarheid, (economische) waarde en individualiseerbaarheid.²⁹ Asser-Mijnssen-De Haan merken over het zaakbegrip op:

'Zaak' in juridische zin mag men (...) niet vereenzelvigen met stof in natuurwetenschappelijke zin. Wat het recht als een zaak beschouwt, wordt uitsluitend bepaald door de eisen van het praktische rechtsleven.³⁰

Westerdijk ziet dan ook in beginsel geen onoverkomelijke interpretatieproblemen bij het kwalificeren van software als een zaak. Maar dat leidt in het algemene vermogensrecht tot te veel problemen, onder andere omdat software daardoor vatbaar zou worden voor alle zakelijke rechten.³¹ Daar komt bij dat de Auteurswet (Aw) een uitgebreide regeling kent van de rechten op software die dan doorkruist worden.

De maker van software is volgens de Auteurswet³² niet de eigenaar van een zaak in de zin van het Burgerlijk Wetboek, maar de auteursrechtelijke maker van die software. Dit houdt in dat de maker in principe het uitsluitend recht heeft om deze computerprogramma's openbaar te maken of te verveelvoudigen. In de Auteurswet bepaalt artikel 45i verder expliciet dat het laden van software (wat voor ieder gebruik noodzakelijk is) een verveelvoudiging in de zin van de Auteurswet is.

Om software legaal te gebruiken moet de gebruiker dus toestemming verkrijgen van de auteursrechtelijke maker of het auteursrecht op die software zelf krijgen. Voor de toestemming tot gebruik hanteert men ook wel de term licentie. Bij de levering van software wordt toegang gegeven tot de software, bijvoorbeeld door het overdragen van dragers waarop de software staat. Daarnaast wordt of een licentieovereenkomst gesloten die de gebruiker het recht geeft de software te gebruiken of wordt het auteursrecht helemaal of deels overgedragen.³³

Zo is over het algemeen de bescherming en levering van (de gebruiksrechten/auteursrechten op) software goed geregeld in de Auteurswet.³⁴ Op een paar punten vult deze de relatie tussen softwareleverancier en afnemer verder in. Zo geeft artikel 45j Aw de afnemer het recht om fouten in software te herstellen. Dat kan hem contractueel niet worden afgenomen. Dat kan van groot belang zijn als een afnemer zijn software zelf geschikt wil maken voor het volgende millennium en de leverancier dit verbiedt vanwege zijn auteursrecht. Verder heeft de afnemer het recht een back-up te maken van software (art. 45k Aw), de werking van software te bestuderen om de ideeën en beginselen erachter te achterhalen (art. 45l Aw) en – onder bepaalde voorwaarden – het programma te decompileren om te weten hoe het met andere programmatuur kan samenwerken (art. 45m Aw). Deze nuanceringen kent het algemene vermogensrecht niet. Het eigendomsrecht geeft een absoluut recht op een zaak, het auteursrecht een geclausuleerd verbodsrecht op het uitvoeren van bepaalde handelingen met het beschermde werk.

Algemene toepassing van het zaakbegrip op software in het vermogensrecht is dus niet wenselijk. Wel kan nog gekeken worden of de kwalificatie van software als een zaak in sommige rechtsgebieden toch op zijn plaats is en regelingen ook op software toegepast moeten worden. Dit zal in de volgende subparagraaf worden gedaan voor het kooprecht, met name voor wat betreft het conformiteitsvereiste.

Wat mag de afnemer van software in het algemeen verwachten?

Als in softwareleverantiecontracten een clausule staat waarin de leverancier de afwezigheid van de millenniumbug garandeert, dan zou duidelijk zijn wat de afnemer mag verwachten. Maar deze clausule komt pas sinds kort sporadisch in contracten voor. Men moet dus met wat wél geregeld is, de relevante omstandigheden, de wet en de jurisprudentie bepalen of de leverancier het contract correct is nagekomen als hij software met de millenniumbug leverde. Daarbij is het conformiteitsvereiste in artikel 17 van de koopregeling van boek 7 BW mogelijk van belang. Het bepaalt nader wat een koper mag verwachten van zijn aanschaf. Als de koopregeling van

25 R.J.J. Westerdijk, *Productaansprakelijkheid voor software*, Kluwer, Deventer, 1995, p. 29.

26 De zaken waarop software wordt vastgelegd, heten ook wel 'dragers'.

27 R.J.J. Westerdijk, *Productaansprakelijkheid voor software*, Kluwer, Deventer, 1995.

28 Westerdijk a.w. p. 192.

29 Vergelijk ook Stuurman/Vandenbergh, *NJB* 1988, p. 1671 en het 'Elektrociteitsarrest' verderop in deze paragraaf.

30 Asser-Mijnssen-De Haan, *Zakenrecht I*, Zwolle 1992, nr. 62.

31 Anders Kleve/De Mulder, 'De juridische status van software', *NJB* 1989, p. 1342 e.v. Zij betoogden dat het eigendomsrecht toegepast zou moeten worden op software daar dit onder andere de rechthebbende de mogelijkheid zou bieden om illegale kopieën te re-vindiceren.

32 Artikel 1 jo. 10 lid 1 sub 12 Auteurswet.

33 Involge artikel 2 lid 2 van de Auteurswet is voor de hele of gedeeltelijke overdracht van een auteursrecht een akte vereist.

34 Begin jaren tachtig is het auteursrecht op software in talrijke vonnissen al erkend, maar pas door de Richtlijn over de rechtsbescherming van computerprogramma's (Rl. 91/250/EEG, PbEG L 122\42, Tekst opgenomen in *Computerrecht* 1991, p. 194) heeft Nederland dit vastgelegd in de Auteurswet.

Een bron van juridische discussie is de vraag of software een stoffelijke zaak is of niet.

toepassing is op softwareleveranties geeft het conformiteitsvereiste misschien meer duidelijkheid over wat afnemers mogen verwachten wat betreft de millenniumbug.

De toepasbaarheid van de koopregeling op softwarelevering

In de vorige subparagraaf is geconcludeerd dat het onwenselijk is om software in het algemeen als zaak te bestempelen. Maar de rechter heeft het zaakbegrip in het verleden al vaker opgerekt, of een regeling voor zaken naar analogie toegepast op casussen waarin software of elektriciteit centraal stonden. Het beroemdste voorbeeld is het 'Elektriciteitsarrest'³⁵ van begin deze eeuw. Een man had illegaal stroom afgetapt. De vraag was of hij veroordeeld kon worden voor diefstal nu daarvoor sprake moet zijn van het wegnemen van enig goed. De Hoge Raad redeneerde daarbij dat elektriciteit een zekere zelfstandigheid niet kon worden ontzegd, door menselijk toedoen op een andere zaak kon worden overgebracht, kon worden opgeslagen, door de mens kon worden opgewekt, ter beschikking kon blijven van hem die haar opwekte, een zekere waarde vertegenwoordigde en tegen vergoeding aan anderen kon worden overgedragen. Daarom achtte de Hoge Raad dit artikel van toepassing op het illegaal aftappen van elektriciteit, ondanks het verbod op analoge toepassing van strafbepalingen in artikel 1 van het Wetboek van Strafrecht.

Het Hof van Den Haag behandelde een zaak³⁶ waarin computergegevens waren gewist. De vraag was of er sprake was van zaakbeschadiging volgens het verzekingsrecht. Het Hof vond van wel want de software vormde een functionele eenheid met de drager. Wissen van de gegevens tastte die eenheid aan.

Ook in de literatuur pleiten diverse schrijvers voor toepassing (naar analogie) van bestaande regelingen van zaken op software, vooral de regeling van de productaansprakelijkheid. Westerdijk behandelt in zijn proefschrift ook de vraag of de koopregeling van toepassing moet zijn op de 'verkoop' van software.³⁷ Hierbij vergelijkt hij ons recht met dat in Duitsland en de Verenigde Staten. Bij de levering van standaardsoftware wordt in de Verenigde Staten het kooprecht toegepast en in Duitsland past men het kooprecht daarbij naar analogie toe. Bij maatwerksoftware neigt men in de Verenigde Staten ook naar toepassing van het kooprecht. In Duitsland overheerst de leer om maatwerksoftwarelevering niet als koop te zien, maar als aanneming van werk.³⁸

Bij vergelijking van de softwareleverantie met de koopovereenkomst moet op twee gronden maatwerk van standaardsoftware worden onderscheiden:

– Ten eerste is bij maatwerksoftware meer sprake van een zekere 'interactiviteit' tussen afnemer en leverancier. Bij de aanschaf van een standaardpakket heeft de afnemer vaak geen of nauwelijks inhoudelijk contact met de leverancier en heeft zelf geen invloed op de specificaties van het aangeschafte product. Maar bij maatwerksoftware is de medewerking van de afnemer nodig om de kwaliteit van de software te waarborgen en de gewenste functionaliteit tot stand te brengen.

– Ten tweede zijn de prestaties die overeengekomen worden verschillend. Bij standaardsoftware be-

staat de prestatie van de leverancier alleen uit het toegang geven tot al ontwikkelde software en het geven van een gebruiksrecht op die software. Bij maatwerksoftware is het op maat maken of ontwikkelen van de software de kern van de prestatie.

De koopregeling kan van toepassing zijn op leveranties van standaardsoftware, maar ligt minder voor de hand bij maatwerksoftware.

Bij de koopregeling gaat het om de overdracht van een bepaald goed en niet om het maken daarvan. Ook heeft de koper normaal gesproken geen invloed op de kwaliteit van hetgeen hem geleverd wordt. In het algemeen kan de levering van standaardsoftware dus als een koop worden gezien. Een maatwerkovereenkomst lijkt minder op koop omdat het maken van een programma en niet het leveren centraal staat. Er is dus wat voor te zeggen om de koopregeling (naar analogie) toe te passen op de levering van standaardsoftware. Minder voor de hand ligt dit voor maatwerksoftware.

De grens tussen de twee is niet scherp te trekken. Is er bijvoorbeeld sprake van een standaardpakket als dit op enkele punten aangepast is aan de wensen van de afnemer? Conclusie: de koopregeling kan van toepassing zijn op leveranties van standaardsoftware, maar toepassing ligt minder voor de hand bij maatwerksoftware.

Het effect van de toepassing van de conformiteitsregeling
Voorzover de koopregeling van toepassing is op de levering van software kan men zich afvragen of het conformiteitsbeginsel van artikel 7:17 BW veel invloed heeft op de uitkomst van conflicten tussen afnemers en leveranciers. Dit artikel bepaalt in lid 1 dat de koopovereenkomst moet worden nagekomen conform die overeenkomst. Hierop staat in artikel 6:74 BW al een sanctie: als een partij tekortschiet, dan is die schadelijkt jegens de schuldeiser. De eerste zin van het tweede lid van artikel 7:17 BW bepaalt verder:

'Een zaak beantwoordt niet aan de overeenkomst indien zij niet de eigenschappen bezit die de koper op grond van de overeenkomst mocht verwachten.'

Deze gedachte is ook neergelegd in artikel 3:35 BW. Uitgangspunt is dat een overeenkomst ontstaat uit een aanbod en de aanvaarding daarvan. De inhoud van deze rechtshandelingen³⁹ bepaalt de inhoud van de overeenkomst en de verbintenis(sen) die daaruit voortvloeien. Als de meningen over de inhoud van de rechtshandelingen achteraf verschillen bepaalt artikel 3:35 BW dat gekeken moet worden welke betekenis onder de gegeven omstandigheden redelijkerwijs aan de rechtshandelingen mocht worden worden toegekend. Als een schuldeiser niet krijgt wat hij op grond van de overeenkomst verwachtte dan is de vraag: wat mocht hij verwachten; waarop mocht hij vertrouwen; en welke eigenschappen mocht de schuldeiser van de prestatie verwachten?

35 HR 23 mei 1921, *BJ* 1921, 564 m.nt. B.M. Taverne.

36 Hof Den Haag 4 juni 1992 *NJ* 1993, 419.

37 R.J.J. Westerdijk, *Productaansprakelijkheid voor software*, Kluwer, Deventer 1995.

38 Westerdijk a.w., p. 188.

39 Aanbod en aanvaarding zijn verklaringen van een op een rechtsgevolg gerichte wil en dus rechtshandelingen (art. 3:33 BW).

Deze gedachte lag vóór de invoering van het nieuw BW al in het standaardarrest 'Haviltex'.⁴⁰ Daarin bepaalde de Hoge Raad hoe een overeenkomst moet worden uitgelegd. De taalkundige benadering volstaat niet. Het komt aan op de zin die partijen onder omstandigheden aan de overeenkomst mochten geven en op wat zij redelijkerwijs van elkaar mochten verwachten. Dit is volgens Hijma en Olthof een tweezijdige toepassing van het vertrouwensbeginsel van artikel 3:35 BW.⁴¹

De aanwezigheid van bugs in software betekent niet meteen dat de software niet voldoet aan de gerechtvaardigde verwachtingen van de afnemer.

40 HR 13/3/1981, NJ 1981, 635. De Hoge Raad bepaalde verder in dit arrest dat voor de uitleg van een overeenkomst ook van belang kan zijn tot welke maatschappelijke kringen partijen behoren en welke rechtskennis van hen verwacht mag worden.

41 Jac. Hijma en M.M. Olthof, *Compendium Nederlands Vermogensrecht*, Kluwer, Deventer 1996, nr. 492.

42 Asser-Hijma I, *Koop en Ruil*, Zwolle 1994, nr. 343.

43 MvA II, Parl. Gesch. Boek 7, p. 125.

44 S. Gerbrandy, 'De omstandigheden. Op de grens tussen dwaling en wanprestatie', *WPNR* 5959, 1990, p. 285.

45 Westerdijk, a.w. p. 4 wijst in verband hiermee op de mislukte automatisering van de studiefinanciering en de vele jurisprudentie over mislukte automatiseringen.

46 Westerdijk a.w. p. 5.

47 Zie bijvoorbeeld voor patches voor fouten in Windows 95: <http://www.microsoft.com/windows95/info/system-updates.htm>.

48 Stichting Raad van Arbitrage voor Metaalnijverheid en -handel 29 augustus 1990, *Computerrecht* 1993/2 p.86.

49 Rb Rotterdam 28 januari 1983, *Computerrecht* 1987/4, p. 258.

50 President Rb Arnhem 14 april 1989, *Computerrecht* 1990/2, p. 88

De tweede zin van het tweede lid van artikel 7:17 BW geeft een nadere aanwijzing hoe bepaald kan worden wat een koper mag verwachten.

'De koper mag verwachten dat de zaak de eigenschappen bezit die voor normaal gebruik daarvan nodig zijn en waarvan hij de aanwezigheid niet behoefde te betwijfelen, (...).'

Volgens zowel Asser-Hijma⁴² als de wetsgeschiedenis⁴³ concretiseert deze regel de eerste zin van het tweede lid van artikel 7:17 BW. Met deze regel is dan ook geen materiële verandering beoogd ten opzichte van hetgeen zonder deze toevoeging had gegolden.⁴³ Goed beschouwd legt die een 'common sense'-gedachte vast.

Om de gerechtvaardigde verwachtingen vast te stellen moet men eerst nagaan welke eigenschappen de schuldenaar expliciet gegarandeerd heeft. Maar daarnaast is een deel van de verbintenis impliciet. Gerbrandy geeft een mooi voorbeeld:

'Men kan zich moeilijk voorstellen dat de leverancier van een tafel, aangesproken ter zake van wanprestatie, met succes zou kunnen aanvoeren: 'Ik heb nooit gegarandeerd dat alle poten even lang zouden zijn.'⁴⁴

Als partijen een prestatie in algemene termen overeenkomen is uiteraard de normale betekenis van de woorden het uitgangspunt. Als het om de levering van een tafel gaat, dan is een normale eigenschap van een tafel een gerechtvaardigde verwachting, bijvoorbeeld dat de poten even lang zijn. Onaannemelijk is dat dit bij een niet-koopovereenkomst niet zo is. Nog een voorbeeld: als een schilder een buitengevel moet schilderen dan mag de opdrachtgever erop vertrouwen dat hij waterbestendige verf gebruikt, ook al is dat niet expliciet afgesproken. Het is een normale eigenschap van de overeengekomen prestatie.

De normale eigenschappen van software

Wat mag een afnemer verwachten dat normale eigenschappen zijn van software?

Een ding is zeker: niemand kan er momenteel van uitgaan dat software foutloos is. Software heeft bijna altijd gebreken. Dat blijkt bijvoorbeeld uit krantenberichten⁴⁵ over mislukte automatiseringsprojecten. En de PC-gebruiker wiens computer nooit vastloopt

of probleemloos werkt moet nog geboren worden. Programma's zonder fouten zijn eerder een rareiteit dan norm. Ten tweede is het haast onmogelijk foutloze programma's te maken.

Het maken van een programma is grofweg te verdelen in drie fasen: ontwerp, bouw en het testen op fouten om het programma te verbeteren. Hoe meer men test, des te meer fouten worden eruit gehaald. Maar het is, mede door de extreem hoge kosten, bijna onmogelijk alle fouten te vinden en te herstellen. Grote hersteloperaties zijn niet rendabel omdat programma's door de snelle ontwikkeling van de automatisering vaak al na enkele jaren worden vervangen. Westerdijk wijst er bovendien op dat het niet mogelijk is meer ingewikkelde programma's uitputtend te testen.⁴⁶ Niet voor niets geven bijna alle softwareleveranciers hun afnemers gratis 'patches' om fouten in geleverde software te verhelpen en soms de functionaliteit te verbeteren.⁴⁷ De afnemer heeft daar zelfs belang bij: de prijs van software kan lager blijven en de software komt eerder uit.

Vaak wordt na levering van software ook een onderhoudscontract overeengekomen want er kunnen storingen optreden. Ook dat wijst erop dat software niet foutloos wordt geleverd. Vaak komen bij (langdurig) gebruik, bijvoorbeeld in combinatie met andere software, nieuwe fouten naar voren. Dat in software bugs zitten, betekent dus niet meteen dat die niet voldoet aan de gerechtvaardigde verwachtingen van de afnemer. Maar waar ligt de grens dan?

De contractvoorwaarden zijn daarbij van belang. Daarin kunnen de risico's van bugs bij een partij worden gelegd en de aansprakelijkheden worden geregeld. Maar wat zijn daarnaast de gerechtvaardigde verwachtingen van de afnemer? Wat zegt de jurisprudentie daarover?

In een zaak over software die moest worden aangepast aan de wensen van de afnemer rekenden de arbiters van de stichting Raad van Arbitrage voor Metaalnijverheid en -handel⁴⁸ de afnemer onder andere sterk aan dat hij zijn wensen over de software nog niet had geuit. Als dus blijkt dat software niet goed werkt doordat de afnemer niet (op tijd) correct zijn wensen duidelijk maakt, dan mag hij door deze uitspraak niet verwachten dat er geen bugs in zitten. In 1983 en in 1989 hebben de rechtbanken van Rotterdam en Arnhem uitspraken gedaan over de verwachtingen die een afnemer van IT-producten mag hebben. In de Rotterdamse zaak⁴⁹ ging het om de levering van maatwerksoftware. De rechtbank stelde vast dat de levering daarvan was overeengekomen (en niet alleen het verrichten van enkele diensten) en

'dat het onder de gegeven omstandigheden een ieder duidelijk had moeten zijn dat hij (de afnemer PE/MS) bij geen andere prestatie belang kon hebben dan een goed functionerend nieuw programma (...).'

In het Arnhemse kort geding in 1989 deed de president een uitspraak over de algemene verwachtingen die een afnemer mocht hebben van een geleverd computersysteem.⁵⁰ De leverancier beriep zich erop dat de garantieclausules volgens de algemene voorwaarden pas van toepassing waren als er een aanvullend onderhoudscontract was afgesloten. Maar de president bepaalde dat een afnemer:

'(...) er in beginsel – ongeacht of ze zich in dat verband op een contractuele garantieregeling kan beroepen – aanspraak op kan maken dat uit ondeugdelijkheid van het geleverde systeem voortkomende storingen en defecten kosteloos worden verholpen'.

Uit deze uitspraken blijkt dat afnemers van IT-producten er in principe (ook zonder toegespitste garantieregelingen) op mogen vertrouwen dat geleverde producten normaal functioneren.

De rechtbank van Rotterdam deed in 1994⁵¹ een uitspraak over een levering van een combinatie van standaard- en maatwerksoftware. Zij stelde bij de beoordeling van de vraag of er op tijd correct was geleverd voorop, dat

'(...) de overeenkomst Van der Horst (de leverancier PE/MS) verplichtte tot het leveren van een samenhangend geheel van computerprogrammatuur dat de eigenschappen zou bezitten die nodig zijn voor een normaal gebruik daarvan door een onderneming als Koster en daarenboven de eigenschappen die zijn beschreven in het functioneel ontwerp'.

Ook deze uitspraak wijst erop, in een formulering die nauw aansluit bij de conformiteitsregeling, dat een afnemer van software in principe mag verwachten dat die normaal functioneert. De specifieke functies die gewenst worden gelden daarbij als extra eisen naast de eis van normale geschiktheid.

Conclusie

Het is onmogelijk software foutvrij te leveren. Toch mag een afnemer van software verwachten dat die geschikt is voor normaal gebruik. De conformiteitsregeling van boek 7 is waarschijnlijk op standaardsoftwareleveranties (naar analogie) van toepassing, maar ligt minder voor de hand bij maatwerksoftware. Toch kan in dat geval de conformiteitsregeling worden gezien als de neerslag van een rechtsregel die ook zonder directe toepasbaarheid van artikel 7:17 BW tussen contractpartijen geldt. Ook van maatwerksoftware mag dus worden verwacht dat die voor normaal gebruik geschikt is.

Zodra de millenniumbug zich manifesteert kan software niet meer normaal gebruikt worden. Maar het kan zijn dat de bug relatief kleine problemen geeft. Bijvoorbeeld als de datum verkeerd op het scherm of op print-outs staat (bijvoorbeeld als 1-3-00). Uit de context kan dan duidelijk worden om welke datum het gaat. In dat geval kan de software nog normaal gebruikt worden en kan de leverancier stellen dat de software aan de gerechtvaardigde verwachtingen van de afnemer voldoet.

Dit is pas de eerste stap bij de bepaling van de aansprakelijkheid van de automatiseerder. De gerechtvaardigde verwachtingen van de afnemer worden namelijk door vele factoren beïnvloed. Hier gaat het alleen nog om de verwachtingen die de afnemer mag hebben op het moment van levering. Maar hoe lang hij mag verwachten dat de software goed werkt, wordt in de volgende paragraaf behandeld.

Is de softwareleverantieovereenkomst een resultaats- of een inspanningsverbintenis?

Over het onderscheid tussen de inspannings- en de resultaatsverbintenis is veel discussie. Niet alleen

over de vraag of bepaalde overeenkomsten resultaats- of inspanningsverbintenissen zijn, maar ook over wat de gevolgen (moeten) zijn van die classificatie.

Een afnemer van software mag verwachten dat die geschikt is voor normaal gebruik.

Asser-Hartkamp geeft aan dat een verbintenis meestal gericht is op een resultaat.

'De verbintenis is eerst dan vervuld, wanneer dat resultaat is verwezenlijkt en het verschuldigde in de macht van de schuldeiser is gekomen.'^{*}

Bij zo'n verbintenis is het niet voldoende als de schuldenaar zich alleen maar inspant om het resultaat te bereiken. Dit soort verbintenissen zijn resultaatsverbintenissen.

Er zijn ook verbintenissen die alleen een inspanning beogen. Hartkamp noemt als voorbeeld de verbintenis tussen de rijsschoolhouder en zijn leerling. De eerste staat er niet voor in dat zijn leerling voor het rijexamen slaagt. Hij belooft alleen dat hij zich daartoe inspant. Hierbij is dus voldoende inspanning van de schuldenaar genoeg om aan de verbintenis te voldoen.

In een bekend arrest van de Hoge Raad, het zogenaamde 'Tram'-arrest⁵², was dit onderscheid wezenlijk. De Raad bepaalde dat een overeenkomst om personen te vervoeren de vervoerder verplicht de reiziger veilig naar diens bestemming te brengen. Hij moet een resultaat leveren. Als een reiziger letsel oploopt tijdens het vervoer schiet de vervoerder tekort. Hij moet dan bewijzen dat deze tekortkoming niet aan hem ligt om onder de aansprakelijkheid uit te komen. Voor een reiziger is de bewijspositie dus gemakkelijker.

Bij procedures over de millenniumbug kan de bewijslastverdeling van groot belang zijn. De afnemer zal stellen dat de geleverde software niet aan de verwachtingen voldoet die hij mocht hebben gezien het contract en dat de leverancier tekortschoot. Als software met de millenniumbug bij levering inderdaad gebrekkig is (wanneer dit het geval is wordt in de volgende paragraaf behandeld), dan kan de leverancier stellen dat hij zich toch aan de afspraken heeft gehouden, omdat hij gezien de omstandigheden niet beter kon presteren, bijvoorbeeld omdat hij moest werken met al aanwezige programma's, gegevens en hardware die hem min of meer dwongen om tweecijferig te werken. Hij kan ook beweren dat het niet aan hem lag maar aan een andere automatiseerder, die de afnemer zelf heeft aangesteld, waarmee hij moest samenwerken bij de ontwikkeling van de software. Daarom is het voor de millenniumproblematiek van belang om vast te stellen of een softwareleverantieovereenkomst inspannings- of resultaatsverbintenissen oplevert en welke invloed die hebben op de verdeling van de bewijslast.

Het onderscheid van overeenkomsten in de beide typen is vrij algemeen aanvaard. Toch is er nog dis-

* Asser-Hartkamp, *Verbintenissenrecht, deel 4 I, De verbintenis in het algemeen*, Zwolle 1996 nr. 184.
51 Rb Rotterdam 3 juni 1994, *Computerrecht* 1996/3, p. 104.
52 HR 26 februari 1971, NJ 1971, 270, *Ars Aequi* 1971 p. 331.

cussie over twee vragen: wat bepaalt of een verbintenis een resultaats- of een inspanningsverbintenis is, en in hoeverre moet de classificatie van de overeenkomst de uiteindelijke bewijslastverdeling bepalen?

Van den Berg behandelt in zijn stuk *Resultaat naar werk* het nut van het onderscheid, waarbij beide discussiepunten aan bod komen.⁵³ Hij begint daarbij met de medische behandelovereenkomst en neemt afstand van de gedachte dat alle verbintenissen die daaruit voortvloeien in één van beide categorieën vallen omdat het om zeer verschillende behandelingen kan gaan: van het vullen van een kies tot het aanbrenge van een bypass.

Ook het classificeren van een individuele verbintenis die voortvloeit uit een medische behandelovereenkomst vindt Van den Berg moeilijk omdat een overeenkomst vaak uit allerlei deel(be)handelingen bestaat, die ieder apart weer geïnclassificeerd kunnen worden. Pitlo geeft hiervan een goed voorbeeld.⁵⁴ Een chirurg heeft wellicht niet meer dan een verplichting om zich in te spannen voor een goede afloop van een operatie, maar hij is wel te houden aan de resultaatsverplichtingen om op tijd voor de operatie te verschijnen, fris te zijn, zijn apparatuur in orde te hebben en over kundig personeel te beschikken.

Ook voor softwareleverantieovereenkomsten geldt dat die zich in allerlei vormen voordoen. Er is niet alleen het onderscheid tussen maatwerk en standaardsoftware. Van de maatwerksoftwarelevering bestaan ook weer verschillende vormen. Zo kan die software onder toezicht van de opdrachtgever worden gemaakt of volgens diens plannen. De leverancier kan ook juist een heel automatiseringssysteem bedrijfsklaar afleveren. Verder zijn bij de levering van software de verplichtingen te onderscheiden die ieder weer een eigen inspannings- of resultaatskarakter hebben, bijvoorbeeld: de puur juridische levering van auteursrechten op software, de implementatie of installatie van software, het creëren van een helpdesk, het gebruik van de juiste ontwikkeltools, het correct ontwerpen van de software, het kiezen van de juiste standaarden daarbij, etc.

Bij de aannemingsovereenkomst noemt Van den Berg nog enige bezwaren tegen de bewijslastverdeling op grond van het onderscheid tussen resultaats- en inspanningsverbintenis. Het komt vaak voor dat de aannemer een bouwwerk maakt naar een ontwerp van de opdrachtgever. Dan moet scherp worden gekeken naar wat precies het resultaat is waartoe de overeenkomst de aannemer verplicht. Het gaat namelijk niet om het bouwen van een goed gebouw, maar van het gebouw dat hem is opgedragen in de bouwtekening. Het onderscheid tussen resultaats- en inspanningsverbintenis heeft voor het vaststellen van de bewijslastverdeling nu minder nut, omdat uit een slecht gebouw niet blijkt of het afgesproken resultaat wel of niet geleverd is. Het slechte gebouw kan namelijk ook te wijten zijn aan de slechte bouwtekening van de opdrachtgever.

Een andere complicatie is dat vaak gewerkt moet worden met bouwmaterialen of onderaannemers die de opdrachtgever voorschrijft. Dan is het onredelijk om de bewijslast zonder meer bij de leverancier te leggen, ook al is een bepaald resultaat overeengekomen. Hij zou dan verantwoordelijk zijn voor fouten van voorgeschreven onderaannemers, ontwerpen en materialen. Van den Berg wijst wel op de plicht van de aannemer om te wijzen op fouten in de bouwtekening en materialen die hij behoort te kunnen herkennen.

Van den Bergs kritiek gaat ook op voor maatwerksoftwareleveringen. Het komt voor dat de leverancier moet werken op aanwijzingen van de afnemer, die daartoe soms een externe adviseur raadpleegt. Meestal moet de leverancier ook met hardware, software en databanken van de afnemer werken. In die gevallen is het niet correct de bewijslast bij de leverancier te leggen alleen omdat de software niet goed werkt. Dat wil overigens niet zeggen dat er geen andere redenen kunnen zijn om dat te doen.

Naast de kwalificatieproblemen vindt Van den Berg de bewijslastverdeling naar verbintenis categorie te veel een zaak van 'alles of niets', omdat het de rechter te weinig vrijheid geeft om rekening te houden met de gang van zaken. Een belangrijke reden voor dit verzet is dat het toewijzen van de bewijslast ook de toewijzing van het bewijsrisico betekent.⁵⁵ Als een feit niet te bewijzen is, dan verliest de partij waarbij de bewijslast ligt de procedure. Van den Berg pleit er daarom voor de bewijslast 'dynamisch' toe te delen. Hij noemt enkele factoren die meespelen bij het toewijzen van bewijsplicht en -risico aan de uitvoerder van een overeenkomst:

- het weigeren om na falen opening van zaken te geven;
- het verzuim om op de gebruikelijke manier een verslag te maken van de werkzaamheden;
- het veronachtzamen van veiligheidsnormen;
- een ongebruikelijke complicatie;
- het feit dat een slechte afloop niet te verwachten is;
- het feit dat de informatie of het overzicht over het hele project voornamelijk bij één partij ligt;
- het feit dat de uitvoerder de integrale ontwerper en uitvoerder van de opdracht is en niet alleen andermans plannen uitvoert;
- het feit dat de aard van het gebrek op een fout wijst bij een taak van de uitvoerder.

Het feit dat de softwareleverancier de meeste informatie heeft en doorgaans meer deskundigheid heeft dan de afnemer is al aanleiding om de bewijslast bij de leverancier te leggen. Ook de factoren die Van den Berg noemt kunnen daartoe leiden, bijvoorbeeld omdat het gebrek op een gebied ligt waar de leverancier vrij is om zelf te beslissen, of omdat hij zijn werk niet genoeg documenteert (een belangrijk onderdeel van software) of te weinig informatie geeft over wat hij heeft gedaan.

Softwareleverantieovereenkomsten zijn zowel als categorie als individueel moeilijk te classificeren als inspannings- of resultaatsverbintenissen. Bovendien zijn veel andere factoren van belang om de bewijslast te bepalen. Met alleen de classificatie is de bewijslast niet goed te bepalen. Toch is een kanttekening op zijn plaats. Tot nu toe is alleen gekeken naar de aard van de overeengeko-

53 In de bundel aangeboden aan prof.nr. W.M.Kleijn, *Quod Licet?*, Kluwer, Deventer 1992, p. 1-17.

54 Pitlo-Bolweg, *Verbindenissenrecht*, 1979, p. 83.

55 Een voorbeeld hiervan is de zaak tussen een chirurg en een vrouw die complicaties van een operatie opliep doordat zij gemeenschap had na die operatie. De zaak spitste zich toe op de vraag of de chirurg haar had gewaarschuwd om na de operatie een aantal weken geen gemeenschap te hebben. Aangezien het hierbij uiteindelijk neerkwam op het woord van de chirurg dat hij wel gewaarschuwd had, en het woord van de patiënt dat het tegendeel het geval was, bepaalde het opleggen van de bewijslast aan de chirurg hier ook de uitslag van deze zaak in het nadeel van deze laatste (HR 18 februari 1994, NJ 1994,

De specifieke afspraken tussen partijen over de prestatie zijn belangrijk bij het bepalen van de rechten en plichten uit een overeenkomst.

men prestatie en de omstandigheden waaronder die wordt geleverd. Maar zeer belangrijk bij het bepalen van de rechten en plichten uit een overeenkomst zijn ook de specifieke afspraken tussen partijen over de prestatie. In het contract kunnen partijen expliciet de aard van de prestatie omschrijven. Als zij expliciet vastleggen dat de schuldenaar een bepaald resultaat levert dan is deze conform dat contract ook verplicht dat te leveren. Maar partijen kunnen ook overeenkomen dat de leverancier zich alleen zal inspannen voor een resultaat of daar bepaalde diensten voor zal leveren. Verder is het mogelijk dat het resultaat deels gegarandeerd wordt en er deels alleen een inspanning wordt geleverd voor een resultaat. Deze vergroting of verkleining van de omvang van de prestatieplicht kunnen partijen verdisconteren in de prijs. Als het risico helemaal bij de leverancier ligt doordat hij het resultaat onvoorwaardelijk tot zijn verantwoordelijkheid rekent, dan kan hij daarvoor een hogere prijs bedingen dan wanneer hij zich alleen verbindt tot het nastreven van een resultaat.

Als een contract bepaalt dat de softwareleverancier een boekhoudpakket levert waarmee altijd binnen vijf minuten een uitdraai van alle debiteuren te maken is, dan is dat voor hem een resultaatsverbintenis. Maar als hetzelfde contract stelt dat hij zorgt dat het programma zo gebruiksvriendelijk mogelijk wordt, dan is dit eerder een inspanningsverplichting.

De rechter moet dus rekening houden met de inhoud van de verbintenis en de daaruit voortvloeiende verplichtingen voor de schuldenaar als hij de bewijslastverdeling bepaalt. Binnen de grenzen van de wet geeft het principe van contractvrijheid partijen immers de mogelijkheid om zelf hun rechten en wederzijdse verplichtingen vast te leggen.

Een voorbeeld van het volgen van de contractinhoud is een arrest van het Hof Amsterdam.⁵⁶ Het bepaalde door een artikel waarin was overeengekomen dat de leveringstermijnen zoveel mogelijk in acht zouden worden genomen maar niet bindend waren, dat het om een inspanningsverbintenis ging. Daarom zag het geen wanprestatie in het feit dat een jaar na het verstrijken van de leveringstermijn van zes maanden het systeem nog niet draaide.

Dit arrest toont ook aan dat het volgen van de contractinhoud ook discussies oproept. Stuurman kritiseerde de uitspraak. Hij wijst erop dat hier was overeengekomen een gespecificeerd computersysteem te leveren en dat er dus wel degelijk sprake was van een resultaat. De enkele bepaling dat de leveringstermijnen niet bindend zijn mag volgens hem niet leiden tot een verandering van de aard van de hele verbintenis. Die bepaling krijgt dan zo'n vergaande toepassing dat die werkt als een vergaand exoneratiebeding. De geldigheid daarvan is twijfelachtig, want de leverancier kan dan nooit gedwongen worden te leveren omdat hij aan geen termijn gebonden is.

Stuurmans kritiek snijdt hout ook al is het uitgangspunt van de uitspraak van het Hof Amsterdam correct dat de inhoud van de overeenkomst primair bepaalt welke verplichtingen partijen hebben. Maar de vergaande interpretatie van een bijkomende clausule perkt het doel van de overeenkomst – het tot stand brengen van een geautomatiseerd systeem – wel erg in. De volgende paragraaf gaat nader in op de geldigheid van exoneratiebedingen.

Conclusie

Of de softwarelevering als een inspannings- of een resultaatsverbintenis kan worden gezien en wat daarvan de consequenties zijn, is vaak niet meteen duidelijk. Daarom is het te arbitrair om de bewijslastverdeling zonder meer daaraan op te hangen. De verregaande consequenties die dat kan hebben voor een procedure eisen dat de rechter ook met de andere omstandigheden rekening houdt.

Het onderscheid kan wel richtinggevend zijn bij het nemen van de bewijsbeslissing. Vooral als partijen in het contract duidelijk kiezen voor een prestatieplicht moet de rechter daar rekening mee houden. De manier waarop de verplichtingen van de leverancier in het contract staan beïnvloedt de bewijslastverdeling en dus de kans dat een claim tegen de leverancier slaagt.

De verwachting die de afnemer mag hebben van de levensduur van software staat niet vaak in contracten. De vraag wie moet aantonen dat de afnemer wel of niet een langere levensduurverwachting mocht hebben dan de millenniumbug toelaat is dus moeilijk te beantwoorden aan de hand van de classificatie van de overeenkomst als inspannings- of resultaatsverbintenis. De toewijzing van de bewijslast is op dit punt moeilijk te voorspellen.

DE VERWACHTINGEN VAN SOFTWARE IN DE TIJD

In de vorige paragraaf is onder andere vastgesteld dat de afnemer van software geen genoeg hoeft te nemen met software die niet volgens de overeengekomen specificaties werkt. De millenniumbug maakt zodra die opspeelt goed functioneren van die software meestal onmogelijk, waardoor die niet voldoet aan de gerechtvaardigde verwachtingen van de afnemer. De volgende vraag is *hoe lang* de afnemer mag verwachten dat de software goed functioneert conform de overeengekomen specificaties.

De levensduurverwachtingen van software in het algemeen

Voor het antwoord is de levensduur die men in het algemeen van software mag verwachten van belang. Op het eerste gezicht zal men zeggen: eeuwig. Software slijt immers niet.⁵⁷ Maar om technische redenen heeft software toch niet het eeuwige leven. Daar komt nog bij dat de economische of maatschappelijke levensduur van zaken meestal korter is dan de technische.

De invloed van de contractuele voorwaarden en de feitelijke omstandigheden

Wat in een specifiek geval verwacht mag worden van de levensduur van software is, naast de algemene levensverwachting, afhankelijk van de omstandigheden. Het voornaamste zijn specifieke bepalingen in het contract over de (gegarandeerde) levensduur, maar die zijn er meestal niet. Wel kan uit andere contractbepalingen soms worden afgeleid wat de toekomstverwachtingen van partijen waren. Ook uit de leveromstandigheden valt soms wat te destilleren.

De mededelings- en onderzoeksplichten

Bij het vaststellen van de gerechtvaardigde verwachtingen van de afnemer speelt ook de mededelings- en de onderzoeksplicht een rol. Men moet zich af-

56 Hof Amsterdam 9 oktober 1987, *Computerrecht* 1987/2 p. 115 e.v. m.nt. C. Stuurman.

57 De dragers van software (diskettes, tapes, e.d.) hebben niet het eeuwige leven. De magnetische velden waarin de gegevens bijvoorbeeld op diskettes worden vastgelegd, kunnen in de loop der jaren worden aangetast. Om dit te voorkomen moeten ze van tijd tot tijd worden gekopieerd.

vragen in hoeverre de afnemer zelf duidelijkheid moet scheppen over de levensduur van de software. Vervolgens moet men bezien in hoeverre de leverancier dat had moeten doen en hoe die mededelings- en onderzoeksplichten zich onderling verhouden.

Software kan vaak om technische redenen niet eeuwig dezelfde functionaliteit bieden.

De levensduur van software in het algemeen

Automatiseringsexperts zeggen dat de levensduur van software sterk afhangt van de aard van het programma. In de praktijk zijn sommige pakketten na een jaar al niet meer te gebruiken, maar sommige programma's uit de jaren zestig en zeventig, of delen daarvan, draaien nog steeds. Over de gemiddelde levensduur van software valt weinig te zeggen. Wel zijn enige technische, economische en maatschappelijke factoren bekend die de gemiddelde levensduur beïnvloeden.

Ook al slijt software niet, toch kan het pakket vaak om technische redenen niet eeuwig dezelfde functionaliteit bieden. Een belangrijke reden daarvoor is dat de hoeveelheid data waarmee een programma moet werken in de loop der tijd vaak toeneemt. Bijvoorbeeld een programma dat een nieuwe transactie met eerdere moet kunnen vergelijken, groeit met de toename van het aantal uitgevoerde transacties en kan te traag worden. Ook kan het zijn dat het programma de maximale hoeveelheid gegevens bereikt die het überhaupt kan bewerken.

Een andere technische reden waarom programma's niet eeuwig bruikbaar zijn, is dat programmeurs vaak allerlei tellers gebruiken. Een teller houdt bijvoorbeeld bij hoe vaak bepaalde commando's zijn doorlopen, hoeveel records zijn opgeslagen in een database, hoeveel transacties zijn uitgevoerd of hoeveel tijds-eenheden zijn verstreken, zoals het aantal jaren. Ook kunnen ze volg- of identificatienummers genereren. Zulke tellers kunnen niet oneindig hoger worden. Hoe lang wel hangt af van hoe de teller gedefinieerd of geïnitieerd is.⁵⁸ Maar hoe meer ruimte een teller krijgt, hoe meer geheugenruimte dat kost. Vooral als de tellerwaarden op vele plaatsen vele malen worden opgeslagen, zoals vaak bij datums, heeft dat grote invloed op de eisen van het programma aan het computergeheugen en de opslagcapaciteit.

Daarom koos men er in programma's bijvoorbeeld vaak voor het jaartal in een getal van twee cijferposities te noteren, hetgeen de oorzaak is van het millenniumprobleem. Waar dit toe kan leiden staat in de eerste paragraaf. Een ander voorbeeld van zo'n teller is die in Unix welke de datum en tijd bepaalt door de seconden te tellen die verstreken sinds de eerste dag van het jaar 1970. Deze teller is gedefinieerd als een 32 bits integer getal. Op 19 januari 2038 om 3:14:07 uur zal de maximale waarde van dit getal worden bereikt.⁵⁹ Sommigen voorspellen dat dit tot een volgende datumcrisis kan leiden, omdat zeer veel netwerken over de hele wereld met Unix draaien. Anderen verwachten in de nieuwe versies

van Unix een oplossing.⁶⁰ Maar dat dachten velen vroeger ook over de millenniumbug.

Ook tellers die iets anders dan de datum bijhouden, kunnen problemen geven. Een voorbeeld is de manier waarop de Dow Jones Index wordt bijgehouden in computers van banken, vermogensbeheerders en effecteninstellingen. Op het moment van schrijven zweeft de index rond 9200 punten en is het niet uitgesloten dat hij door de 10.000-puntengrens gaat. Maar de meeste programma's houden de index bij met vier cijfers. Ze zien een index van 10.000 als 0.000 of 1000. Er wordt gewaarschuwd dat wanneer deze magische grens wordt bereikt automatische verkoopprogramma's van beleggers in werking kunnen treden en analytische programma's door rekenfouten verkeerde gegevens kunnen doorgeven.⁶¹

Of er sprake is van een programmeerfout als een teller zijn maximum bereikt hangt van de omstandigheden af. Voorop staat dat de programmeur bij het definiëren van de teller een maximumwaarde moet kiezen en dat die waarde niet ongestraft oneindig hoog kan zijn. Daar komt bij dat dit meestal geen problemen oplevert. Een extreem voorbeeld: het is nu ongebruikelijk om het jaartal in vijf cijfers bij te houden; het duurt immers nog 8000 jaar voordat het jaar 10.000 aanbreekt. De programmeur moet dus inschatten welke waarden een teller kan aannemen en vervolgens afwegen welke marge hij aanhoudt en hoeveel geheugen- en opslagruimte die kost. Hoe ouder een programma, hoe groter de druk op programmeurs om de maxima zo laag mogelijk te kiezen omdat geheugen- en opslagcapaciteit vroeger veel duurder waren. Hierdoor hebben veel programma's een maximale gebruiksduur die afhankelijk is van het gebruik en van het verstrijken van de tijd.

Ook externe factoren zijn van belang voor het functioneren van software. Zo moet de computer geschikt zijn voor de software, moeten gebruikers weten hoe ze met computer en software moeten omgaan, moeten computer en software worden onderhouden, en tot slot moeten hard- en software met andere programma's kunnen communiceren. Ieder aspect beïnvloedt de levensduur van software. Doordat de ontwikkelingen in de automatisering zo snel gaan blijven deze factoren niet eeuwig betaalbaar en beschikbaar. De ondersteuning en dergelijke worden namelijk voor nieuwe, meer lucratieve zaken ingezet. Dit komt op de eerste plaats doordat de mogelijkheden van computers enorm snel toenemen. Niet alleen groeit de verwerkingssnelheid van processors exponentieel⁶² en dalen de prijzen voor geheugen- en opslagruimte snel, ook worden steeds nieuwe automatiseringstechnieken en toepassingen ontworpen. Een ander voorbeeld is de trend om steeds meer met grafische interfaces te werken.

Afnemer en gebruiker volgen deze trends om verschillende redenen. De beste reden voor een afnemer om zijn systemen up-to-date te houden is dat het zijn productiviteit en concurrentiepositie verbetert. Een andere reden is dat hij de standaard in zijn bedrijfstak moet volgen. Een voorbeeld hiervan is de tekstverwerker WordPerfect die lange tijd standaard was bij PC-gebruikers. Iedereen die tekstverwerkingsbestanden wilde uitwisselen, moest WordPerfect hebben of een WordPerfect-compatibel programma. Nu Microsoft met Windows 95 een groot deel van de PC-markt in handen heeft gekregen, is

58 In Pascal (een oudere programmeertaal) kunnen variabelen onder andere worden geïnitieerd als 'integer' of als 'long integer'. Een integer kan maximaal de waarde (-)32767 aannemen en een long integer maximaal de waarde (-)2147483647.

59 Capers Jones, 'Dangerous dates for software applications', Versie 2, 24 maart 1998, <http://www.year2000.com/archive/NF dangers.html>. Dit artikel gaat in op de diverse data waarop tellers in veel gebruikte programma's hun maximum bereiken.

60 Er wordt echter ook gewaarschuwd dat sommige programmeurs het getal 999.999.999 bij de Unix-datumteller hebben gebruikt om het einde van een file aan te geven. Dit getal correspondeert met de datum 8 september 2001. Zie hierover ook het artikel genoemd in de vorige noot.

61 P. de Waard, 'Dow Jones-bug', *Volkskrant*, 6 mei 1998, p. 17.

62 Zie de subparagraaf 'Hoe konden die programmeurs zo stom zijn?' aan het begin van dit artikel.

in het kielzog daarvan gebruik van het tekstverwerkingspakket Word vrijwel onvermijdelijk geworden.

Wie niet meegaat met de trends wordt op den duur toch gedwongen te moderniseren. De hardware voor oude software zal ook verouderen en reserveonderdelen worden schaarser en duurder, want voor high-tech-producten als computerchips geldt dat ze alleen als massaproduct kosteneffectief zijn. Verder wordt het moeilijker personeel te krijgen dat met de verouderde software overweg kan. Secretariaesseopleidingen richten zich bijvoorbeeld niet meer op oude versies van WordPerfect maar op nieuwe van Word. Ook de technische kennis van de software en zelfs de taal waarin die is geschreven, is minder voorhanden. Onderhoud van de software is dan steeds moeilijker te krijgen en duurder. Softwarehuizen moeten immers met hun personeel en de software mee met de markt. Het beschikbaar houden van capaciteit voor steeds minder gebruikers van oude software wordt door schaalverkleining en het incourant raken van technieken steeds duurder.

De klant zelf beïnvloedt ook de levensduur van software. De eisen die hij aan de software stelt zijn namelijk niet stabiel. Als hij zijn bedrijfsvoering verandert of uitbreidt veranderen ook zijn eisen. Dat kan het noodzakelijk maken de software aan te passen of te vervangen voordat de markt hem daartoe dwingt.

Verder kan de overheid invloed hebben op de levensduur van software. Bijvoorbeeld door haar eisen aan de beveiliging van automatiseringssystemen⁶³, het archiveren van (financiële) gegevens voor de belastingdienst, en de veiligheidsnormen bij productie-inrichtingen. Verder moet software voor de uitvoering van wetten en andere regels worden aangepast bij wijzigingen in die wet- en regelgeving. Loonadministratiepakketten bijvoorbeeld moeten soms worden aangepast als de regelingen over de inkomstenbelasting of de sociale verzekeringen veranderen.

Een algemene levensduurverwachting van software is niet te geven omdat de bepalende factoren per programma verschillen. Hieronder worden enkele factoren uitgediept waarmee soms de verwachte levensduur van specifieke software kan worden vastgesteld.

1. Bij sommige soorten software veranderen de functionaliteitseisen niet zo snel of zelfs helemaal niet, waardoor een langere levensduur meer voor de hand ligt. De boekhoudkundige regels van een debiteurenadministratie bijvoorbeeld veranderen haast niet, terwijl de functionele eisen aan een Internet-browser zich vaak wijzigen, doordat er steeds nieuwe technieken komen om Internet-pagina's te maken. Van software die in chips is gebrand, is het vaak niet de bedoeling dat die wordt aangepast tijdens de levensduur van de machine waarin de chip zit.⁶⁴ Dan is de levensverwachting van die zogenaamde embedded software te koppelen aan de levensverwachting van de machine.

2. Bij grote (maatwerk)softwarepakketten waarvoor jaren nodig zijn om die te ontwerpen of op maat te maken en in het bedrijf in te voeren, ligt een langere levensverwachting meer voor de hand dan bij een standaardpakket dat men in een uur kan vervangen. Grote automatiseringssystemen die verweven zijn met de hele bedrijfsvoering kunnen niet in

Een algemene levensduurverwachting van software is niet te geven.

één keer worden vervangen of in korte tijd drastisch worden aangepast. Ze worden stukje bij beetje aangepast aan nieuwe eisen of 'upgraded' met nieuwe technieken en functionaliteiten. Daarom draaien in veel computersystemen van vooral grote bedrijven nog steeds delen van oude programma's, weliswaar met allerlei aanpassingen en toevoegingen. De verwachte levensduur van dergelijke complexe, moeilijk direct te vervangen software, of delen daarvan, is in principe dan ook groter.

3. Onder omstandigheden is ook van modulair opgebouwde software een langere levensduur te verwachten. Iedere module biedt een set functies waarbij de afnemer kiest welke modules en functies hij in huis haalt. Hierdoor kan hij gemakkelijker zijn systeem aanpassen aan zijn wensen. Hij kan van sommige modules nieuwere versies kiezen, terwijl hij van andere de oude gebruikt. Maar soms ondersteunen leveranciers dat niet, bijvoorbeeld omdat alleen modules met hetzelfde versienummer met elkaar samenwerken.

4. Programma's waarvan bekend is dat zij regelmatig moeten worden aangepast aan overheids-wensen zullen een kortere levensverwachting hebben dan programma's waarvoor dat niet geldt.

5. Voor programma's waarbij de verwerkingssnelheid en capaciteit belangrijk is, ligt regelmatig vervangen of aanpassen meer voor de hand dan bij andere programma's. Een programma dat een productieproces regelt zal, zolang dat productieproces zelf niet verandert, in principe niet hoeven worden aangepast. Het productieproces zelf bepaalt vaak de maximumsnelheid waarop gewerkt wordt. Daarentegen zal een programma dat berekeningen uitvoert waar een gebruiker op moet wachten, zoals voor de beeldopbouw bij een CAD-CAM-programma⁶⁵, meestal worden vervangen zodra snellere programma's uitkomen, bijvoorbeeld programma's die met nieuwe, snellere hardware overweg kunnen.

Met onder andere deze factoren kan men de gemiddelde levensverwachting inschatten die een afnemer mag hebben van software. Hiervoor zal men experts moeten raadplegen.

Met het vaststellen van de gemiddelde levensduur van bepaalde software is nog niet beantwoord hoe lang de afnemer in een geval mag verwachten dat die software werkt volgens de overeengekomen specificaties. De volgende subparagraaf behandelt hoe omstandigheden de gerechtvaardigde verwachtingen in een specifiek geval beïnvloeden.

De invloed van de omstandigheden van het specifieke geval

De duidelijkste invloed op de tijd dat een afnemer mag verwachten dat de geleverde software goed werkt is de vermelding van een uiterste gebruiksdatum in het leverantiecontract. Maar zo'n bepaling

63 Denk aan de verplichte beveiliging van persoonsgegevens involge de Wet persoonsregistraties of aan de gedachten in overheidskringen om encryptie in het algemeen juist aan banden te leggen om (georganiseerde) criminaliteit beter te kunnen opsporen.

64 Soms is er wel een mogelijkheid om deze chips aan te passen. Bijvoorbeeld door chips te gebruiken die opnieuw kunnen worden geprogrammeerd (een voorbeeld hiervan is zogenaamde Flashbios op moderne moederborden en videokaarten in PC's), of door ervoor te zorgen dat de chip los in een voetje zit zodat die gemakkelijk kan worden vervangen.

65 Met CAD-CAM-programma's kan men complexe, technische, eventueel driedimensionale tekeningen maken, bijvoorbeeld ontwerptekeningen van nieuwe chips. Omdat ze veel gegevens, snel en efficiënt, tegelijk moeten verwerken, hebben ze sterke computers met veel werkgeheugen nodig.

staat er in de praktijk vrijwel nooit in. Toch kunnen de inhoud van de overeenkomst en de overige omstandigheden de verwachtingen beïnvloeden. In de overeenkomst moet worden gekeken naar bepalingen die iets te maken hebben met het gebruik van de software in de toekomst. Bij de overige omstandigheden moeten vooral de situatie van de afnemer en de eisen aan de levensduur bij de software die daaruit voortvloeien onderzocht worden.

De volgende bepalingen en omstandigheden kunnen invloed hebben op de levensduurverwachtingen van de afnemer.

Licentievoorwaarden

Doorgaans worden licenties voor onbepaalde tijd gegeven voor software. Maar als de licentie voor een zekere periode is aangegaan, kan daaruit worden afgeleid dat de software ten minste die tijd functioneert. In dat geval zou kunnen worden gesteld dat de software wordt verhuurd. De afnemer heeft bij een periodieke licentie immers niet een permanent recht om de software te gebruiken. Als iemand een winkelpand huurt voor een periode van vijf jaar en het pand is na drie jaar niet meer te gebruiken doordat er gaten in de muren vallen, dan is de geleverde prestatie niet conform het contract. Vooral als de betaling voor de licentie over de periode is verdeeld, is die conclusie gerechtvaardigd. De betaling is dan gekoppeld aan het periodieke gebruik.

Onderhoudsbepalingen

Als een onderhoudscontract voor een bepaalde tijd is aangegaan, is dat een indicatie voor de levensduur die de afnemer mag verwachten. Een afnemer zal een onderhoudscontract bedingen om zich ervan te verzekeren dat de programmatuur betrouwbaar en goed blijft in de overeengekomen onderhoudsperiode. Hieruit blijkt ook duidelijk dat de software bedoeld is om ten minste in die tijd te worden gebruikt.

Een onderhoudscontract voor een bepaalde tijd is een indicatie voor de levensduur die de afnemer mag verwachten.

Anderzijds kan de afwezigheid van een onderhoudscontract onder omstandigheden duiden op een korte levensverwachting van de software. Dit kan vooral zo zijn als een leverancier expliciet verklaart dat voor de correcte werking onderhoud noodzakelijk is. De vraag is dan of de leverancier niet moet waarschuwen omdat hij niet alleen de correcte werking niet kan garanderen, maar ook omdat hoogstwaarschijnlijk de software op een tijdstip niet meer goed functioneert. De volgende subparagraaf behandelt die mededelingsplicht.

Het recht op of een plicht tot afname van nieuwe versies

Als in het contract bepalingen staan over nieuwe toekomstige versies van geleverde software geeft dit de afnemer een indicatie van de periode dat hij mag verwachten dat zijn programma normaal werkt. Maar het kan de verwachtingen zowel beperken als verlengen, afhankelijk van wat er over nieuwe versies staat. Als het contract bepaalt dat de leverancier alleen ser-

vice biedt en updates levert voor nieuwe versies, kan dit een indicatie zijn dat de levensduur beperkt is tot de release van de volgende versie. Maar ook kan zijn bepaald dat de afnemer een periode recht heeft op nieuwe versies. Daaruit kan de afnemer afleiden dat hij in die tijd een werkende versie heeft.

Het kenbare bijzonder gebruik waarvoor de software is bestemd

Een bepaald programma is niet bij iedere afnemer even lang in gebruik of bruikbaar. Dit hangt af van het doel waarvoor het programma is aangeschaft en eventueel van de planning van de automatiseringsactiviteiten van de afnemer. Stel dat voor een bepaald type software de algemene levensverwachting op vijf jaar wordt vastgesteld en een pakket van dat type is in 1992 geleverd, dan kan men stellen dat de millenniumbug geen reden is om aan te nemen dat de gerechtvaardigde verwachtingen van de afnemer geschaad worden. Maar als hij hetzelfde pakket aanschaft om in een automatiseringssysteem te bouwen voor een project dat tien jaar gaat duren, kan de conclusie anders zijn. Als het contract verwijst naar dit gebruik van de software, dan mag de afnemer erop vertrouwen dat de software geschikt is voor die tien jaar. Ook als er geen directe verwijzing in het contract staat naar het beoogde gebruik de komende tien jaar, dan kan het feit dat de leverancier dat wist ertoe leiden dat de gebruiker dit langere gebruik ook mag verwachten. De leverancier kan in dat geval namelijk een mededelingsplicht hebben tegenover zijn afnemer. Zie ook de volgende subparagraaf.

Het feit dat er is aangesloten bij reeds aanwezige (oudere) software of apparatuur

Van software die speciaal ontwikkeld wordt om in een oudere IT-omgeving te draaien mag om twee redenen een kortere levensduur worden verwacht. Allereerst moet de programmeur vaak aansluiten bij de gebruikte technieken en gemaakte keuzen, bijvoorbeeld de tellers. Daarnaast moet een programmeur bij zijn keuzen er rekening mee houden dat het programma minder lang gebruikt wordt omdat de omgeving waarin het moet draaien een korter leven beschoren is.

Lange implementatieperiode

Als aanpassen en implementeren van een programma veel tijd en inspanning kosten kan dit een langere levensverwachting rechtvaardigen. Want het is zeer inefficiënt om veel geld uit te geven om een programma aan te passen en te implementeren dat al snel vervangen of ingrijpend aangepast moet worden. Dit geldt in het algemeen voor pakketten die zo aangepast moeten worden. Maar het kan zijn dat de afnemer vraagt een pakket van een type dat doorgaans makkelijk wordt geïmplementeerd, toch uitgebreid aan te passen. Dan verwacht de afnemer ook een langere levensduur. Als de leverancier hem niet zegt dat het aan te passen pakket niet geschikt is voor langer gebruik, terwijl de afnemer die gezien de investering verwacht, dan mag de afnemer een langere levensduur verwachten.

De prijs van de software

Als een softwarepakket veel goedkoper wordt aangeboden dan normaal, kan dat een indicatie zijn dat het een ouder pakket is of een pakket dat niet met de nieuwste technieken is gemaakt. Dat kan de ge-

rechtvaardigde levensduurverwachting temperen. Omgekeerd kan een hogere prijs een langere levensduurverwachting rechtvaardigen.

Conclusie

De verwachting die een afnemer van de levensduur van zijn software mag hebben, is afhankelijk van zeer uiteenlopende factoren. Deze verwachting hangt allereerst van het soort software af, maar ook de contractbepalingen en de leveringsomstandigheden zorgen ervoor dat de levensverwachting van een bepaald type software kan variëren.

De mededelings- en onderzoeksplichten

Bij de bepaling van wat de afnemer mag verwachten van de levensduur van geleverde software moet men ook kijken naar de mededelings- en onderzoeksplichten van partijen. Had de leverancier de afnemer moeten wijzen op de beperkte levensduur door de millenniumbug of had de afnemer zich op dit punt beter moeten informeren? Deze subparagraaf beschrijft eerst kort wat de plichten inhouden en wat de gevolgen kunnen zijn van nalatigheid. Verder wordt gekeken wanneer in het kader van het niet nakomen van de mededelings- en onderzoeksplichten, een mogelijke wanprestatie van de leverancier is vast te stellen.

De mededelings- en onderzoeksplichten van partijen bij overeenkomsten zijn in de eerste plaats ontwikkeld in de rechtspraak over dwaling, met name bij koopovereenkomsten. In het arrest Baris/Riezenkamp⁶⁶ behandelde de Hoge Raad beide plichten voor het eerst naast elkaar. Voorop werd gesteld dat partijen die met elkaar contracteren in een rechtsverhouding staan die wordt beheerst door de goede trouw. Het Nieuw Burgerlijk Wetboek spreekt van redelijkheid en billijkheid. Dit betekent volgens de Hoge Raad allereerst dat de koper een plicht heeft om voldoende onderzoek te plegen om te voorkomen dat hij met een verkeerde voorstelling van zaken de overeenkomst aangaat. Als hij deze onderzoeksplicht niet 'nakomt' draagt hij het risico van de verkeerde voorstelling van zaken die hij had toen hij de overeenkomst aanging, en kan hij zich niet op dwaling beroepen. De mededelingen van de verkoper begrenzen deze onderzoeksplicht. In de regel mag men afgaan op mededelingen van de verkoper, aldus de Hoge Raad.

In latere arresten heeft de Hoge Raad op grond van de goede trouw aangenomen dat op de verkoper ook een plicht kan rusten om mededelingen te doen over het verkochte. In het arrest Van der Beek/Van Dartel⁶⁷ bijvoorbeeld verzweeg de verkoper van een huis een aanschrijven van de gemeente waarin stond dat het huis bij onvoldoende bewoning zou worden gevorderd. De koper mocht zich daarom beroepen op dwaling. In dit arrest en twee latere bepaalde de Hoge Raad ook wat geldt als er naast de mededelingsplicht van de ene partij een onderzoeksplicht van de andere bestaat.⁶⁸

In het arrest Van Geest/Nederhof ging het om de verkoop van een tweedehands auto waarbij de verkoper verzweeg dat de wagen een schadeverleden had.⁶⁹ Vastgesteld werd dat de koopster wat lichtvaardig had gehandeld door als autoleek de wagen niet te laten onderzoeken, bijvoorbeeld door een ANWB-keuring te laten doen. Het Hof concludeerde dat zij zich daarom niet kon beroepen op dwa-

De mededelingen van de verkoper begrenzen de onderzoeksplicht van de koper.

ling. Maar de Hoge Raad bepaalde dat deze onderzoeksplicht de mededelingsplicht van de verkoper niet ophief, omdat de mededelingsplicht:

'(..) juist ertoe strekt ook aan de onvoorzichtige koper bescherming te bieden tegen de nadelige gevolgen van dwaling veroorzaakt door het verzwijgen van relevante gegevens.' (r.o. 3.4).

Nieuwenhuis geeft daar een goede en mooie rationalisering voor:

'het verwijt van lichtvaardigheid ten aanzien van het eigenbelang weegt minder zwaar dan het gebrek aan contractuele naastenliefde met betrekking tot het belang van de wederpartij.'⁷⁰

Veel schrijvers wijzen erop dat de afweging van de mededelings- en onderzoeksplichten niet alleen van belang is voor het dwalingsvraagstuk, maar ook om een wanprestatie vast te stellen.⁷¹ Bij de vraag of er sprake is van wanprestatie is van belang of de prestatie voldoet aan de gerechtvaardigde verwachtingen van de afnemer. Relevant zijn dan de mededelingen die de leverancier wel en niet deed en in hoeverre de afnemer de plicht had zelf de wezenlijke feiten boven water te halen.

Hijma wijst erop dat er wel een verschil is in de rechtsgevolgen van dwaling of wanprestatie. Bij aanneming van dwaling kan alleen de rechtshandeling vernietigd worden⁷², terwijl bij wanprestatie de overeenkomst ontbonden kan worden en een schadevergoeding (positief belang) mogelijk is⁷³. Daarom, stelt hij, moet bij een mogelijke wanprestatie voorzichtiger worden omgegaan met het aannemen van een mededelingsplicht dan bij dwaling. Maar diverse schrijvers menen dat een partij die zich op dwaling beroept soms toch een schadevergoeding kan krijgen.⁷⁴ Daarbij wijst Nieuwenhuis erop dat het verschil in rechtsgevolgen van dwaling en wanprestatie te verkleinen is door de 'eigen schuld'-regeling van artikel 6:101 BW.⁷⁵ Als men vaststelt dat schuldenaar een mededelingsplicht heeft geschonden, maar de schuldeiser tegelijk te verwijten is dat die niet genoeg onderzoek heeft gedaan naar de eigenschappen van de prestatie, dan is dat in eerste instantie een wanprestatie van de schuldenaar. Als de rechter daarna een schadevergoeding vaststelt moet hij rekening houden met de eigen schuld van de schuldeiser. Ook artikel 6:230 BW geeft de rechter bij een geslaagd beroep op dwaling de mogelijkheid op verzoek van een partij de overeenkomst aan te passen in plaats van te vernietigen. Zo kan hij ook bij dwaling rekening houden met de omstandigheden. Een voordeel hiervan is dat de rechter één set criteria kan hanteren als hij bij dwaling en wanprestatie onderzoeks- en mededelingsplichten afweegt.

Het volgende gaat over de vraag welke omstandigheden een rol spelen bij de afweging van onderzoeks- en mededelingsplichten in de millenniumproblematiek, met name in relatie tot de levensduur van software.

66 HR 15 november 1957, NJ 1958,67.

67 HR Raad 30 november 1973, NJ 1974, 97.

68 HR 4 december 1987, NJ 1988, 345 (Willart/Snijders) en HR 21 december 1990, NJ 1991, 251 (Van Geest/Nederhof).

69 Zie voor een uitgebreide behandeling van dit arrest Jac. Hijma in *Ars Aequi* 1991/9, p. 661 e.v.

70 J.H. Nieuwenhuis, 'Wat mogen koper en verkoper van elkaar verwachten?', *WPNR* 6304, 7 maart 1998, p. 156.

71 Zie voor een overzicht Tjittes, *De hoedanigheid van contractspartijen*, Diss. RUG 1994, p. 176.

72 Zie art. 6:228 lid 1 BW.

73 Zie art. 6:74 en 6:265 BW.

74 Tjittes, a.w. p. 176, 177 en M.M. van Rossum, 'Gebreken bij de koop van een Old Timer', *NTBR* 1994/9, p. 226.

75 J.H. Nieuwenhuis, a.w., p. 156.

De onderzoeksplicht

De onderzoeksplicht van de afnemer is de basis. Hij moet gezien het arrest Baris/Riezenkamp zelf zorgen dat hij niet met een verkeerd beeld een overeenkomst aangaat. Hoe ver gaat die plicht? Voorop staat dat een partij die wil kopen enige basiskennis moet hebben van de markt die hij opgaat. Het arrest Joba/Gerber geeft hier een voorbeeld van.⁷⁶ In deze zaak kocht een afnemer polystyreen in een verpakking waarin het materiaal beperkt houdbaar was volgens de fabrieksvoorschriften. Hierdoor kwam de handelswaar na verscheping naar Japan niet goed aan. Dit bleef voor rekening van de afnemer. De leverancier had geen mededelingsplicht voor het risico van de soort verpakking omdat hij volgens de overeenkomst had geleverd. Brunner stelt in een noot bij dit arrest:

De vorm van de softwareleveringsovereenkomst beïnvloedt de onderzoeksplicht.

'Wie zich begeeft in een tak van handel zonder enige kennis van zaken te hebben, kan er m.i. geen aanspraak op maken, dat hij door zijn contractuele wederpartij wordt behoed voor de gevolgen van zijn onkunde.'

Uit dit arrest volgt dat twee omstandigheden een rol spelen bij het vaststellen van de omvang van de onderzoeksplicht van de schuldeiser (en dus ook van de mededelingsplicht van de schuldenaar). De eerste is de deskundigheid van de schuldeiser. In de literatuur wordt aangenomen dat wanneer het om een particuliere, ondeskundige koper gaat er een mededelingsplicht bestaat.⁷⁷ De tweede is de aard van de overeenkomst. Het ging hier om een handelskoop. Daarbij zijn de zekerheid en snelheid van het rechtsverkeer van groot belang.⁷⁸ Transacties worden in grote volumes en met weinig tot geen direct contact overeen- en nagekomen. Daarin past het niet om een uitgebreide mededelingsplicht voor de verkoper aan te nemen en behoort een afnemer op de hoogte te zijn van de eigenschappen van de handelswaar. Een ondernemer die software afneemt zal geen software- of automatiseringsdeskundige zijn, maar van hem mag wel enige algemene kennis van software worden verwacht. Bovendien mag van een grotere onderneming met een IT-afdeling meer worden verwacht dan van een kleine die zijn IT-werk uitbesteedt. De vorm van de softwareleveringsovereenkomst beïnvloedt de onderzoeksplicht. De behandeling van de mededelingsplichten hierna gaat daarover.

Op het voorgaande na zijn er weinig criteria om de omvang van de onderzoeksplicht te bepalen. De gedane mededelingen en de mededelingsplicht van de wederpartij begrenzen de onderzoeksplicht. De afnemer mag in principe afgaan op een mededeling en heeft over dat onderwerp geen onderzoeksplicht meer. Als een wederpartij een mededelingsplicht verzuimt dan kan die zich er niet meer op beroepen dat de ander zijn onderzoeksplicht verzaakt.

Het volgende gaat eerst over de mededelingen die van belang zijn en verder over de omstandigheden

die een rol spelen bij het aannemen van een mededelingsplicht.

Gedane mededelingen

Mededelingen van een contractpartij komen in meerdere vormen voor en de waarde die een wederpartij eraan mag hechten kan door omstandigheden sterk verschillen. De sterkste mededelingen staan in het contract dat beide partijen ondertekenden. De informatie die de afnemer daaruit put is van grote waarde. Hetzelfde geldt voor mondelinge en schriftelijke garanties die daarnaast zijn gegeven. Bij de beoordeling van andere mededelingen spelen allerlei factoren een rol. Als het om een direct antwoord op een vraag gaat, is de waarde groter. Gaat het om een algemene aanprijzing, dan is de waarde kleiner. Ook bij een voorbehoud zoals 'bij mijn weten ...' is de waarde geringer.⁷⁹ Dan moet de wederpartij nader onderzoek doen en mag hij er niet van uitgaan dat de meegedeelde of geïmpliceerde feiten juist zijn. Een teken van twijfel zijn ook omstandigheden als een zeer lage prijs of andere voorbehouden van de wederpartij bij de prestatie.

In de praktijk worden zelden directe uitspraken gedaan over de levensduur van software. Onder 'De invloed van de omstandigheden van het specifieke geval' bleek al dat sommige contractvoorwaarden en omstandigheden indirect iets zeggen over de levensverwachting die de afnemer mag hebben van de software. Mededelingen over de beschikbaarheid van onderhoud en nieuwe versies bijvoorbeeld beïnvloeden ook of de afnemer nader onderzoek moest plegen naar de levensduur van software.

Mededelingsplicht

Voor het aannemen van een mededelingsplicht zijn er drie algemene eisen:⁸⁰

- a. de betrokkene kent de stand van zaken, of behoort die te kennen;
- b. hij beseft of moet beseffen dat de kwestie voor de ander belangrijk is;
- c. hij moet er rekening mee houden dat de ander dwaalt.

Maar er is een uitzondering. Van een partij kan soms niet worden verwacht dat hij zijn prestatie negatief afschildert. Niemand verwacht bijvoorbeeld dat een verkoper tegen een potentiële afnemer zegt dat deze de koopwaar aan de overkant van de straat voor de helft van de prijs kan krijgen.

Om dat te ondervangen formuleerde Hijma een vierde eis:

- d. de betrokkene behoort naar redelijke, in het verkeer gangbare opvattingen de ander uit de droom te helpen.

Met deze vier eisen kan men omstandigheden vinden die meespelen als vastgesteld moet worden of een leverancier van software met de millenniumbug een mededelingsplicht had.

Ad a De betrokkene kent de stand van zaken, of behoort die te kennen

Een excuus dat de leverancier kan opperen, is dat hij niet wist dat in de software de millenniumbug zat. Hierbij is belangrijk dat de meeste softwareleveranciers zich afficheren als softwaredeskundige en een afnemer die deskundigheid dus ook mag verwacht

76 HR 15 mei 1981, NJ 1981, 641 m.nt. CJHB (Joba/Gerber).

77 Zie voor een overzicht van de literatuur daarover Tjittes, a.w., p. 178-180.

78 Zie aldus Van Dunne, *Verbintenissenrecht*, Deel 2, 2e druk, 1993, p. 26-27.

79 Aldus de Hoge Raad 18 april 1986, NJ 1986, 747.

80 Deze zijn zo geformuleerd door Jac. Hijma, a.w. p. 661 e.v. Zie ook de bronnen die Hijma aanhaalt: MvA II, Parl. Gesch., Boek 6 NBW, het zeer interessante artikel van E. Cohen Henriquez, 'Spreken is zilver, zwijgen is fout', NJB 1976, p. 631 (sub 1) en Asser/Schut (1981), p. 125.

ten.⁸¹ Dit geldt ook als de leverancier software van derden doorlevert. Van professionele leveranciers mag men verwachten dat zij op de hoogte zijn van de essentiële, technische eigenschappen van hun producten. De levensduur van software is zo'n essentiële eigenschap. Niet gesteld kan worden dat pas sinds kort bekend is dat de levensduur van software ook afhangt van hoe bijvoorbeeld de tellers zijn ingesteld, want zonder die kennis kan een programmeur geen programma schrijven. Bovendien komt de datumteller in veel programma's op veel plaatsen voor en is het dus een bekend fenomeen. Verder zijn programmeurs bij sommige toepassingen al ruim voor het jaar 2000 geconfronteerd met de gevolgen van de tweecijferige jaarnotering, bijvoorbeeld in programma's die met geboortedata werken, of met gegevens over hypotheeken met een lange looptijd, of financiële en logistieke planningsprogramma's. Daarmee bestaan al (lang) voor het jaar 2000 problemen, dus die moesten worden aangepast. Het ontkennen van bekendheid met het probleem is dus waarschijnlijk geen sterk argument tegen het aannemen van een mededelingsplicht.

Ad b Betrokkene beseft of moet beseffen dat de kwestie voor de ander belangrijk is

Hiervoor is wezenlijk met welke levensduurverwachting van de afnemer de leverancier rekening moet houden. Hij moet beseffen dat de millenniumbug aanwezig is en wanneer die een probleem wordt, en wanneer dat belangrijk is voor de afnemer, want de bug veroorzaakt op een gegeven moment fouten in de software of maakt die zelfs onbruikbaar. Om te bepalen met welke levensduurverwachtingen van de afnemer de leverancier rekening moet houden, zijn de algemene levensverwachtingen van de software en de specifieke omstandigheden van het geval belangrijk. Zie daarvoor de vorige twee subparagrafen.

Ad c Betrokkene moet er rekening mee houden dat de ander dwaalt

Hierbij speelt de kennis en betrokkenheid van de afnemer bij het onderwerp een grote rol.⁸² Bij een afnemer met een eigen IT-afdeling die zelf de eindverantwoordelijkheid draagt voor het aanpassen of maken van software door de leverancier, zal de leverancier minder snel hoeven aan te nemen dat de afnemer zich niet bewust is van het gebruikte datumformaat en de gevolgen daarvan. Maar gaat het om een 'turnkey'-overeenkomst, waarbij de leverancier eindverantwoordelijk is en de afnemer niet direct betrokken is bij het ontwerpen en maken van de software, dan moet de leverancier sneller rekening houden met het feit dat de afnemer niet weet dat de millenniumbug aanwezig is.

Ad d Betrokkene behoort naar redelijke, in het verkeer gangbare opvattingen de ander uit de droom te helpen

Er zijn geen redenen waarom de leverancier de afnemer niet behoorde in te lichten over de aanwezigheid van de millenniumbug als hij wist dat dit wezenlijk was voor de afnemer. Volgens de verkeersopvattingen wordt dit zelfs van hem als deskundige verwacht.

Naast middel om een dwaling of wanprestatie vast te stellen kan het verzaken van een mededelingsplicht op zich een grond zijn voor schadevergoe-

ding. De Hoge Raad bepaalde dat als het niet nakomen van een mededelingsplicht in strijd is met de goede trouw, dat dan kan leiden tot een schadevergoedingsplicht.⁸³ De noot bij dit arrest gaat over de vraag wat de juridische grondslag voor de schadevergoedingsplicht is en oppert twee mogelijkheden: het schenden van de mededelingsplicht in strijd met de goede trouw is een onrechtmatige daad; of uit de goede trouw (redelijkheid en billijkheid) vloeit een verbintenis voort om bepaalde mededelingen te doen en de schending van die verbintenis is een tekort in de nakoming daarvan.

Met name bij een 'turnkey'-overeenkomst moet de leverancier er rekening mee houden dat de afnemer niet weet dat de millenniumbug aanwezig is.

Conclusie

De omvang van de onderzoeksplicht van de afnemer heeft geen duidelijke grenzen. Maar de gedane mededelingen en de mededelingsplicht van de leverancier zijn een afbakening. De onderzoeksplicht speelt bij het bepalen van een wanprestatie geen rol meer als de leverancier over de kwestie een mededeling doet of als de leverancier een mededelingsplicht heeft.

Om de omvang van de mededelingsplicht te bepalen speelt de voor de leverancier kenbare verwachting die de afnemer heeft van de levensduur van de software een grote rol. Deze kennis bepaalt of de leverancier zich bewust is van de problemen die de afnemer kan krijgen door de millenniumbug. Verder is bij de afweging het verschil in deskundigheid en de vraag wie eindverantwoordelijk is voor het ontwerpen en maken van de software van belang vanwege de vraag of de leverancier er rekening mee moest houden dat de afnemer niet op de hoogte was van de aanwezigheid en de gevolgen van de millenniumbug. Als wordt aangenomen dat de leverancier de afnemer had moeten meedelen dat de software een beperktere levensduur heeft dan de afnemer in principe mag verwachten, dan pleegt de leverancier wanprestatie. Hij levert dan software met een levensduur die korter is dan de afnemer mocht verwachten.

EFFECTUEERBAARHEID VAN EEN MILLENNIUMCLAIM

De vorige twee paragrafen gingen over de omstandigheden die in een geval de slaagkans beïnvloeden van een claim wegens wanprestatie tegen de leverancier van software met de millenniumbug. Maar al is die wanprestatie vastgesteld, dan kan het toch voorkomen dat de afnemer zijn claim niet (meer) kan effectueren.

In de eerste plaats spelen bij de effectueerbaarheid enkele praktische en economische overwegingen mee:

- Wil ik mijn leverancier wel aanspreken en zo misschien een goede of voor het bedrijf cruciale relatie op het spel zetten?

81 Zie over het belang van de deskundigheid van de schuldenaar voor het aannemen van een spreekplicht E. Cohen Henriquez, a.w., p. 631 (sub 2) en Jac. Hijma, a.w., p. 664.

82 E. Cohen Henriquez, a.w., p. 631 (sub 7) en Jac. Hijma a.w., p. 664.

83 HR 2 april 1993, NJ 1995, 94 m.nt. CJHB.

84 Zie bijvoorbeeld de zaak Glimmerveen/XTEC (Rb Den Bosch 4 februari 1994, *Computerrecht* 1994/4, p. 174) waarin de rechter een beroep op een dergelijke exoneratie toeliet. Dit had in dit geval een vergaand gevolg, daar de rechter de overeenkomst zelf had vernietigd en de leverancier het factuurbedrag moest terugbetalen. Er was dus uiteindelijk geen factuurbedrag verschuldigd onder het contract en de aansprakelijkheid van de leverancier was aldus beperkt tot f 0,00.

85 In de functionele specificaties wordt vermeld aan welke functionaliteits-eisen de software moet voldoen. Hierin kunnen, behalve de bewerkingen die de software moet kunnen uitvoeren, ook zaken als de snelheid waarmee dit gebeurt, het aantal gebruikers dat tegelijkertijd het programma kan gebruiken en de hoeveelheid data die het programma kan verwer-

- Wat zijn de kosten van een procedure en hoe zeker is de toewijsbaarheid van de claim, met andere woorden: wat is de slaagkans?
- Is mijn leverancier wel solvabel genoeg?

Daarnaast zijn er twee juridische gronden waarop een wanprestatieclaim kan stranden. De eerste zijn de exoneratiebedingen die in de meeste softwareleverantieovereenkomsten staan. Die sluiten de aansprakelijkheid van de leverancier meestal vergaand uit en blokkeren claims. Maar een leverancier kan zich in redelijkheid niet in alle omstandigheden daarop beroepen. De tweede is dat claims na verloop van tijd vervallen of verjaren als de schuldeiser te lang stilzit. Deze paragraaf behandelt beide juridische obstakels.

De inroepbaarheid van exoneratiebedingen bij millenniumclaims

Als is vastgesteld dat de gerechtvaardigde verwachtingen van de afnemer van een softwarepakket zijn geschaad door de millenniumbug kan er sprake zijn van een wanprestatie. Maar de vraag is of de afnemer zijn millenniumclaim tegen de leverancier kan effectueren. De meeste softwareleverantiecontracten perken de aansprakelijkheid van de leverancier namelijk vergaand in. De rechtspraak bepaalt evenwel dat een beroep op een exoneratiebeding soms in redelijkheid en billijkheid onaanvaardbaar is. Deze subparagraaf behandelt eerst de invloed van de exoneratiebedingen op millenniumclaims en daarna wanneer een beroep op exoneratiebedingen in strijd kan zijn met de redelijkheid en billijkheid.

De meeste softwareleverantiecontracten perken de aansprakelijkheid van de leverancier vergaand in.

ken, worden vastgelegd.

86 Zie voor meer info over de Fenit:

<http://www.fenit.nl>

87 Deze zijn uitgegeven in een losbladige bundel onder redactie van J.G.J. Janssen, W.F.R. Rinzema en D.W.F. Verkade, Samsom HD Tjeenk Willink, Alphen aan den Rijn 1991.

88 Zie over de beide sets voorwaarden nader D. Oosterbaan en E. Thole, 'Fenit of BIZA: met welke voorwaarden is men beter af', *IT en Recht*, Special 2000, december 1997, p. 5.

89 Zie bijvoorbeeld HR 8 januari 1926, *NJ* 1926, 203 (Sarong).

90 HR 19 mei 1967, *NJ* 1967, 261.

91 HR 26 maart 1926, *NJ* 1920, 476 (Surinaamse postbode) en HR 3 juni 1938, *NJ* 1938, 920 (Bovag I).

De leverancier kan zijn aansprakelijkheid op vele manieren en in vele gradaties inperken. Zo kan een maximumbedrag worden genoemd waarvoor een contractpartij aansprakelijk kan worden gesteld, bij automatiseringscontracten meestal het verschuldigde factuurbedrag of een gespecificeerd deel daarvan.⁸⁴ Verder beperken garantiebepalingen vaak de periode waarin claims wegens softwaregebreken kunnen worden ingediend, bijvoorbeeld tot drie maanden of een jaar na levering. Vaak worden ook drempels opgeworpen voor claims van de afnemer door de gebreken in de software waarvoor de leverancier aansprakelijk is te beperken tot een afwijking van de 'functionele specificaties'.⁸⁵ Bovendien staat vaak expliciet in het contract dat de leverancier niet garandeert dat de software zonder onderbrekingen of fouten werkt of dat hij alle fouten zal herstellen. Dat is niet zo uitzonderlijk omdat het leveren van foutloze software praktisch bijna onmogelijk is, zoals onder 'Wat mag de afnemer van software in het algemeen verwachten?' al uiteen is gezet.

Voor softwareleverantiecontracten worden de algemene voorwaarden van bijvoorbeeld de Fenit⁸⁶ of de 'modelcontracten automatisering'⁸⁷ van het Ministerie van Binnenlandse Zaken veel gebruikt. De Fenit is een brancheorganisatie van IT-leveranciers

en haar algemene voorwaarden zijn vanuit het perspectief van de leverancier opgesteld. De modelcontracten van het Ministerie van Binnenlandse Zaken zijn opgesteld als inkoopvoorwaarden van de overheid, maar worden ook daarbuiten ruim gebruikt als uitgangspunt, met name door grote IT-afnemers. Zij zijn meer geschreven vanuit het perspectief van de afnemer.⁸⁸

De exoneratie door een garantietermijn waarbinnen claims moeten worden ingediend, komt in beide sets voorwaarden voor. Bij de Fenit-voorwaarden is de garantietermijn drie maanden en bij de BiZa-voorwaarden een jaar.

Voor dit exoneratiebeding kan bij het millenniumprobleem een grote hindernis zijn voor claims van de afnemer. De millenniumbug wordt bij de oplevering niet opgemerkt en de afnemer spreekt de leverancier daar dus niet op aan. Zodra hij later als het programma datums uit de volgende eeuw moet verwerken tegen de bug aanloopt, is de garantietermijn meestal verstreken. Dat betekent totale uitsluiting van aansprakelijkheid van de leverancier voor de gevolgen van de millenniumbug. Het is dus van groot belang om te weten of de leverancier zich redelijkerwijze mag beroepen op exoneratiebedingen in de contracten.

In artikel 1374 lid 3 van het oud BW staat sinds 1838 de regel dat overeenkomsten 'te goeder trouw worden ten uitvoer gebracht'. Deze regel heeft bijna de hele eerste eeuw van zijn bestaan een relatief onbelangrijke rol gespeeld. De goede trouw was alleen van belang bij de wijze van uitvoering van de overeenkomst en had dus alleen een aanvullende werking. Een beperkende werking wees de Hoge Raad af⁸⁹, want het eerste lid van artikel 1374 bepaalde dat gemaakte afspraken moeten worden nagekomen: 'Alle wettiglijk gemaakte overeenkomsten strekken den genen die dezelfde hebben aangegaan tot wet.' Pas in het arrest Saladin/HBU erkende de Hoge Raad voor het eerst dat het afhangt van 'tal van omstandigheden' of een partij een beroep kan doen op een exoneratiebeding⁹⁰ en noemde enkele omstandigheden die van belang kunnen zijn:

- de zwaarte van de schuld;
- de betrokken belangen;
- de aard en verdere inhoud van de overeenkomst;
- de maatschappelijke positie en onderlinge verhouding van partijen;
- de wijze waarop de overeenkomst tot stand kwam;
- de mate waarin de wederpartij zich de inhoud en strekking van het exoneratiebeding bewust is geweest.

Bij de eerste omstandigheid moet worden opgemerkt dat al vóór deze uitspraak was aangenomen dat men zich in geval van opzet of grove schuld niet kon beroepen op exoneratiebedingen. Dat zou in strijd zijn met de goede zeden en de openbare orde. Iemand zou anders door een contract te tekenen dat de aansprakelijkheid van de wederpartij vergaand uitsluit volledig zijn overgeleverd aan de willekeur van die andere partij. Wel werd in principe geaccepteerd dat de aansprakelijkheid voor opzet en grove schuld van ondergeschikten van een contractpartij was uitgesloten.⁹¹

In het Pseudovogelpesst-arrest noemt de Hoge Raad

een concreet voorbeeld waarbij men kan aannemen dat een partij geen beroep kan doen op een exonerationbeding:

'(...) dat immers ... de verkoper die goederen heeft geleverd waarvan hem vóór of bij de levering bekend was dat zij gebreken hadden die de koper niet behoefde te verwachten, niet met succes een beroep kan doen op een contractueel beding tot uitsluiting of beperking van zijn aansprakelijkheid voor de schade die als voorzienbaar gevolg van de aanwezigheid van deze gebreken aan de koper wordt toegebracht; dat in het algemeen bekendheid met de gebreken bij degene die de verkoper in zijn bedrijf belast heeft met de leiding van de uitvoering van de betreffende verkoopcontracten, wat dit betreft gelijk gesteld moet worden met bekendheid bij de verkoper zelf.'⁹²

De Hoge Raad vervolgt met te zeggen dat wanneer de wetenschap van het gebrek bij een niet-leidinggevende ondergeschikte ligt of als de verkoper zelf of één van zijn ondergeschikten een ernstig verwijt te maken is dat zij niet op de hoogte zijn van het gebrek, het antwoord op de vraag of de verkoper vanwege de goede trouw ook geen beroep kan doen op een exonerationbeding afhankelijk is van de weging van tal van omstandigheden (de afweging uit het arrest Saladin/HBU). Hierbij geeft de Hoge Raad opnieuw enkele omstandigheden die kunnen meespelen. Nieuw zijn dan:

- de strekking van het beding;
- het gedrag van de koper aangaande de gebreken of de schade die daardoor ontstond;
- de verhouding tussen de beperking van de aansprakelijkheid en de grootte van de voorzienbare schade.

In het Ontwateringspomp-arrest past de Hoge Raad zijn mening nog iets aan wat betreft de gevolgen van het verwijtbaar niet op de hoogte zijn van de verkoper zelf.⁹³ Het ging om de verkoop van een huis waarvan de fundering was aangetast door een ontwateringspomp die de verkoper had aangebracht. Niet duidelijk was of de verkoper van de aantasting wist, maar de koper stelde dat, omdat de verkoper ingenieur en architect was, hem in ieder geval een ernstig verwijt te maken was dat hij van de aantasting niet wist. De Hoge Raad bepaalde dat wanneer die verwijtbaarheid werd aangetoond, de verkoper geen beroep op een exonerationbeding kon doen. Daarbij repte de Hoge Raad niet meer van een weging van omstandigheden. Wel hechtte hij er belang aan dat de verkoper de koper 'zelfs niet op de hoogte had gebracht van de aanwezigheid van de pomp'. De annotator van dit arrest interpreteert deze toevoeging zo dat, wanneer de verkoper de aanwezigheid van de pomp wel had gemeld, de overige omstandigheden wel gewogen moesten worden om te bepalen of een beroep op het exonerationbeding mogelijk was.

Als in een concreet geval moet worden getoetst of de leverancier van software met de millenniumbug een beroep kan doen op de exonerationbedingen in zijn leveringscontract, dan moet eerst worden gekeken of de criteria van het Pseudovogelpest-arrest (en de latere verfijning daarvan) kunnen worden toegepast. Dit arrest geeft namelijk concrete toetsingsregels, terwijl het Saladin/HBU-arrest alleen

de omstandigheden noemt die meespelen bij de afweging.

De regel die de Hoge Raad in het Pseudovogelpest-arrest formuleert, is gericht op koopovereenkomsten, want in het citaat is sprake van de *verkoper* die zich niet kan beroepen op exonerationbedingen in zijn contract als hij gebreken kent die de afnemer niet hoeft te verwachten. In de paragraaf 'Wanprestatie bij softwarelevering: algemene vragen' is stilgestaan bij de vraag of en zo ja, wanneer de levering van software als een verkoop kan worden gezien. De conclusie was dat dit bij de levering van standaardpakketten waarschijnlijk is, maar bij maatwerksoftware vaak niet. Daarbij was de grens tussen beide niet helder. Maar waarom zou de regel van de Hoge Raad niet ook gelden voor prestaties die geleverd worden op grond van niet-koopovereenkomsten? Als een partij weet dat hij een prestatie levert waaraan een gebrek kleefte dat de afnemer niet hoeft te verwachten is dit waarschijnlijk afkeurenswaardig onder elke overeenkomst. Het Pseudovogelpest-criterium is dus waarschijnlijk ook bij maatwerksoftwareleveringen te gebruiken.

Het Pseudovogelpest-criterium is waarschijnlijk ook bij maatwerksoftwareleveringen te gebruiken.

Bij de toepassing van het Pseudovogelpest-criterium zijn de volgende voorwaarden van belang:

1. de verkoper (leverancier) was op de hoogte van de gebreken die aan zijn product kleefden. Daarbij is degene die de verkoper in zijn bedrijf heeft belast met de leiding van de uitvoering van de desbetreffende verkoopcontracten gelijk aan de verkoper;
- 1a. of de verkoper is een ernstig verwijt te maken dat hij niet op de hoogte was van gebreken (aanvullende regel van het Ontwateringspomp-arrest);
2. het moet gaan om gebreken die de koper niet behoefde te verwachten;
3. de schade die uit deze gebreken voortvloeit moet de leverancier kunnen voorzien.

Ad 1(a)

Bij de behandeling van de mededelingsplicht in de vorige paragraaf kwam al aan de orde dat de verkoper waarschijnlijk moeilijk staande kan houden dat hij niet op de hoogte was van de aanwezigheid van de millenniumbug. Het gaat immers om een niet verborgen gebrek aan een essentiële eigenschap. Bovendien kan hem snel een ernstig verwijt worden gemaakt dat hij hiervan niet op de hoogte was als deskundige professional (de verkoper in het Ontwateringspomp-arrest was een particulier!).

Ad 2

Of de afnemer de bug niet behoefde te verwachten, hangt af van de levensduurverwachtingen die de afnemer redelijkerwijs mocht hebben van de software. De bepaling daarvan is, zoals in vorige paragrafen bleek, van zeer veel omstandigheden afhankelijk. Men kan zich nog afvragen of de bekendheid die de afgelopen tijd aan de millenniumbug is gegeven in

92 HR 20 februari 1976, NJ 1976, 486 (Pseudovogelpest).

93 HR 7 mei 1982, NJ 1083, 509 met noot CJHB. (Ontwateringspomp).

dit opzicht nog een rol speelt. Het antwoord is: waarschijnlijk niet, want de afnemer mag ervan uitgaan dat zijn leverancier beter op de hoogte is van deze problematiek, er rekening mee houdt en hem zal inlichten als het tegendeel het geval is. Want zoals in de vorige paragraaf al bleek gaat de mededelingsplicht vóór de onderzoeksplicht.

Ad 3

Bij het toetsen aan deze voorwaarde moet men verschillende soorten schade onderscheiden. De eerste wordt gevormd door de kosten waarvan te voorzien is dat die gemaakt moeten worden om de software aan te passen of (voortijdig) te vervangen. Dit kan tot bedrijfsstagnatie leiden met daaraan verbonden kosten, met name als men met de aanpak van de bug te laat begint. Beide schadevormen kunnen vaak hoger uitvallen doordat op de markt voor IT-specialisten steeds grotere schaarste heerst.

De vraag is wanneer de leverancier al die kosten kon voorzien. In ieder geval zijn de kosten van het voortijdig vervangen of aanpassen van de software te voorzien omdat die direct volgen uit de aanwezigheid van de millenniumbug en de onmogelijkheid om de software na de eeuwwisseling nog te gebruiken. Voor de extra kosten door bedrijfsstagnatie geldt hetzelfde, maar de stijging van de kosten door schaarste op de IT-markt kon de verkoper minder voorzien, want die is pas de laatste drie à vier jaar ontstaan. Die schaarste wordt deels wel veroorzaakt door de millenniumbug, maar het is misschien wat veel gevraagd om van een IT-leverancier macro-economische voorspellingen voor de IT-markt te verwachten.⁹⁴

Bij toetsing aan het Pseudovogelpest-criterium moet de rechter waarschijnlijk vooral de tweede voorwaarde afwegen. De leverancier, althans de leidinggevenden van zijn onderneming, moet waarschijnlijk altijd bekend worden geacht met de aanwezigheid van de bug. Maar de relevantie van die wetenschap hangt af van de levensduurverwachting die de afnemer van de software mag hebben. Als die zo is dat de software niet meer gebruikt wordt op het moment dat de bug opspeelt, is de leverancier weinig te verwijten. Maar als de verwachting van de afnemer is dat de software datums in de volgende eeuw kan verwerken dan heeft de leverancier wel verwijtbaar gehandeld. Verder is van belang te beseffen dat meestal de gerechtvaardigde levensduurverwachting van software geschat moet worden. Een leverancier moet die ook schatten. Men kan zich afvragen of een kleine misschatting van de leverancier direct zo'n groot verwijt oplevert dat hij zich in redelijkheid en billijkheid niet meer kan beroepen op de overeengekomen exoneratiebedingen. Het uitsluiten van aansprakelijkheid voor eigen fouten is op zich immers toegestaan. Maar de vraag is of van de leverancier (soms) niet verwacht mag worden dat hij een zekere marge aanhoudt nu het regelmatig voorkomt dat afnemers software langer gebruiken dan de gemiddelde levensduur.

Als het Pseudovogelpest-criterium niet direct kan worden toegepast, moet men terugvallen op de algemenere criteria van het Saladin/HBU-arrest en de latere aanvulling daarop van de Hoge Raad. Ook in dat geval hangt veel van de levensduurverwachting af die de afnemer van de software mocht hebben. Die is namelijk mede bepalend voor de mate van schuld die de leverancier kan worden toegerekend.

Voor de overige omstandigheden uit de Saladin/HBU-afweging zijn de volgende opmerkingen nog te maken:

- de leverancier is doorgaans veel deskundiger dan de afnemer;
- de exoneratiebedingen heeft de leverancier vaak eenzijdig opgesteld in de vorm van algemene voorwaarden;
- men kan zich afvragen of partijen deze bedingen wel hebben bedoeld voor de dekking van schade die de leverancier kan voorzien;
- bepaalde exoneratiebedingen sluiten schade volledig uit van vergoeding terwijl die zeer hoog kan oplopen en de leverancier die relatief goedkoop kan voorkomen.

Conclusie

De beantwoording van de vraag of de leverancier zich in redelijkheid en billijkheid kan beroepen op de overeengekomen exoneratiebedingen hangt waarschijnlijk nauw samen met de gerechtvaardigde levensduurverwachting die de afnemer mocht hebben van de software die hem geleverd is. Die gerechtvaardigde levensduurverwachting bepaalt of de leverancier kan weten dat de afnemer schade zal lijden door de bug. Het bepalen van de gerechtvaardigde levensduurverwachting van geleverde software is bijna altijd een schatting. De rechter zal daarom in gevallen waarin niet helder is dat de gerechtvaardigde levensduurverwachtingen zijn geschonden waarschijnlijk ook kijken naar de omstandigheden die in het Saladin/HBU-arrest relevant genoemd worden.

Indien de leverancier software heeft geleverd waarvan hij wist of had moeten weten dat deze de millenniumbug bevat, en bovendien wist dat de afnemer daardoor schade zal lijden, dan wordt naar alle waarschijnlijkheid een beroep op een exoneratiebeding afgewezen, gelet op het Pseudovogelpest-arrest.

Verjaring en rechtsverwerking van wanprestatieclaims

In de eerste paragraaf staat dat het Millennium Platform adviseert om bij de aanpak van het millenniumprobleem voorrang te geven aan de technici. Het is beter het probleem eerst op te lossen en daarna met de leverancier in discussie te gaan over wie de kosten daarvan moet dragen, want zo blijven die kosten zo laag mogelijk. Een reden om nu toch al aandacht te schenken aan de juridische aspecten is het gevaar dat mogelijke claims verjaren of door rechtsverwerking tenietgaan. Hieronder worden daarom kort de artikelen behandeld die in het Burgerlijk Wetboek de verjaring, rechtsverwerking en het voorkomen daarvan regelen.

Als een rechtsvordering verjaart gaat niet het recht zelf verloren, maar alleen de rechtsvordering. Het recht wordt dan een natuurlijke verbintenis⁹⁵ die de rechthebbende niet meer kan afdwingen.⁹⁶ De algemene verjaringsregeling van het BW is neergelegd in titel 11 van Boek 3. Deze geldt voor alle verjaringen voorzover de wet daar niet elders van afwijkt.⁹⁷ Voor de wanprestatieclaims in dit artikel zijn van deze titel vooral de artikelen 310, 311 en 312 van belang.

Vorderingen tot herstel

Artikel 3:311 BW is het eenvoudigst toe te passen. Het bepaalt dat de rechtsvordering tot herstel van

94 Bij de uiteindelijke toewijzing van een schadevergoeding zal, met name bij de schade door bedrijfsstagnatie, moeten worden gekeken of de afnemer door de bekendheid die hij kon hebben met de millenniumbug de problematiek niet eerder had moeten aanpakken. Deze extra kosten zouden dan door de 'eigen schuld'-regeling van art. 6:102 BW voor rekening van de afnemer kunnen worden gelaten.

95 Zie over natuurlijke verbintenissen de artikelen 6:3 - 6:5 BW.

96 Toelichting Meijers, Parl. Gesch. Boek 3, p. 917.

97 Asser-Hartkamp I, inleiding van nr. 664.

een tekortkoming in de nakoming vijf jaar nadat de schuldeiser met de tekortkoming bekend is geworden, verjaart en anders twintig jaar nadat de tekortkoming is ontstaan. Zodra de afnemer dus weet dat hem software is geleverd met een millenniumbug, gaat de vijfjaarstermijn in voor de vordering tot herstel van die tekortkoming.

Vorderingen tot schadevergoeding

Artikel 3:310 BW regelt de verjaring van schadevergoedingsvorderingen.⁹⁸ Het bepaalt dat een rechtsvordering tot vergoeding van schade vijf jaar nadat de schuldeiser met de schade en de aansprakelijke persoon bekend is, verjaart, en twintig jaar na de gebeurtenis die de schade veroorzaakt. Bij het bepalen van de start van de vijfjaarstermijn is niet helemaal helder op welk moment de schuldeiser op de hoogte is van de schade. In ieder geval is niet nodig dat de schuldeiser precies weet hoe hoog de schade is.⁹⁹ Taxatie daarvan of herstel van het gebrek is niet nodig om de termijn te laten beginnen.

De literatuur is niet helder over schadeposten die pas later optreden. Hartkamp meent dat voor latere schadeposten die dus later bekend zijn aan de schuldeiser, de termijn pas begint als die schadeposten ontstaan.¹⁰⁰ Daarnaast stelt Hartkamp dat de schuldeiser bekend is met de schade, waarvan hij weet dat de afnemer haar in de toekomst zal lijden.¹⁰¹ Het onderscheid dat Hartkamp maakt tussen voorzienbare en onvoorzienbare toekomstige schade kan bij millenniumclaims tot onduidelijkheid leiden over het startpunt van de verjaringstermijn voor de vordering van sommige schadeposten. Als de afnemer bekend wordt met de millenniumbug, is duidelijk dat er kosten komen om die te verwijderen en begint voor deze kosten de verjaringstermijn als de bug ontdekt wordt. Maar onduidelijk is wat moet gelden voor schadeposten als bedrijfsstagnatie door de bug en latere claims van derden vanwege die bedrijfsstagnatie. Deze schadeposten kunnen optreden, maar zeker is dat niet. Of dit als bekendheid moet gelden in de zin van artikel 3:310 BW is onduidelijk.

Het gevolg van artikel 3:312 BW

Artikel 3:312 BW zorgt ervoor dat artikel 3:310 BW waarschijnlijk niet van belang is voor de verjaring van millenniumclaims bij wanprestatie. Het bepaalt namelijk dat: rechtsvorderingen ter zake van een tekortkoming in de nakoming (dus ook schadevergoedingsvorderingen ter zake van die tekortkomingen¹⁰²) niet later verjaren dan de rechtsvordering tot nakoming van de hoofdverplichting of, zo de tekortkoming vatbaar is voor herstel, de rechtsvordering tot herstel van de tekortkoming. De hoofdverplichting van een overeenkomst verjaart volgens artikel 307 BW vijf jaar na de dag waarop die vordering opeisbaar is. Maar meestal is de afnemer pas nadat de hoofdverplichting opeisbaar is geworden bekend met de aanwezigheid van de millenniumbug en start de vordering tot herstel van deze tekortkoming in de nakoming involge artikel 311 BW (zie hierboven) pas op dat latere moment. Alle schadevergoedingsvorderingen die door wanprestatie kunnen voortvloeien uit de millenniumbug in software zullen dus op zijn laatst vijf jaar nadat de afnemer weet dat de bug aanwezig is verjaren, samen met de vordering tot herstel van die tekortkoming. Het is alleen anders als de millenniumbug een tekortkoming in de nakoming oplevert die niet voor herstel vatbaar is, en de vordering tot schadevergoe-

Het gevaar dat mogelijke claims verjaren of door rechtsverwerking tenietgaan, is een reden om nu al aandacht te schenken aan de juridische aspecten van de millenniumbug.

ding dus samen met de vordering tot nakoming van de hoofdverplichting verjaart. Als de onherstelbare tekortkoming pas aan het licht komt nadat de vordering tot nakoming van de hoofdverplichting is verjaard, leidt dit tot het onbillijke resultaat dat de vordering tot schadevergoeding voor deze tekortkoming al verjaart voordat de schuldeiser zich er bewust van kan zijn. De millenniumbug kan altijd weggehaald worden, maar het kan zijn dat de software speciaal was bedoeld om te worden gebruikt voor één, aan een vaste tijd gebonden activiteit en de bug pas tijdens die activiteit naar voren komt. Dan is de tekortkoming dus onherstelbaar. In het hypothetische geval dat de software langer dan vijf jaar voor het tijdstip van de activiteit is geleverd, lijkt de claim van de afnemer voor deze tekortkoming dus al verjaard voor hij ermee bekend is.

De verjaring in de kooptitel van Boek 7

Artikel 7:23 lid 2 BW heeft voor vorderingen uit koopovereenkomsten een afwijkende verjaringstermijn. Het geeft een verjaringstermijn van twee jaar aan voor vorderingen gebaseerd op het feit dat, het geleverde niet aan de overeenkomst beantwoordt. Deze termijn begint te lopen zodra de afnemer van de tekortkoming in het geleverde op de hoogte is (of moest zijn) en dit meldt bij de leverancier. Op deze protestplicht wordt hieronder nader ingegaan. Bij dit artikel is het van belang of een overeenkomst tot levering van software een koopovereenkomst is. Onder 'Wat mag de afnemer in het algemeen van software verwachten?' is bij de toepasbaarheid van de conformiteitsregeling van artikel 7:17 BW daar al op ingegaan. Onder andere werd geconcludeerd dat overeenkomsten tot levering van standaardsoftwarepakketten waarschijnlijk wel koopovereenkomsten zijn, waarbij werd aangetekend dat het onderscheid tussen standaard- en maatwerksoftware niet altijd helder is. Onder omstandigheden kan een millenniumclaim wegens wanprestatie dus twee jaar nadat de afnemer de millenniumbug ontdekt al zijn verjaard.

De plicht tot protest

Maar de afnemer kan nog eerder zijn claim op de leverancier verliezen. Artikel 6:89 BW bepaalt namelijk dat de schuldeiser dient te protesteren binnen bekwame tijd nadat hij een gebrek in een aan hem geleverde prestatie ontdekt of redelijkerwijs had moeten ontdekken. Als de schuldeiser dit nalaat kan hij op dit gebrek geen beroep meer doen en verliest hij alle claims op de schuldenaar op grond van dit gebrek. Artikel 7:23 lid 1 BW bepaalt hetzelfde voor gebreken in het geleverde bij een koopovereenkomst. Wat als 'binnen bekwame tijd' geldt hangt volgens de parlementaire geschiedenis af van de aard van de overeenkomst en de gebruiken.¹⁰³ Doorgaans mag men enige tijd nemen voor onderzoek of beraad. Duidelijk is dus dat een millenniumclaim al

98 Dit artikel ziet naast de verjaring van vorderingen op grond van wanprestatie ook op vorderingen uit onrechtmatige daad en op vorderingen tot betaling van bedongen boetes.

99 Parl. Gesch. Boek 3, p. 928.

100 Asser-Hartkamp, *Verbindenissenrecht I*, Zwolle 1996, nr. 674.

101 Bloembergen (*Schadevergoeding bij onrechtmatige daad*, Dissertatie Kluwer, Deventer 1965, nr. 95) is het met deze laatste stelling niet eens. Hij vindt dat het onbevredigend is als een vordering verjaren kan voordat zij opkomt.

102 H. Stein, 'Bevrijdende verjaring', *Advocaatenblad*, 9 juni 1989, p. 296 ad 4, Asser-Hartkamp I, nr. 676.

103 Toelichting Meijers, Parl. Gesch. Boek 6, p. 317 voor artikel 6:89 BW en VVI in MvA I, Parl. Gesch. Invoeringswet Boek 7, p. 156/7 voor artikel 7:23 lid 1.

veel eerder dan door verjaring verloren kan gaan door protest na te laten.

Het stuiten van de verjaring

Om de rechtsverwerking van de artikelen 6:89 BW en 7:23 lid 1 BW te voorkomen is het protesteren of melden van het gebrek bij de leverancier al genoeg. Hiervoor geeft de wet geen vormvereisten en dit protest kan dus mondeling gebeuren.¹⁰⁴ Om een verjaringstermijn die loopt nog te stuiten moet men wel aan enkele voorwaarden voldoen. Artikel 3:317 BW bepaalt dat de schuldeiser de verjaring kan stuiten door de schuldenaar schriftelijk aan te manen of door zich schriftelijk het recht op nakoming voor te behouden. Verder kan verjaring ex artikel 3:316 lid 1 BW worden gestuit door het instellen van een eis of iedere andere daad van rechtsvervolgning. Verder wordt de verjaring gestuit als de schuldenaar het recht van de schuldeiser erkent. Artikel 3:319 BW bepaalt dat de nieuwe verjaringstermijn die door de stuiting begint even lang is als de gestuite verjaringstermijn, maar niet langer dan vijf jaar.

Om niet op voorhand claims op zijn leverancier te verliezen, kan men bij voorbaat bij hem protest aantekenen wegens de aanwezigheid van de bug.

Conclusie

Een afnemer van producten met de millenniumbug doet er goed aan zodra hij op de hoogte is van de millenniumbug in geleverde producten hierover schriftelijk te protesteren bij zijn leverancier. Omdat niet duidelijk is of softwareleverantieovereenkomsten koopovereenkomsten zijn, is het verder verstandig om iedere twee jaar na het bekend worden met de aanwezigheid van de millenniumbug de verjaring te stuiten van de mogelijke vordering op de leverancier. Tot slot moet gewaarschuwd worden dat de artikelen 6:89 en 7:23 lid 1 BW de vordering ook afsnijden als de afnemer niet geprotesteerd heeft op het moment dat hij het gebrek in het gepresteerde c.q. geleverde had moeten ontdekken. Nu de pers steeds meer aandacht schenkt aan het millenniumprobleem en bedrijven worden aangespoord er aandacht aan te besteden, kan een rechter oordelen dat de afnemer de aanwezigheid van de millenniumbug had moeten onderzoeken. Door geen actie te ondernemen kan de afnemer, ook als hij nog niet weet of de software die hij in huis heeft de millenniumbug bevat, zijn claims verliezen op zijn leverancier. Om dat gevaar te verkleinen kan men bij voorbaat protest aantekenen bij de leverancier wegens de aanwezigheid van de bug.¹⁰⁵

SAMENVATTING EN CONCLUSIE

De millenniumbug is een vreemd insect. In de eerste programma's was het meer een praktische, slimme manier om met datums om te gaan waardoor minder computergeheugen nodig was. Maar na verloop van tijd breekt dit de gebruiker op. De millenniumbug kan dan de werking van het programma waar-

in hij voorkomt ernstig aantasten zodra het datums van na de eeuwwisseling moet verwerken. Daar was in de meeste programma's lang geen behoefte aan, maar nu het volgende millennium nadert wordt die steeds groter. Het verwijt dat een programmeur kan worden gemaakt om zo te programmeren is niet gekoppeld aan die werkwijze op zich, maar aan het moment waarop hij die toepaste.

Om de omstandigheden te bepalen waaronder het leveren van software met de millenniumbug een wanprestatie oplevert, moet worden gekeken naar wat de afnemer daarvan mag verwachten. Door de conformiteitsregeling van artikel 7:17 BW die waarschijnlijk (naar analogie) van toepassing is op de levering van standaardsoftwarepakketten mag de afnemer allereerst verwachten dat de software in zijn algemeenheid goed werkt, ook na het jaar 2000. Maar ook van maatwerksoftware mag de afnemer verwachten dat deze zo gebouwd is dat die in het algemeen geschikt is voor het beoogde gebruik. In enkele arresten over mislukte automatiseringen is deze gedachte te vinden. Maar het is niet reëel een totale afwezigheid van bugs te verlangen, want het is praktisch onmogelijk alle fouten te verwijderen. De millenniumbug tast de werking van programma's vaak zo aan dat van een klein gebrek geen sprake meer is. Bovendien is de millenniumbug niet te vergelijken met de gemiddelde kleine bug. Het gaat bij de millenniumbug ook niet om een fout die alleen bij vergaand testen blijkt. Als de millenniumbug de werking van software ernstig aantast, worden de gerechtvaardigde verwachtingen van de afnemer in principe geschonden.

De volgende vraag is hoe lang de afnemer mag verwachten dat de software geschikt blijft. Hierbij is allereerst van belang wat de gemiddelde levensduurverwachting is van de software die de afnemer heeft aangeschaft. Die is niet altijd oneindig. Bij het programmeren worden bijvoorbeeld vaak tellers ingesteld die bijhouden hoeveel tijd verstreken is, maar ook hoeveel keer een set commando's is uitgevoerd, en hoeveel records een database bevat. Bij het instellen van die tellers moet de programmeur een maximum kiezen. Zodra de tellers dat bereiken kan dit problemen geven, bijvoorbeeld omdat ze terugspringen naar nul. Als de tellers erg ruim worden ingesteld, heeft het programma extra geheugen- en opslagcapaciteit nodig en is het programma duurder in het gebruik. Vooral in de beginjaren van het programmeren was dit van belang omdat computergeheugen en opslagcapaciteit toen veel duurder waren dan nu. Bij het instellen van tellers richt een programmeur zich naar de periode dat de afnemer doorgaans verwacht het programma te kunnen gebruiken. Die periode hangt van het type software af. Maar de gerechtvaardigde levensduurverwachting van de software hangt niet alleen van het type software af. Afhankelijk van de contractvoorwaarden waaronder de software is geleverd en de specifieke omstandigheden kan de gerechtvaardigde levensduurverwachting hoger of lager zijn.

Bij de bepaling van wat de afnemer mocht verwachten van de levensduur moet men ook kijken naar de mededelings- en onderzoeksplichten van partijen. Ervan uitgaande dat de leverancier weet of behoort te weten dat de millenniumbug aanwezig is, heeft hij een mededelingsplicht op het moment dat hij behoort te weten dat de afnemer de software langer

104 Om bewijsproblemen te voorkomen is het aan te raden dit protest per aange-tekende post te maken.

105 Een mogelijke formulering van een dergelijk voorbehoud zou als volgt kunnen luiden:

Omdat wij niet kunnen uitsluiten dat zal blijken dat bepaalde van uw producten of diensten niet (tijdig) millennium-conform zijn en dat dit als een gebrek van dat product of die dienst moet worden beschouwd, willen wij geacht worden dergelijke gevallen reeds nu als gebrek bij u te hebben gemeld. (Ontleend aan een voorbeeldbrief opgesteld door het Millennium Platform en gepubliceerd op zijn website <http://www.mp2000.nl> onder 'Hulpmiddelen'.)

wil gebruiken dan de millenniumbug toestaat. Laat de leverancier deze mededeling na, dan kan de afnemer zich later daarop beroepen omdat hij die langere levensduur mocht verwachten. Bij het aannemen van een mededelingsplicht kan ook meespelen in wat voor verhouding de afnemer en de leverancier staan: is het contact tussen partijen nauw, is de afnemer een leek op IT-gebied of is de leverancier ook adviseur. Dat de onderzoeksplicht de afnemer verplicht te voorkomen dat hij met een verkeerde voorstelling van zaken een overeenkomst aangaat, speelt geen rol meer als een mededelingsplicht wordt aangenomen, want in de jurisprudentie is bepaald dat de mededelingsplicht vóór de onderzoeksplicht gaat.

Als wordt vastgesteld dat de geleverde software niet voldoet aan de gerechtvaardigde verwachtingen van de afnemer, kan de leverancier worden aangesproken op wanprestatie. De vraag is of deze claim effectueerbaar is. Dan moet eerst worden gekeken of een claim uit bedrijfseconomische overwegingen wel opportuun is. Zekerheid dat de rechter de claim toewijst is er niet, terwijl de kosten van de procedure gemaakt moeten worden. Ook kan een goede of voor de bedrijfsvoering cruciale relatie op het spel worden gezet. Daarnaast kunnen twee juridische barrières de effectuering van de claim belemmeren.

De eerste barrière zijn de exoneratiebedingen die in veel softwareleverantieovereenkomsten staan. Uit jurisprudentie blijkt dat een beroep op een exoneratiebeding onder omstandigheden in redelijkheid en billijkheid onaanvaardbaar kan zijn. Hiervoor is vooral het Pseudovogelpest arrest van belang. Het bepaalt dat de leverancier zich bij een claim door een gebrek in het geleverde niet mag beroepen op de beperking van zijn aansprakelijkheid als hij bij de levering wist van dat gebrek en de eventuele schade daardoor voor de afnemer. Of de leverancier kan weten dat de afnemer schade zal lijden door de bug is afhankelijk van de levensduurverwachting die de afnemer van de software heeft en waar de leverancier rekening mee moet houden. Omdat de bepaling van de gerechtvaardigde levensduurverwachting van de software bijna altijd op een schatting berust, kijkt de rechter ook naar de overige omstandigheden van het geval die volgens het arrest Saladin/HBU van belang zijn om te beantwoorden of een beroep op een exoneratiebeding mogelijk is. Deze barrière is onder omstandigheden dus te nemen.

De tweede barrière is dat de millenniumclaim kan verjaren of door rechtsverwerking teniet kan gaan. Volgens de algemene verjaringsregeling verjaart ie-

dere claim op grond van wanprestatie in beginsel uiterlijk vijf jaar nadat de schuldeiser op de hoogte is van het gebrek dat schade veroorzaakt. Het gaat er dus niet om wanneer de bug tot schade leidt, maar wanneer de afnemer weet dat de bug aanwezig is.

De koopregeling geeft hiervoor een termijn van twee jaar. Omdat de koopregeling op de levering van software (naar analogie) van toepassing kan zijn, kan de claim dus al verjaren twee jaar nadat de afnemer weet dat de bug in zijn software zit. De afnemer zal de verjaring derhalve tijdig moeten stoppen door middel van een stuitingsbrief.

De afnemer kan zijn claim echter nog eerder kwijtrakken. De artikelen 6:89 en 7:23 lid 1 BW verplichten hem namelijk binnen bekwame tijd te protesteren bij zijn wederpartij zodra hij weet of behoort te weten van het gebrek in de geleverde prestatie. Binnen bekwame tijd is weliswaar niet direct – de afnemer mag even de tijd nemen om het gebrek te onderzoeken en eventueel advies in te winnen – maar varieert afhankelijk van de omstandigheden tussen enkele dagen en enkele weken. Stilstaan kan dus al zeer snel tot het verlies van de millenniumclaims van de afnemer leiden.

Slot

Onder omstandigheden heeft een claim tegen de leverancier van software met de millenniumbug zeker kans van slagen. Bij die kans speelt vooral een rol welke levensduurverwachting de afnemer van de software mocht hebben. Dit bepaalt of de millenniumbug een aantasting is van de gerechtvaardigde verwachtingen omtrent het functioneren van de software. Omdat deze levensduurverwachting afhangt van het geleverde pakket en de manier waarop het is geleverd, is geen algemene levensverwachting te bepalen voor alle software.

Hieruit kan men afleiden dat het niet waarschijnlijk is dat in de jurisprudentie uiteindelijk één breekdatum naar voren komt waarmee kan worden bepaald of software op een moment een gebrekkig product is. Franken deed hiertoe in zijn editorial 'Het millenniumprobleem'¹⁰⁶ een suggestie. Hij wees op de bodemverontreinigingsarresten van 1992. Hierin bepaalde de Hoge Raad dat de saneringskosten voor bodemverontreiniging van vóór 1 januari 1975 voor rekening van de overheid zijn omdat daarvóór niet genoeg duidelijk was dat vervuilen van grond een vermogensnadeel voor de overheid zou meebrengen. Maar of de millenniumbug in een concreet geval tot vermogensnadeel bij de afnemer leidt, hangt van de levensduurverwachting af, en die is niet voor alle software gelijk.

*Mr P.P.J.L. Enneking
Is als adviseur informatica-
recht werkzaam bij KPMG
EDP Auditors te Amstelveen.*

*Mr M. Seelt
Schreef in de periode januari
tot en met juli 1998 onder be-
geleiding van mr P.P.J.F.L. En-
neking zijn afstudeerscriptie
over dit onderwerp bij KMPG
EDP Auditors en is thans
werkzaam als advocaat bij
Loeff Claeyss Verbeke te Am-
sterdam. Dit artikel is een be-
werking van voornoemde
scriptie.*

¹⁰⁶ H. Franken, 'Het millenniumprobleem', *RM Themis*, november 1997.

Y2Kkosten, baten

Drs. T.G. Kloosterman

Uit alle inspanningen nodig om een organisatie millenniumbestendig te krijgen, vloeien kosten en baten voort. Dit artikel beoogt enerzijds de accountant een handvat te bieden bij het in kaart brengen van de diverse factoren die van belang zijn bij het inschatten van de kosten en baten uit hoofde van het millenniumprobleem. Anderzijds gaat dit artikel in op de verwerking van het millenniumprobleem in de jaarrekening.

INLEIDING

Iedereen kijkt ernaar uit: het magische Jaar 2000. Het jaar waarin een nieuwe eeuw, zelfs een nieuwe periode van duizend jaar ingaat, een nieuw millennium!¹ Een millennium waarin technische hoogstandjes en hypermoderne technieken ons het leven een stuk gemakkelijker zullen maken. Althans, als je alle sciencefiction boeken van de afgelopen eeuw mag geloven. Intussen lijkt het een trefzekere gok dat al die moderne apparatuur het in het jaar 2000 ernstig kan laten afweten.

Was de scope van het millenniumprobleem eerst nog beperkt tot de oude, voornamelijk administratieve systemen, tegenwoordig weten we dat de millenniumbug zich tevens manifesteert in moderne systemen. Dat ook de embedded software in het onderzoek moet worden betrokken, had men eveneens in eerste instantie niet voorzien, evenals de afhankelijkheid van derden: de ketenproblematiek. Deze nieuwe inzichten leiden tot aanpassingen in de oorspronkelijke aanpak, hogere kosten dan voorzien en langere doorlooptijden van het project, met alle gevolgen van dien. Op dit moment worden door organisaties dan ook aanzienlijke uitgaven gedaan om systemen aan te passen, teneinde mogelijke problemen, publicitaire schade of zelfs faillissement van de organisatie te voorkomen. Schattingen geven nu al aan dat voor Nederland alleen al de uitgaven voor de oplossing van het probleem rond de 20 miljard gulden liggen.

'Always look on the bright side of life'. Ondanks alle negatieve berichtgeving zijn er wel degelijk voordelen te behalen uit het aanpakken en oplossen van het millenniumprobleem. De noodzaak tot inventarisatie van alle informatietechnologie (IT) binnen de organisatie zal talloze onvolkomenheden in de documentatie aan het licht brengen en wellicht leiden tot het inzien van de noodzaak van een geüpdatet documentatie van systemen. Ervaringen die men opdoet in het managen van dit specifieke project zullen zich terugverdienen in het managen van toekomstige (automatiserings)projecten. Ook de zeer uitgebreide testervaring die wordt opgedaan, kan in de toekomst zeer wel van pas komen. Denk hierbij ook aan het aanpassen van systemen inzake de invoering van de euro.

Dat het millenniumprobleem ook gevolgen heeft voor de beroepsuitoefening van accountants behoeft naar aanleiding van bovenstaande geen uitleg meer. De accountant onderzoekt immers of de jaarrekening volgens normen die in het maatschappelijk verkeer als aanvaardbaar worden beschouwd, een zodanig inzicht geeft dat een verantwoord oordeel kan worden gevormd omtrent het vermogen en het resultaat, alsmede – voorzover de aard van een jaar-

¹ Het volgende millennium begint pas 1 januari 2001. Dit is een gevolg van het feit dat het jaar 0 (als periode van 366 dagen) niet heeft bestaan. Na het tijdstip nul begon direct het jaar 1, met datum 01/01/01, en net zoals we nu in de twintigste eeuw leven terwijl het eeuwcijfer nog 19 is. Pas als het jaar 2000 vol is, hebben we tweeduizend jaar achter de rug en begint het derde millennium. Bovendien – we rekenen nu *terug*, waarmee we voor het gemak maar even vergeten dat er in de Middeleeuwen is overgestapt van de Juliaanse naar de Gregoriaanse kalender, en die twee hepen niet synchroon.

rekening dat toelaat – omtrent de solvabiliteit en de liquiditeit van de rechtspersoon.

Dit artikel beoogt enerzijds de accountant een handvat te bieden bij het in kaart brengen van de diverse factoren die van belang zijn bij het inschatten van de kosten en baten uit hoofde van het millenniumprobleem. Eerst wordt ingegaan op de inrichting van een millenniumproject. Aan de hand van een korte bespreking van de projectfasen wordt aandacht besteed aan de verschillende factoren die het inschatten van de kosten van een millenniumproject bemoeilijken. Vervolgens worden de baten besproken die voortvloeien uit alle inspanningen die zijn (of nog moeten worden) gedaan om de organisatie zoveel als mogelijk millenniumbestendig te krijgen.

Anderzijds gaat dit artikel in op de verwerking van het millenniumprobleem in de jaarrekening. Hierbij is onderscheid gemaakt tussen de verwerking in de jaarrekening van uitgaven die zijn gedaan om het millenniumprobleem op te lossen en de consequenties voor de jaarrekening als blijkt dat het millenniumprobleem niet of onvoldoende is opgelost.

Y2K-KOSTEN

Uit de inleiding kwam al naar voren dat het millenniumprobleem van een automatiseringsprobleem is uitgegroeid tot een organisatieprobleem. Derhalve is een organisatiebrede projectaanpak vereist, onder de directe verantwoordelijkheid van de hoogste organen binnen de organisatie.

Elk millenniumproject is uniek wat grootte en complexiteit betreft. Inschattingen van de te maken kosten zijn dan ook een eenmalige aangelegenheid; er zijn geen statistieken. Er is geen algemeen geldige, vaststaande manier om een millenniumproject tot een goed einde te brengen. Elke aanpak brengt een ander kostenplaatje met zich mee. Er zijn geen algemeen geldende regels of prijzen voor de vele verschillende activiteiten en kostendragers. Vuistregels die worden gehanteerd zijn 3 procent van de jaaromzet of 30 tot 38 procent van het IT-budget. Volgens één van de bekendste vuistregels worden bedragen per regel broncode (software) genoemd van 2 tot 17 dollar! Bovendien kunnen sommige kosten, zoals voor embedded chips, pas gaandeweg het project worden vastgesteld. Het is zelfs mogelijk dat twee chips met eenzelfde typenummer verschillen qua millenniumgevoeligheid - de chips zijn intern anders.

Neem als voorbeeld Unilever, die zich genooddaakt ziet haar oorspronkelijke kostenramingen inzake de millenniumproblematiek binnen Unilever te verdrievoudigen tot 1 miljard gulden.

Teneinde een uiteenzetting te geven van de kosten die voortvloeien uit het aanpakken en oplossen van het millenniumprobleem wordt per projectfase aandacht besteed aan de verschillende factoren die in ogenschouw moeten worden genomen bij het inschatten van de kosten van een millenniumproject.

Bewustwording

Doel van deze fase is bewustwording en betrokkenheid van iedereen, met name het hoogste management, in de organisatie te verkrijgen. Luid en duidelijk reclame maken voor het millenniumproject zal hard nodig zijn. Het management zal een leidende en sturende rol moeten hebben bij het oplossen van het millenniumprobleem. Hiertoe dient het management zich bewust te zijn van de mogelijke gevolgen ervan. Dit bewustzijn beperkt zich niet tot het onderkennen van het probleem, maar houdt tevens in dat er reeds concrete (inventarisatie)plannen bestaan of worden ontwikkeld teneinde het millenniumprobleem op te lossen. Kosten die hiermee gepaard gaan, zullen hoger zijn dan het opstellen van een communicatieplan dat bij 'normale' projecten ervoor zorgt dat de betrokkenen worden geïnformeerd. De betrokkenheid van het hoogste management houdt in dat de doorberekende tarieven hoger zullen zijn. Daar komt nog bij dat de bewustwording niet alleen intern moet worden verkregen, maar ook extern in verband met de ketenproblematiek.

Projectmanagement

In het kader van het projectmanagement worden onderscheiden de strategiebepaling en de totaalplanning.

Strategiebepaling

De leiding moet voldoende toezicht uitoefenen op de voortgang van het project. Er dient een duidelijke definitie van de projectomvang te bestaan, waarbij ook aandacht wordt besteed aan decentrale ontwikkelingen en embedded software alsmede de ketenproblematiek. Tevens dient de gekozen projectstructuur ruimte te bieden voor duidelijke tijdslijnen en meetpunten teneinde de hiervoor genoemde voortgangscntrole mogelijk te maken.

Met betrekking tot de ketenproblematiek is het van belang dat in de projectaanpak aandacht wordt besteed aan vendor- en customermanagement. Indien de organisatie voor haar bedrijfsvoering in enige mate afhankelijk is van derden, is het noodzakelijk na te gaan in hoeverre deze derden adequate maatregelen hebben getroffen om discontinuïteit van hun bedrijfsvoering te voorkomen. Als daarover geen duidelijkheid kan worden verkregen, kan het wenselijk zijn na te gaan of daarvoor noodscenario's kunnen worden opgesteld. Anderzijds zullen afnemers informatie willen over de millenniumbestendigheid van de desbetreffende organisatie.

Bij de bepaling van de strategie moet ook worden beslist of bij het aanpassen van systemen ook allerlei andere wijzigingen zoals toevallig gevonden fouten of aanpassingen voor de introductie van de euro binnen dezelfde (deel)projecten worden aangepakt. Vanuit de ervaringen in de praktijk zijn de meningen verdeeld, met een voorkeur voor het niet meenemen van additionele wijzigingen. De problematiek is al zo omvangrijk en complex dat alle bijkomstigheden voortvloeiend uit andere problemen de complexiteit alleen maar vergroten. Bij de behandeling van het verwerken van de kosten en baten in de jaarrekening wordt hierop teruggekomen.

Totaalplanning

In het plan van aanpak moet, naast de taken, verantwoordelijkheden en bevoegdheden van de betrokkenen, worden aangegeven op welke wijze het millenniumprobleem zal worden aangepakt, welke middelen (menskracht, geldmiddelen, technische hulpmiddelen) per fase benodigd zullen zijn en wat het tijdsbeslag en de doorlooptijd zullen zijn. Overigens verschillen de planningsaspecten van millenniumprojecten niet principieel van die van andere automatiseringsprojecten. Wel is een aantal specifieke kanttekeningen te plaatsen:

- De beschikbare tijd is slechts nog circa tweehonderd werkdagen! Anders dan bijvoorbeeld bij de euro-problematiek is de deadline hard als graniet. En voor veel systeemaanpassingen zal de deadline zelfs veel eerder liggen dan 31 december 1999.
- Organisaties hebben normaliter budgetten die maar net toereikend zijn voor de normale gang van zaken. Het millenniumproject zuigt daarbij nog eens zeer veel extra middelen op (budget maar ook computercapaciteit) zonder dat er directe opbrengsten of functionaliteit tegenover zullen staan. Toch zijn grote extra budgetten noodzakelijk.
- Wanneer er externen in het projectteam worden betrokken, dient men rekening te houden met de toenemende schaarste op de arbeidsmarkt voor automatiseringspersoneel. Wanneer er wordt gewerkt op regiebasis, zullen de kosten exponentieel stijgen.

Inventarisatie

Een gedegen en actuele inventarisatie is van groot belang. Onvolledigheden hierin (denk aan embedded software) kunnen bij de millenniumovergang tot onvoorziene situaties leiden. Per object dienen de functie en relaties met de bedrijfsprocessen in kaart te worden gebracht, evenals koppelingen en interfaces. Het verdient aanbeveling de geïnventariseerde objecten met al hun kenmerken adequaat vast te leggen. Andere belanghebbenden kunnen deze vastlegging vervolgens raadplegen, bijwerken of controleren. Een kwalitatief goed inventarisatieoverzicht dient als uitgangspunt voor de volgende stappen in het millenniumproject en kan tevens worden gebruikt bij andere projecten (euro).

De inventarisatie kan bijdragen tot het indelen van de objecten in onderling samenhangende clusters. Door de clusters zo te definiëren dat er onderling relatief weinig systeemkoppelingen zijn, kan het aantal aan te passen interfaces en te ontwikkelen oplossingen worden beperkt. Criterium voor clustering kan dan bijvoorbeeld zijn de gelijke prioriteit van bepaalde IT-systemen die van doorslaggevend belang zijn voor het overeind blijven van de organisa-

tie. Zeker wanneer organisaties te laat zijn gestart met het aanpakken van het millenniumprobleem is deze prioriteitenstelling onontbeerlijk. Men kan dan zelfs gaan overwegen eerst een prioriteitenstelling te gaan opstellen, om daarna slechts die IT-systemen welke de hoogste prioriteit verdienen aan een grondige inventarisatie te onderwerpen. De inventarisatie dient sowieso hand in hand te gaan met de prioriteitenstelling, zeker met het oog op de grote omvang van het probleem. Daarbij zal het belang van een systeem voor de bedrijfsuitoefening veruit de belangrijkste maatstaf dienen te zijn.

Grootschalig onderzoek

Het uitvoeren van een (impact)analyse heeft tot doel per object vast te stellen:

- of het object onderhevig kan zijn aan toekomstige millenniumproblemen;
- in welke mate het object kritiek is voor de bedrijfsvoering;
- op welke manier het probleem dient te worden opgelost.

Voortbordurend op de inventarisatiefase vindt hier een impactanalyse plaats op basis van een grootschalig onderzoek. Hierbij kan gebruik worden gemaakt van de tijdens de inventarisatiefase gedefinieerde clusters. Informatie die benodigd is voor dit onderzoek kan worden verkregen door:

- Het beoordelen van de documentatie. Hierbij moet worden bedacht dat deze met name voor oude systemen voor problemen kan gaan zorgen. Vaak is de documentatie niet meer op orde en zal ook de kennis van deze oudere systemen wellicht niet meer in de organisatie aanwezig zijn.
- Het bouwen van een testsysteem in een zo vroeg mogelijke fase te starten, tezamen met het zo vroeg mogelijk verkrijgen van voldoende documentatie. Tot nu toe is gebleken dat het opzetten van een testsysteem in de praktijk meer werk vraagt dan de brochures van de leveranciers beloven.
- Het op voorhand testen van de gevoeligheid van een systeem voor jaar 2000 overschrijdende jaartallen. Dit is een voor de hand liggend maar nogal eens vergeten onderwerp in de aanloopfase van millenniumprojecten.
- Overleg met de leverancier. Dit is met name aan de orde indien sprake is van standaardpakketten, embedded software, of maatwerksoftware die door een externe organisatie is ontwikkeld. Dit aspect dient tevens in een breder verband te worden gezien in het kader van de ketenproblematiek.

Bovengenoemde problemen die kunnen worden gesignaleerd bij het verzamelen van de benodigde informatie, moeten worden meegenomen in de kostenschattingen. Het resultaat van de impactanalyse is vervolgens een plan van aanpak dat per object dan wel per cluster wordt uitgevoerd. Hierbij moet rekening worden gehouden met de benodigde inzet van mensen en middelen, de doorlooptijd van het project, de resterende levensduur van de objecten, de eventuele gevolgen voor de organisatie en mogelijke alternatieven.

Het op voorhand testen van de gevoeligheid van een systeem voor jaar 2000 overschrijdende jaartallen wordt nogal eens vergeten in de aanloopfase van een millenniumproject.

Modificaties/vervanging

Na alle voorbereiding en analysewerk zullen de feitelijke aanpassingen moeten worden doorgevoerd. Hierbij is het van belang onderscheid te maken tussen twee situaties. Dient de onderneming de oplossing zelf te realiseren (veelal bij maatwerk en eigen ontwikkeling) of zorgt de leverancier (als deze nog bestaat) hiervoor (bij een standaardpakket of embedded software). Uit het oogpunt van kwaliteitsbeheersing is het wenselijk om nadere afspraken te maken omtrent het gebruik van de verschillende oplossingsrichtingen. Het is niet aan te raden om millenniumaanpassingen te combineren met regulier onderhoud. Door combinatie wordt het toch al complexe testen van systemen en processen onnodig bemoeilijkt.

Bij het bepalen van de strategie is reeds gekozen voor een voorkeursoplossing teneinde alle systemen millenniumbestendig te maken. De mogelijkheden zijn:

- systemen aanpassen en data zoveel mogelijk ongemoeid laten;
- nieuwe systemen kiezen en de data indien nodig daaraan aanpassen.

Hierbij dienen tevens de voorkeuren voor de technische oplossingen, waaronder de te hanteren kwaliteits- en dataformaatstandaarden, te worden bepaald. Met deze twee beslissingen kan het werk zoveel mogelijk worden gestandaardiseerd, zodat op de aspecten projectmanagement, kennis, ervaring en toolondersteuning economies of scale kunnen worden behaald en bovendien het aantal aan te passen interfaces tussen systemen zo beperkt mogelijk blijft.

Uiteraard is het van groot belang de doorgevoerde wijzigingen goed te documenteren, zowel in de broncode als in de systeem- en projectdocumentatie. Naast het bijwerken van de documentatie zal ook moeten worden getraind in het gebruik van gewijzigde systemen. Enerzijds zullen systeembeheerders en operators extra alert moeten worden gemaakt op het detecteren van optredende fouten. Anderzijds zullen ook gebruikers moeten worden getraind in het mogelijk anders invoeren van gegevens en het interpreteren van eventuele (resterende) dubbelzinnige jaartallen.

Testen

'Test early, test often' is als altijd het devies. Zeker omdat niemand in de organisatie de deadline kan verschuiven en er geen vertragingen door te lange ontwikkeliteraties mogelijk zijn. De aangepaste of (nieuw) aangeschafte programmatuur zal moeten worden getest op het correct functioneren voor, tijdens en na de overgang naar het jaar 2000 (millenniumbestendigheid). Met betrekking tot het testen zal een omgeving moeten worden gecreëerd, zoals deze in het jaar 2000 zal bestaan.

Met name het realiseren van een testomgeving die overeenkomt met de situatie zoals die zich in het jaar 2000 zal voordoen, blijkt in de praktijk zeer complex. Zo blijkt uit inmiddels opgedane ervaringen bij organisaties dat het testen circa 50 procent van de totale kosten veroorzaakt. Tijdens het testen kunnen tevens nieuwe problemen aan het licht komen die men in eerste instantie niet had voorzien, hetgeen een grote

Het realiseren van een testomgeving die overeenkomt met de situatie zoals die zich in het jaar 2000 zal voordoen, is zeer complex.

impact kan hebben op de planning en daarmee op eerder gemaakte ramingen van de kosten.

Voor de oordeelsvorming van de accountant is deze fase van groot belang. Wanneer namelijk al het testen volgens de testdocumentatie conform de hoogste normen is uitgevoerd en alle millenniumproblemen volgens de testverslagen zijn weggewerkt, dan heeft de accountant 'circumstantial evidence' dat de problemen zijn weggenomen. Het verkrijgen van deze evidence zal een groot beroep doen op de deskundigheid van de accountant. Het is dan ook niet onaannemelijk te achten dat de accountant er goed aan zal doen een beroep te doen op een ter zake deskundig iemand: de EDP-auditor.

Implementatie/migratie

Het is aan te bevelen de implementatie van alle millenniumbestendige systemen niet uit te stellen tot eind 1999. Teneinde dit mogelijk te maken zullen de finale systeem-, migratie- en acceptatietests goed moeten worden gepland. Wanneer een onderneming voor de levering van millenniumbestendige software en systemen in belangrijke mate afhankelijk is van derden bestaat het risico dat de eigen planning niet wordt gehaald door het te laat (of in het geheel niet) beschikbaar komen van millenniumbestendige versies. Duidelijke en tijdige communicatie met de leverancier is dus gewenst.

Het dynamiseren van het migratiepad betekent een toename van de complexiteit, temeer daar gedurende dit traject de vele interfaces diverse malen moeten worden aangepast. Meer dan gebruikelijk dienen controles te worden uitgevoerd. Het versiebeheer zal meer dan normaal op de proef worden gesteld. Tevens is het van belang dat er back-ups van gegevens en programmatuur worden aangeemaakt zodat hierop kan worden teruggevallen mocht het migratietraject niet goed verlopen door bijvoorbeeld conflicterende millenniumbestendige versies.

Stabilisatie/contingencyplanning

Aanschaffingen en nieuw ontwikkelde objecten dienen in elk geval bestendig te zijn (aangetoond door testen). Binnen de organisatie dienen vervolgens maatregelen te worden getroffen om zeker te stellen dat millenniumbestendige objecten millenniumbestendig blijven.

Maar wat te doen wanneer er onverwacht toch nog dingen fout gaan? Vanuit het oogpunt van de accountant een zeer belangrijk issue. De accountant zal de maatregelen moeten beoordelen die binnen de organisatie zijn getroffen om de continuïteit van de geautomatiseerde gegevensverwerking te waarborgen. Contingencyplanning is zeker in het kader van de millenniumproblematiek zeer relevant.

Het is noodzakelijk om, ook gedurende de conversietrajecten, hoogstaande calamiteitenopvangplannen beschikbaar en liefst getest te hebben. Er kan niet worden vertrouwd op de algemene calamiteitenplannen; als die al gedetailleerd en up-to-date genoeg zijn, zullen ze zich hoogstwaarschijnlijk op andere risico's richten dan die in de risicoanalyse ten behoeve van het millenniumproject zijn gedefinieerd. Zeker voor wat betreft de opvang van problemen met systemen die gaan disfunctioneren zal het opvangen van de calamiteit niet zozeer bestaan uit het op een uitwijklocatie operationeel maken van back-uptapes van het huidige systeem. Op de uitwijklocatie zal het systeem immers ook falen.

Voor vitale processen is het van belang eventuele noodscenario's beschikbaar te hebben indien deze processen onverwachts toch stagneren. Deze scenario's zullen zich voornamelijk moeten richten op het in zeer korte tijd overschakelen op handmatig schaduwdraaien (tijdelijke oplossing) en vervangen van de systemen (langetermijnoplossing). Hierbij moet rekening worden gehouden met de schaarste van deskundig personeel en vervangende apparatuur. Het is dan ook gewenst rond de jaarovergang naar het jaar 2000 zoveel mogelijk rekening te houden met deze voorspelde schaarste teneinde bij het optreden van problemen zo snel mogelijk te kunnen ingrijpen. Tevens is het van belang de gehele organisatie te betrekken bij het zo snel mogelijk detecteren van het stagneren van processen. Opmerksaamheid van alle betrokkenen is in dit kader gewenst.

Verzekeringen en aansprakelijkheid

Zodra er hoge kosten met weinig baten in het spel zijn in combinatie met menselijk handelen, is men al snel geneigd daarvoor een zondebok aan te wijzen. De aansprakelijkheidskwestie van leveranciers van software en hardware (en adviesdiensten) zal naar alle waarschijnlijkheid ontaarden in een heus juridisch mijnenveld, hetgeen buiten het onderwerp van dit artikel valt. In het kader van kostenschattingen is het wel degelijk van belang in hoeverre organisaties kosten kunnen afwentelen op andere partijen of in hoeverre bepaalde onvolkomenheden onder 'de garantie' vallen. Ook is het interessant na te gaan in hoeverre eventuele calamiteiten als gevolg van de millenniumproblematiek door verzekeringsmaatschappijen worden gedekt. Verscheidene verzekeringsmaatschappijen hebben hun polisvoorwaarden aangescherpt. Het feit dat er door de verzekeringsmaatschappijen gezamenlijk een 'millenniumvangnet' is gecreëerd voor eventuele claims uit de zakelijke markt geeft aan dat men wel degelijk verwacht dat organisaties zullen proberen kosten te verhalen.

*Het millenniumprobleem maakt
organisaties bewust van hun toenemende
afhankelijkheid van IT.*

Y2K-BATEN

Naast alle negatieve aspecten waarmee het millenniumprobleem voortdurend in de publiciteit komt zijn er wel degelijk positieve aspecten te noemen. Deze plaats biedt de kans enkele voordelen onder de aandacht te brengen die voortvloeien uit het gestructureerd aanpakken en oplossen van het millenniumprobleem. Hierna volgt een niet-uitputtende opsomming:

- De noodzaak tot inventarisatie van alle IT binnen de organisatie zal talloze onvolkomenheden in de documentatie aan het licht brengen en wellicht leiden tot het inzien van de noodzaak van een geupdate documentatie van systemen. Vele inventarislijsten zijn nu opgeschoond.
- Ervaringen die men opdoet in het managen van projecten zullen zich terugverdienen. Ook de zeer uitgebreide testervaring die wordt opgedaan, kan in de toekomst zeer wel van pas komen. Denk hierbij ook aan het aanpassen van systemen inzake de invoering van de euro.
- Meer organisaties worden zich bewust van hun toenemende afhankelijkheid van IT. Dit komt een gedegen contingencyplanning ten goede. Daar waar men het belang van een gedegen continuïteitsplan eerst niet inzag - 'dat gebeurt ons toch niet' - komt men hier van nu terug en zullen de plannen serieuzer worden aangepakt en daarmee ook worden getest. Er zal meer reservecapaciteit aanwezig zijn.

- Omdat organisaties hebben gekozen voor het implementeren van nieuwe systemen, zal er worden geprofiteerd van betere functionaliteit van de systemen. Wanneer de systemen beter aansluiten op de organisatie en daarmee de bedrijfsprocessen zijn er aanzienlijke efficiencyvoordelen te behalen.

- Concurrenten worden in een kwaad daglicht gesteld omdat ze hun zaakjes (nog) lang niet op orde hebben. En nog beter: concurrenten gaan failliet.

Het is zeer moeilijk deze baten te kwantificeren. Toch is het van belang te onderkennen dat ze wel degelijk bestaan, teneinde te rechtvaardigen dat de bestedingen in het kader van de millenniumproblematiek kunnen leiden tot een verhoging van de toekomstige (netto-)opbrengsten in verband met het eventueel activeren van deze bestedingen.

Y2K-VERWERKING IN DE JAARREKENING

Hoe dient nu de millenniumproblematiek te worden verwerkt in de jaarrekening? Teneinde hierop antwoord te kunnen geven is onderscheid gemaakt tussen:

- de verwerking in de jaarrekening van uitgaven die zijn gedaan om het millenniumprobleem op te lossen;
- consequenties voor de jaarrekening als blijkt dat het millenniumprobleem niet of onvoldoende is opgelost.

De verwerking in de jaarrekening van uitgaven die zijn gedaan om het millenniumprobleem op te lossen

Eerst vindt behandeling plaats van het verwerken van uitgaven in de jaarrekening in het algemeen. Vervolgens wordt ingegaan op de verwerking van uitgaven in de jaarrekening die zijn gedaan om het millenniumprobleem op te lossen. Hierbij is de volgende indeling van belang:

- uitgaven die onderdeel uitmaken van de normale periodieke kosten voor onderhoud aan bestaande systemen (hardware en software);
- uitgaven die zijn gedaan om bestaande systemen aan te passen in het kader van de millenniumproblematiek;
- uitgaven als gevolg van het investeren in nieuwe systemen (hardware en/of software).

Algemeen

Uitgaven kunnen op drie manieren worden verwerkt in de jaarrekening:

1. Voor de toekomstige uitgaven een voorziening opnemen

Volgens artikel 374 lid 1 BW2 worden voorzieningen gevormd voor:

- a. verplichtingen en verliezen waarvan de omvang op balansdatum onzeker is, doch redelijkerwijs is te schatten;
- b. op de balansdatum bestaande risico's ter zake van bepaalde te verwachten verplichtingen of verliezen waarvan de omvang redelijkerwijs is te schatten;
- c. kosten die in een volgend boekjaar zullen worden gemaakt, mits het maken van die kosten zijn oorsprong mede vindt in het boekjaar of een voorafgaand boekjaar en de voorziening strekt tot gelijkmatige verdeling van lasten over een aantal boekjaren.

Bij deze verwerkingwijze worden de kosten eerder verantwoord dan de uitgaven.

2. Het verantwoorden van de kosten in de winst- en verliesrekening van het jaar waarin de werkzaamheden zijn verricht

Volgens deze verwerkingwijze is het jaar waarin de werkzaamheden zijn verricht bepalend voor het jaar waarin de kosten worden verantwoord.

3. Het activeren van de uitgaven

Bij deze verwerkingwijze worden de kosten verantwoord in perioden nadat de werkzaamheden zijn verricht (met uitzondering van de eventueel verantwoorde eerste afschrijvingskosten). Door de kosten te activeren en af te schrijven ten laste van de winst- en verliesrekening worden deze kosten toegerekend aan de jaren waarin de afschrijving plaatsvindt. Dit is slechts aanvaardbaar indien de bestedingen leiden tot een verhoging van de toekomstige (netto-)opbrengsten.

Uitgaven die onderdeel uitmaken van de normale periodieke kosten voor onderhoud aan bestaande systemen (hardware en software)

Gezien de naderende millenniumovergang zal worden gewerkt aan de inventarisatie en de oplossing van eventuele systeemproblemen. Er is geen aanleiding om de kosten van personeel voor deze tijdsbe-

steding anders te behandelen dan de kosten voor de tijdsbesteding aan andere onderhoudsprojecten. Het ligt dan ook voor de hand de hiervoor voortvloeiende projectkosten in de winst- en verliesrekening als kosten te verantwoorden in het jaar waarin de werkzaamheden zijn verricht.

Het is gewenst de last van extra uitgaven in verband met het aanpassen van bestaande systemen thans te nemen.

Uitgaven die zijn gedaan om bestaande systemen aan te passen in het kader van de millenniumproblematiek

In de brochure van NOREA, NOvAA en NIVRA (1998) wordt een duidelijke voorkeur uitgesproken voor het vormen van een voorziening uit hoofde van artikel 374 lid 1 letter b BW2 (zie hierboven). Volgens de Richtlijnen voor de Jaarverslaggeving moet het gaan om specifieke risico's die uitgaan boven het algemene ondernemersrisico. In deze brochure wordt gesteld dat de millenniumwijziging zo'n risico is. Op grond van het voorzichtigheidsbeginsel is het gewenst de last van de extra uitgaven in verband met het aanpassen van bestaande systemen thans te nemen en niet te wachten tot het moment van de daadwerkelijke uitgaven. Voorzover de lasten een waardevermindering van voorheen geactiveerde systemen representeren, dient wettelijk de voorziening als waardevermindering op de desbetreffende resterende actiefpost te worden verwerkt. In de Verenigde Staten is het volgens US GAAP niet toegestaan voorzieningen te vormen voor uitgaven zoals hier bedoeld. Volgens deze regelgeving dienen de uitgaven als kosten te worden geboekt op het moment dat de uitgaven worden gedaan.

Voorwaarde voor het vormen van een voorziening is dat de toekomstige uitgaven redelijkerwijs te schatten zijn. Waardering vindt vervolgens plaats tegen de best mogelijke schatting. Deze schattingen kunnen zich bevinden binnen een bepaalde bandbreedte. In dat geval dient het laagste bedrag als voorziening te worden opgenomen met een aanvullende vermelding in de toelichting dat er nog een risico van extra uitgaven boven het voorziene bedrag bestaat.

Uitgaven die zijn gedaan om bestaande systemen aan te passen in het kader van de millenniumproblematiek kunnen ook worden geactiveerd. Dit is slechts aanvaardbaar als de uitgaven leiden tot een verhoging van de toekomstige opbrengsten welke ruimte laten voor de toekomstige afschrijvingen. De kosten die worden gemaakt om millenniumproblemen op te lossen teneinde de bestaande functionaliteit van de systemen te behouden en waardevermindering te beperken kunnen dus niet worden geactiveerd. Bij hogere toekomstige opbrengsten kan worden gedacht aan een langere economische levensduur van systemen dan de oorspronkelijke (los van de millenniumproblematiek), of verbeteringen in de functionaliteit die leiden tot hogere opbrengsten voor de organisatie. In de praktijk zal dit niet vaak het geval zijn. Het invoeren van verbeteringen legt immers extra beslag op de zeer schaarse tijd die

er nog rest. Het is realistischer te denken dat de plannen voor verbeteringen in functionaliteit al snel door het projectteam zullen worden vervangen door plannen die ervoor zorg dragen in elk geval de bestaande functionaliteit te behouden: 'als we niet kunnen wat we willen, moeten we maar willen wat we kunnen'. Als aanvullende eis geldt nog dat activering slechts plaats kan vinden indien de organisatie ook als bestendige gedragslijn heeft dat uitgaven voor nieuwe systemen worden geactiveerd en afgeschreven.

Het vormen van een kostenegalisatievoorziening (art. 374 lid 1 letter c BW2, zie hierboven) is niet mogelijk. De met de systeemaanpassingen gemoeide kosten houden namelijk geen verband met het gebruik van de activa vanaf het eerste jaar van vorming van de egalisatievoorziening tot aan het moment van daadwerkelijke aanpassing. Om die reden is het niet aanvaardbaar de aanpassingskosten aan die gebruiksjaren toe te rekenen, hetgeen bij de vorming van een kostenegalisatievoorziening wel het geval zou zijn.

Uitgaven als gevolg van het investeren in nieuwe systemen (hardware en/of software)

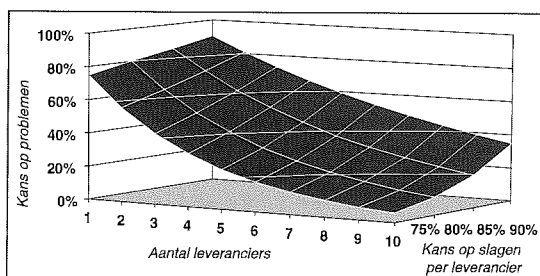
Wanneer in het kader van de naderende millenniumovergang wordt geïnvesteerd in nieuwe systemen zal vrijwel altijd worden voldaan aan de vereisten voor activering zoals hiervoor beschreven. Bij deze verwerkingswijze kan het noodzakelijk zijn bestaande systemen versneld af te schrijven of een duurzame waardevermindering door te voeren.

Activering van hardware geschiedt als materieel actief. Activering van de software kan geschieden als immaterieel vast actief of als bijkomende kosten van de onder de materiële vaste activa gepresenteerde computersystemen. Dit dient wel consistent te zijn met eerder gehanteerde grondslagen.

Consequenties voor de jaarrekening als blijkt dat het millenniumprobleem niet of onvoldoende is opgelost

Groot probleem hierbij is het vaststellen van het tijdstip vanaf wanneer blijkt dat de onderneming aan millenniumproblemen onderhevig is of zal zijn. Drie alternatieven:

- in de loop van 1999 bij het opmaken van de jaarrekening over 1998 wordt het zichtbaar dat de organisatie haar problemen niet of niet tijdig kan oplossen;
- reeds in de eerste weken van 2000 blijkt dat de organisatie niet millenniumproof is;
- pas later in het jaar 2000 blijken millenniumproblemen door een onvoldoende werkend detectiemechanisme.



Figuur 1.
De ketenproblematiek. Let op: In de praktijk zal de kans op slagen niet 75-90 procent zijn, maar 25-30 procent.

In de loop van 1999 bij het opmaken van de jaarrekening over 1998 wordt het zichtbaar dat de organisatie haar millenniumproblemen niet of niet tijdig kan oplossen

Voor het bepalen van de invloed op de jaarrekening is het uiteraard van groot belang wat de consequenties zijn voor de continuïteit van de onderneming. De waarderings- en resultaatbepalingsgrondslagen zijn immers gebaseerd op de verwachting dat de organisatie zal blijven voortbestaan, de 'going concern'-gedachte. Over het niet voldoen aan deze continuïteitsveronderstelling of wanneer deze veronderstelling aan gerede twijfel onderhevig is zegt artikel 384 lid 3 BW2 het volgende: 'alsdan wordt dit onder mededeling van de invloed op vermogen en resultaat in de toelichting uiteengezet'.

Wanneer duidelijk blijkt dat discontinuïteit van de organisatie niet is te voorkomen, dan zullen de waarderingsgrondslagen moeten worden aangepast, ervan uitgaande dat liquidatie van het geheel der werkzaamheden van de organisatie volgt. Activa worden dan gewaardeerd op directe opbrengstwaarde en er kan een noodzaak bestaan aanvullende voorzieningen op te nemen. Wanneer er gerede twijfel bestaat over de continuïteit van de organisatie hoeft er niet te worden afgewaardeerd naar directe opbrengstwaarde. Er mag dan worden gewaardeerd op basis van de 'going concern'-gedachte, mits in de toelichting toereikend wordt ingegaan op de continuïteitsproblemen. In dit geval zal door de accountant een goedkeurende verklaring worden verstrekt waarbij een toelichtende paragraaf verplicht is. In deze toelichtende paragraaf wordt verwezen naar de plaats in de toelichting waar de ernstige onzekerheid inzake de continuïteit wordt uiteengezet.

De accountant wordt geconfronteerd met twee onmogelijke opgaven:

- het vaststellen dat de onderneming haar millenniumproblemen niet of niet tijdig kan oplossen;
- het inschatten van de mogelijke gevolgen van de verwachte millenniumproblemen voor de continuïteit van de organisatie.

Denk hierbij bijvoorbeeld alleen al aan de ketenproblematiek, met een kansrekening in figuur 1.

Toelichting op de figuur:

Deze grafiek geeft inzicht in de kans dat een organisatie geen last zal ondervinden van het millenniumprobleem. Hierbij is er van de gunstige veronderstelling uitgegaan dat de organisatie slechts een beperkt aantal leveranciers 'te beheersen' heeft en de slaagkans (leverancier ondervindt ook geen millenniumproblemen) relatief hoog is. In de praktijk lijkt de slaagkans beduidend lager te zijn; gezaghebbende cijfers spreken van een slaagkans van zo'n 25-30 procent, waarmee de grafiek beduidend lager komt te liggen.

De accountant dient dan ook in zijn opdrachtbevestiging bij de controle van de jaarrekening te benadrukken dat er met geen enkele zekerheid een oordeel kan worden gegeven over de millenniumbestendigheid van de organisatie. De accountant kan samen met de EDP-auditor de voortgang van het millenniumproject regelmatig toetsen, evenals rapportages met betrekking tot de uitkomsten van testresultaten. Tevens kunnen zij zich een oordeel vormen over de kwaliteit van de contingencyplanning,

maar dit kan nooit leiden tot een oordeel inzake de millenniumbestendigheid van een organisatie. In de praktijk zal dan ook met betrekking tot de jaarrekening van 1998 door de accountant worden aangedrongen op het opnemen van de verwachte problemen in het jaarverslag. In dat geval wordt een goedkeurende verklaring afgegeven zonder toelichtende paragraaf. De verwachte problemen moeten in de toelichting worden opgenomen indien er aanwijzingen bestaan dat er een probleem is dat niet tijdig kan worden opgelost en dat leidt tot ernstige onzekerheden omtrent de continuïteit. Dan zal de accountant, uitgaande van een toereikende toelichting, een goedkeurende verklaring afgeven met een verplicht toelichtende paragraaf.

Reeds in de eerste weken van 2000 blijkt dat de organisatie niet millenniumproof is

In dit geval is er met betrekking tot de jaarrekening van 1999 sprake van een gebeurtenis na balansdatum. In de wet is bepaald dat gebeurtenissen na balansdatum slechts van invloed zijn op de waardering van posten per balansdatum voorzover die gebeurtenissen een nieuw licht werpen op de feitelijke situatie per balansdatum. Hierbij kan men denken aan nadere gegevens over risico's en/of verliezen die per balansdatum bestonden, maar waarvan de omvang toen nog niet vaststond. Gebeurtenissen na balansdatum die geen nadere informatie bevatten over de feitelijke situatie per balansdatum mogen niet in de jaarrekening worden verwerkt, tenzij als gevolg van deze gebeurtenissen de veronderstelling van continuïteit van de werkzaamheden onjuist blijkt dan wel aan gereide twijfel onderhevig is. In dit laatste geval dient eveneens verwerking in de jaarrekening plaats te vinden.

Teneinde antwoord te geven op de vraag of de gevolgen van het niet millenniumbestendig zijn van organisaties te beschouwen is als een gebeurtenis na balansdatum welke een nieuw licht werpt op de situatie per balansdatum, wordt de millenniumproblematiek hier gerelateerd aan het volgende nieuwsbericht: 'More than a hundred world war II bombs lie unexploded around London'. Deze problematiek is zeer wel te vergelijken met het millenniumprobleem. Per balansdatum is men zich terdege bewust van het risico, echter men weet niet:

- waar de bommen liggen;
- wanneer de explosie zal plaatsvinden;
- of de bommen überhaupt tot explosie zullen komen;
- wat de (financiële) gevolgen zullen zijn (trillend kop en schoteltje of totale ravage).

Gevolgen van het niet-millenniumbestendig zijn van organisaties die aan het licht komen in de eerste weken van 2000 zijn volgens deze zienswijze op te vatten als een gebeurtenis na balansdatum welke een nieuw licht werpt op de situatie per balansdatum.

Een andere opvatting kan zijn dat men het millenniumprobleem opvat als een calamiteit, bijvoorbeeld een uitslaande brand, welke zich voordoet na balansdatum. Verwerking in de jaarrekening van 1999 vindt dan slechts plaats indien de calamiteit een serieuze bedreiging vormt voor de continuïteit van de organisatie. Wanneer de calamiteit de continuïteitsveronderstelling niet bedreigt, maar wel belangrijke financiële gevolgen heeft voor de organisatie, is ver-

De brand woedt al wel degelijk, maar de vlammen zie je nog niet.

melding onder de overige gegevens noodzakelijk. In tegenstelling tot hiervoor genoemde verwerkingswijze moet in het kader van de millenniumproblematiek wel worden bedacht dat deze brand per balansdatum al wel degelijk aan het woeden is, echter de vlammen zie je nog niet. Ook de mate waarin een organisatie alle mogelijke maatregelen heeft getroffen om de risico's uit hoofde van het millenniumprobleem te beperken, spelen hierbij een rol.

Pas later in het jaar 2000 blijken millenniumproblemen door een onvoldoende werkend detectiemechanisme

Stel dat, naarmate de deadline dichterbij is gekomen, het voor de organisatie steeds duidelijker is geworden dat ze haar oorspronkelijke planning niet gaat halen. De nadruk van het millenniumproject zal dan komen te liggen op de meest bedrijfskritieke IT-systemen. Dat de ondersteunende administratieve systemen het dan moeten ontgelden, zal zeker invloed hebben op de werkzaamheden van de accountant ten behoeve van de jaarrekening van 2000. De continuïteit van de organisatie blijkt dan wel gewaarborgd, maar hoe zit het met de continue werking van de onvervangbare AO/IC waarop de accountant genoodzaakt is te steunen in het kader van de jaarrekeningcontrole? Dit zou kunnen leiden tot onzekerheden in de controle, hetgeen van invloed is op de af te geven verklaring bij de jaarrekening over 2000 (verklaring met beperking wanneer de onzekerheid van materieel belang is, oordeelonthouding wanneer de onzekerheid van wezenlijk belang is).

AFSLUITEND

In dit artikel is ingegaan op de kosten en baten die voortvloeien uit alle inspanningen die worden gedaan om de organisatie zoveel mogelijk millenniumbestendig te krijgen. Daarnaast is de verwerking in de jaarrekening van het millenniumprobleem behandeld.

De diverse factoren die van belang zijn bij het inschatten van de kosten en baten uit hoofde van het millenniumprobleem zullen per organisatie verschillen, en door het voortschrijdend inzicht in de problematiek dienen de projectaanpak en daarmee de kostenschattingen periodiek te worden geëvalueerd en wanneer nodig te worden aangepast.

Bij de behandeling van de verwerking in de jaarrekening van het millenniumprobleem is naar voren gekomen dat ook de accountant wordt geconfronteerd met een aantal problemen. De door het NIVRA aangekondigde nieuwe Audit Alert zal wellicht helderheid scheppen in de wijze waarop met deze problemen moet worden omgegaan. Bij het schrijven van dit artikel was de inhoud hiervan nog niet bekend.

Drs. T.G. Kloosterman

Is als EDP-auditor werkzaam bij KPMG EDP Auditors. Na twee jaar werkzaam te zijn geweest bij KPMG Accountants is hij onlangs overgestapt als rotational naar de EDP-auditingpraktijk.

LITERATUUR

[Bosm97] Bosman, Eeftink, Graafsma, Van Helleman, Holla, Klaassen en Timmers, *Jaarboek externe verslaggeving 1997/1998*.

[FinD97] *Unilever voorziet sterke stijging van de millenniumkosten*, Het Financieele Dagblad, 23 december 1997.

[Hoog98] M.N. Hoogendoorn, *Verwerking in de jaarrekening van uitgaven in het kader van de millenniumproblematiek*, MAB, september 1998.

[IFAC98] *Implications for management and auditors of the year 2000 issue*, uitgewerkt door de International Auditing Practices Committee van de International Federation of Accountants, juni 1998.

[Mill 98] Artikelen in de Millennium Monitor, nummers 1, 2, 3 en 4 van 1998.

[NIVR97] NIVRA, *NIVRA berichten Audit Alert 4: het millenniumvraagstuk*, december 1997.

[NIVR98] NIVRA/NOREA/NOvAA, *Het millenniumprobleem beheerst?!*, april 1998.

[Vlug97] J. van der Vlugt, *Een overzicht van Y2K-problemen*, Compact 1997/1.

Behalve door bovenstaande literatuur is informatie vergaard door middel van het raadplegen van een groot aantal Internet-sites.

Y2K voor de registeraccountant

J.C. van Praat Re Ra

De rol van de accountant en die van het NIVRA in het kader van het millenniumprobleem staan in dit artikel centraal. Daarbij wordt ook ingegaan op de consequenties voor de toekomstige beroepsuitoefening en de verdere ontwikkeling van het vak.

INLEIDING

De oprichting van het Millennium Platform onder voorzitterschap van Jan Timmer heeft al snel geleid tot discussies over de rol van de accountant met betrekking tot de voortgang en de oplossing van het millenniumprobleem in organisaties. Timmer wees het management op de zekerheden die de accountant zou kunnen geven met betrekking tot het millenniumprobleem. Voor de accountant was dit mede aanleiding via een Audit Alert (nummer 4) aandacht te vragen voor dit probleem. Tot teleurstelling van velen bleek uit deze Audit Alert dat de accountants op vaktechnische gronden niet in staat zijn verregaande uitspraken te doen omtrent de millenniumbestendigheid van organisaties. Na verloop van tijd bleek echter dat deze 'voorzichtige' uitspraak terecht is; ook automatiseerders waren zeer terughoudend in het doen van zekerheidgevende uitspraken. Op dit moment spelen accountants in toenemende mate een rol bij het toetsen of organisaties wel voldoende maatregelen treffen om het probleem op te lossen.

In dit artikel zal worden ingegaan op de rol van de accountant, waarbij de rol van het NIVRA nadrukkelijk aan de orde zal komen. Ook zal worden ingegaan op de consequenties voor de toekomstige beroepsuitoefening en de verdere ontwikkeling van het beroep. Eerst wordt echter nog even kort ingegaan op het millenniumprobleem zelf.

HET MILLENNIUMPROBLEEM

Na de vele publicaties over het millenniumprobleem is het nu niet echt meer nodig om nog uitgebreid aandacht te besteden het probleem zelf. Wel is het nog belangrijk even stil te staan bij de objecten waar het millenniumprobleem zich kan voordoen, terwijl ook de hieruit voortvloeiende risico's nog even worden samengevat.

Het millenniumprobleem kan zich in principe voordoen in alle (bedrijfs)processen waarin de volgende objecten worden gebruikt:

- alle soorten toepassingsprogrammatuur;
- technische infrastructuur;
- hardware of componenten;
- embedded software;
- gegevens;
- formulieren en contracten.

Voorbeelden van risico's en de mogelijke gevolgen van het millenniumprobleem zijn onder meer:

- verstoring of uitval van bedrijfsprocessen, hetgeen kan leiden tot discontinuïteit van de organisatie;
- juridische risico's, omdat niet meer voldaan kan worden aan wettelijke of andere juridische verplichtingen;
- financiële risico's, omdat de kosten voor het oplossen van te laat geconstateerde problemen uit de hand kunnen lopen;
- risico's als gevolg van het keteneffect, omdat organisaties steeds meer afhankelijk van elkaar worden;
- het risico dat het probleem wordt onderschat. Te veel organisaties beschouwen het millenniumprobleem nog steeds als een relatief beperkt probleem. Dit alles kan leiden tot imagooverlies of het verlies van marktaandeel.

Door deze risico's is ook de accountant gedwongen aandacht te besteden aan het millenniumprobleem. De waarderings- en resultaatbepalingsgrondslagen zijn immers gebaseerd op de verwachting dat de onderneming zal blijven voortbestaan ('going concern'-gedachte).

Het is echter van groot belang op te merken dat de leiding van de organisatie primair verantwoordelijk blijft voor de aanpak en de oplossing van het millenniumprobleem. Dit geldt voor de bewustwording, het zoeken van oplossingsmogelijkheden en het daadwerkelijk oplossen van het probleem. Ten overvloede wordt nog opgemerkt dat dit geldt voor zowel de eigen systemen als voor de systemen van derden waarvan de organisatie afhankelijk is.

HET MILLENNIUM PLATFORM

Het verstrekken van informatie en het onderling uitwisselen van ervaringen tussen organisaties vervult een belangrijke rol bij de aanpak van het millenniumprobleem. Om hierbij de nodige ondersteuning te kunnen verlenen heeft de overheid in het najaar van 1997 in samenwerking met het VNO-NCW en MKB-Nederland het Millennium Platform opgericht. Het doel van het Platform is bedrijven, instellingen en particulieren te waarschuwen voor de gevolgen van

het millenniumprobleem in hun automatiseringssystemen. Tevens heeft het Platform als doelstelling om breed maatschappelijk de aandacht op het onderwerp te vestigen en de bewustwording over de omvang van de problematiek te vergroten. Daarnaast stimuleert het Platform het realiseren van oplossingen en het uitwisselen van kennis en ervaringen. Het Platform bestaat uit vertegenwoordigers van diverse organisaties. Namens de accountants en de EDP-auditors is de voorzitter van het NIVRA – prof.dr. A.J. Bindinga – begin 1998 als lid tot het Platform toegetreden. Voorzitter van het Platform is J.D. Timmer, voormalig bestuursvoorzitter van Philips.

Voor het realiseren van de doelstellingen heeft het Millennium Platform gekozen voor een sectorbenedering. Via vertegenwoordigers van de verschillende sectoren probeert het Platform de individuele organisaties tot actie te brengen. In zijn hoedanigheid als voorzitter van het Millennium Platform heeft Jan Timmer ook een inleiding verzorgd op de millenniumbijeenkomst die op 12 januari 1998 voor de leden van het Koninklijk Nederlands Instituut van Registeraccountants (NIVRA), de Nederlandse Orde van Accountants-Administratieconsulenten (NOvAA) en de Nederlandse Orde van Register EDP Auditors (NOREA) door de Werkgroep Millennium is georganiseerd. Deze werkgroep is samengesteld uit vertegenwoordigers van de drie hiervoor genoemde organisaties en staat onder voorzitterschap van J. Pasmooij.

DE ACTIVITEITEN VAN HET NIVRA

Gezien de aard en omvang van de millenniumproblematiek was te verwachten dat dit millenniumprobleem ook gevolgen zou hebben voor de beroepsuitoefening van accountants en EDP-auditors. Zij worden, onder meer bij de controle van de jaarrekening, voor de vraag gesteld in hoeverre het millenniumprobleem bedreigend kan zijn voor de continuïteit van de organisaties van hun cliënten. Aangezien accountants en EDP-auditors, mede in het kader van hun controle- en adviestaak, vertrouwd zijn met de organisatiestructuur, de bedrijfsprocessen en de diverse binnen de organisatie werkende systemen, zijn zij een belangrijke gesprekspartner voor de ondernemingsleiding.

Omdat de problematiek om een gezamenlijke aanpak en stellingname vraagt, hebben de besturen van het Koninklijk NIVRA, de NOvAA en de NOREA in het najaar van 1997 een gezamenlijke Werkgroep Millennium in het leven geroepen. Deze werkgroep heeft de gevolgen voor de beroepsuitoefening van deze drie beroepsgroepen bestudeerd en nagegaan welke bijdrage zij kunnen leveren aan de aanpak en oplossing van de millenniumproblematiek. Doordat men gebruik kan maken van de expertise van met name de grote accountantskantoren was het mogelijk in zeer korte tijd de problematiek in kaart te brengen en een handreiking in de vorm van een Audit Alert op te stellen.

Naast concrete handreikingen in de vorm van Audit Alerts heeft de werkgroep een millenniumbrochure *Het Millenniumprobleem Beheerst?!* samengesteld. Deze brochure, die tot doel heeft de cliënten van ac-

countants en EDP-auditors nader te informeren en waar nodig een handreiking te bieden, is in april 1998 beschikbaar gekomen. Daarnaast biedt de brochure accountants en EDP-auditors ondersteuning bij de aanpak van de millenniumproblematiek. Naast de brochure is een folder beschikbaar waarin de hoofdlijnen van de brochure zijn opgenomen. Op dit moment wordt door de werkgroep gewerkt aan het opstellen van een geactualiseerde Audit Alert waarin zal zijn aangegeven hoe om te gaan met de jaarrekening 1998.

In het voorjaar van 1997 is ook door de Fédération des Experts Comptables Européens (FEE) het initiatief genomen voor internationale afstemming tussen de verschillende beroepsorganisaties van accountants. In dat kader is de door het Koninklijk NIVRA uitgebrachte Audit Alert 4 in het Engels vertaald en onder de andere beroepsorganisaties verspreid. Duidelijk is dat de Verenigde Staten, het Verenigd Koninkrijk en Nederland voorlopen op een aantal grote landen binnen Europa.

Voorts is inmiddels door de International Federation of Accountants (IFAC) de International Auditing Practice Statement 1011 – gedateerd juli 1998 – *Implications for Management and Auditors of the Year 2000 Issue* uitgebracht.

HET AUDIT OVERLEG 2000

Recentelijk is door het Millennium Platform het Audit Overleg 2000 ingesteld. Dit overleg bestaat uit vertegenwoordigers van de grote accountantskantoren in Nederland. Het Audit Overleg functioneert binnen de kwaliteitswerkgroep van het Millennium Platform en heeft de volgende doelstelling:

Bij voortdurende vaststellen dat binnen de Nederlandse samenleving de risico's met betrekking tot de millenniumproblematiek zodanig worden beheerst dat een eventuele ontwrichting van de Nederlandse samenleving wordt voorkomen.

In het kader van deze doelstelling worden de volgende activiteiten uitgevoerd:

- volgen van de ontwikkelingen met betrekking tot de sectoren in de Nederlandse samenleving;
- indien voor een bepaald aandachtsgebied de signalen daartoe aanleiding geven, het instellen van een taskforce die het desbetreffende aandachtsgebied nader gaat onderzoeken;
- het uitvoeren van audits op het geselecteerde aandachtsgebied;
- het rapporteren over de uitkomsten van het onderzoek aan het Millennium Platform.

Ten behoeve van de uit te voeren audits staat het Millennium Platform het volgende instrumentarium ter beschikking:

- een vragenlijst ten behoeve van de analyse van het millenniumprobleem;
- een raamwerk dat gebruikt gaat worden voor het uitvoeren van audits;
- auditors voor het uitvoeren van audits.

Voor het uitvoeren van een eigen onderzoek door organisaties wordt door het Audit Overleg een vra-

Het Audit Overleg 2000 bestaat uit vertegenwoordigers van de grote accountantskantoren in Nederland.

genlijst ontwikkeld, ondersteund door middel van een geautomatiseerd hulpmiddel. De invulling van de vragenlijst leidt tot een risicoprofiel waaruit blijkt in hoeverre de organisatie 'millennium-gereed' is. Tevens blijkt uit dit profiel waar extra aandacht nodig is om het millenniumprobleem op te lossen. Het is belangrijk deze vragenlijst in te vullen voorafgaande aan de te organiseren hearings.

Voor het uitvoeren van audits wordt een raamwerk ontwikkeld waarin wordt aangegeven op welke wijze een audit uitgevoerd wordt. Aan de hand van het raamwerk kan de te auditen organisatie inzicht krijgen in de werkzaamheden die door de auditors zullen worden uitgevoerd. Uitgangspunt voor de audit is de hiervoor genoemde vragenlijst. Aan de hand van deze vragenlijst wordt door de auditor de voortgang van het proces beoordeeld. Verder zal tijdens de audits nagegaan worden in hoeverre de beweringen die uit de beantwoording van de vragenlijst blijken, terecht zijn. De audit wordt afgesloten met een rapportage.

De leden van het Audit Overleg vertegenwoordigen de vier grote accountantsorganisaties. Vanuit deze organisaties zullen auditors worden ingezet voor het uitvoeren van de werkzaamheden. Door de inzet van auditors van de grote accountantsorganisaties zijn de onafhankelijkheid, de onpartijdigheid en de deskundigheid gewaarborgd.

DE GEVOLGEN VOOR DE BEROEPSUITOEFENING

Uit de voorgaande paragrafen mag duidelijk zijn geworden dat het millenniumprobleem een maatschappelijk probleem is dat vraagt om een gemeenschappelijke aanpak door alle betrokken partijen, zoals overheid, ondernemingsleiding, werknemers, leveranciers, accountants, EDP-auditors en andere (IT-)deskundigen. Er is weliswaar sprake van een gemeenschappelijke aanpak, maar niet van een gelijke of gemeenschappelijke verantwoordelijkheid. Het is vanzelfsprekend dat de ondernemingsleiding verantwoordelijk is voor de aanpak van het millenniumprobleem vanaf de bewustwording tot en met het zoeken van oplossingsmogelijkheden, de uitvoering van de gekozen oplossing, alsmede de nazorg. Accountants, EDP-auditors en IT-deskundigen kunnen echter wel behulpzaam zijn bij de aanpak van het probleem.

Eind 1997 is Audit Alert nummer 4 gepubliceerd. In deze Alert is aangegeven dat het millenniumprobleem zo complex is dat het vaktechnisch niet verantwoord is oordelen te geven met een hoog zekerheidsgehalte. Het gaat hierbij om oordelen over de millenniumbestendigheid van processen, systemen en/of organisaties. Een belangrijke oorzaak hier-

Het millenniumprobleem is zo complex dat het vaktechnisch niet verantwoord is oordelen te geven met een hoog zekerheidsgehalte.

voor is het feit dat een object niet of nauwelijks geïsoleerd kan worden beoordeeld. Hoewel programmatuur als object op zich wel kan worden beoordeeld op het millenniumbestendig zijn, ontstaan problemen waarin dezelfde programmatuur in combinatie met andere programmatuur (bijvoorbeeld besturingsprogrammatuur) wordt gebruikt.

Gezien deze problematiek wordt in de Audit Alert aangegeven dat wel oordelen gegeven kunnen worden over de aanpak van het millenniumprobleem aangevuld met een rapportage van de bevindingen aan het Bestuur en de Raad van Commissarissen. Om de accountant en de EDP-auditor hierbij behulpzaam te zijn, is een lijst van aandachtspunten en voorbeeldteksten bijgevoegd. Verder is met betrekking tot andere opdrachten, waaronder specifieke millenniumopdrachten, aangegeven dat het wenselijk is dat voorafgaande aan het onderzoek volstreekte duidelijkheid bestaat omtrent de vereiste deskundigheid en de reikwijdte van de opdracht.

Deze Audit Alert leidde tot de nodige kritiek op het functioneren van accountants met betrekking tot het millenniumprobleem. Ook binnen het accountantsberoep heeft dit geleid tot nieuwe discussies, wat uiteindelijk zal moeten leiden tot een nieuwe Audit Alert. In deze Audit Alert nummer 5, die tweede die is gewijd aan de millenniumproblematiek, zal met name de continuïteitsproblematiek verder worden uitgewerkt.

Momenteel werkt de Werkgroep Millennium aan deze nieuwe Audit Alert, waarbij rekening moet worden gehouden met:

- de opvatting van de IFAC, zoals verwoord in de International Auditing Practice Statement 1011, *Implications for Management and Auditors of the Year 2000 Issue*;
- de relevante bepalingen opgenomen in het Burgerlijk Wetboek;
- de Richtlijnen voor de Accountantscontrole;
- de Richtlijnen voor de Jaarverslaggeving.

Recentelijk is, zoals reeds vermeld, de International Auditing Practice Statement 1011 gepubliceerd door de International Auditing Practices Committee (IAPC) van de International Federation of Accountants (IFAC). De doelstelling van deze richtlijn is:

- het verduidelijken van de verantwoordelijkheden van de accountant richting het management van organisaties;

- het aangeven welke informatie de accountant zou moeten opvragen bij het management;
- het aangeven van onderwerpen die gerapporteerd kunnen worden aan het management;
- het verduidelijken van de omstandigheden wanneer de accountant een aangepaste rapportage zou moeten uitbrengen;
- het aangeven hoe omgegaan moet worden met een eventuele verwachtingskloof naar aanleiding van de uitgebrachte rapportage.

Zoals in Audit Alert nummer 4 al is aangegeven, is ook de IAPS-richtlijn duidelijk over de mate van zekerheid die kan worden gegeven. De richtlijn geeft aan dat de verantwoordelijkheden van de accountant niet verder gaan dan de verantwoordelijkheid zoals die voortvloeit uit de verantwoordelijkheden die samenhangen met de jaarrekeningcontrole. Er kan dus nooit enige zekerheid worden gegeven over systemen die geen invloed hebben op de jaarrekening van een onderneming. Het is van groot belang dat de accountant dit aspect duidelijk maakt aan het management. Hierbij wordt aanbevolen aan te geven dat het management primair verantwoordelijk is voor het millenniumbestendig maken van de systemen.

Met betrekking tot de op te vragen informatie bij het management wordt in de richtlijn in het kader van 'understanding the business' een aantal voorbeelden gegeven waarover de accountant nadere informatie zou moeten vragen. Deze zijn:

- de invloed van de automatisering en de embedded software op het dagelijks opereren van de onderneming;
- de aard van de belangrijkste computersystemen die met name financiële informatie opleveren;
- de afhankelijkheid van geautomatiseerde systemen die draaien bij derden en die informatie opleveren ten behoeve van de financiële verantwoording.

Vervolgens moet de accountant voldoende bewijs verkrijgen met betrekking tot het millenniumprobleem. In de richtlijn worden de volgende voorbeelden gegeven waarover de accountant dit bewijs zou moeten verzamelen. De accountant zou zich hierbij het volgende moeten afvragen:

- Is er een systematisch uitgevoerde impactanalyse beschikbaar?
- Zijn alle processen in de impactanalyse betrokken?
- Is er informatie beschikbaar van alle door derden geleverde (standaard)programmatuur?
- Is de impactanalyse uitgevoerd door voldoende deskundig personeel?

Om misverstanden te voorkomen moet de accountant aan het management duidelijk maken wat het management van de accountant mag verwachten. Hoewel het management van de accountant mag verwachten dat hij in het kader van de jaarrekeningcontrole aandacht besteedt aan de voor zijn beroepsuitoefening relevante aspecten met betrekking tot het millenniumprobleem, is het erg belangrijk dat de accountant de beperkingen die hiervoor al uitgebreid aan de orde zijn gekomen, voortdurend aan het management rapporteert. Deze clausules zullen in elke rapportage nadrukkelijk opgenomen moeten worden.

Er kan nooit enige zekerheid worden gegeven over systemen die geen invloed hebben op de jaarrekening van een onderneming.

SLOTOPMERKINGEN

Het zal duidelijk zijn dat het millenniumprobleem een veel grotere impact heeft dan in eerste instantie door velen werd aangenomen. Ook het accountantsberoep is geconfronteerd met deze grotere impact, hetgeen de vraag oproept in hoeverre de accountant wel voldoende deskundig is om een verantwoord oordeel te kunnen geven over de millenniumbestendigheid. Er is in dit verband wellicht sprake van een

verwachtingskloof, omdat velen van mening zijn dat juist de accountant de nodige zekerheid zou kunnen geven terwijl dit uit de uitingen (Audit Alert) niet als zodanig tot uitdrukking komt. Misschien dat het millenniumprobleem weer eens de aandacht vraagt voor deze verwachtingskloof, waarbij nagegaan zou moeten worden over welke IT-kennis de huidige en de toekomstige accountant moet beschikken om in de toekomst de eindverantwoordelijkheid te kunnen blijven dragen.

J.C. van Praat RE RA is directeur bij KMPG EDP Auditors. Na een aantal jaar werkzaam te zijn geweest in de accountantspraktijk is hij reeds vijftien jaar werkzaam als IT-auditor. Hij is tevens hoofd-docent bij de postdoctorale EDP-audit-opleiding aan de Erasmus Universiteit Rotterdam, en lid van een aantal vakcommissies.

CUMULATIEF

OVERZICHT VAN EERDER VERSCHENEN ARTIKELEN IN COMPACT

6 24e jaargang 97/6

Ontwikkelomgevingen

Softwaremetingen binnen het Capability Maturity Model

Drs. C.M. Piek

Selectie van CASE-hulpmiddelen: een casebeschrijving

Drs. ing. R.F. Koorn CISA en J.C.J.M. Vrakking

Benchmarking van systeemontwikkeling

Drs. J.C. de Boer, ir. J.A.M. Donkers RE en ir. K.M. Lof

Multimedia in open omgevingen; de mogelijkheden van het World Wide Web

Drs. A.M. Buren

1 25e jaargang 98/1

Platformen

Common Criteria voor evaluatie van beveiliging van IT-producten

Dr. ir. P.L. Overbeek en ir. G.N. Nelemans

Beheer en beveiliging van Unix-omgevingen

Ir. P. Kornelisse RE

NT en (veilig) netwerken

Ir. drs. J. van der Vlugt

Beveiligingsaspecten van Novell NetWare

Drs. M.J. van Beek RE

2 25e jaargang 98/2

Management van informatietechnologie

De EDP-auditor en de veranderende ICT-organisaties

Drs. J.C. de Boer en drs. J.R.M. Vandecasteele

Strategie en informatietechnologie

Drs. M.W. van Aalst en drs. ing. P. Olieman

Inzicht in de kosten van informatietechnologie

Ir. W.J. Neuteboom, mw. ir. E.R. van Sommeren en drs. R.J.J. Weerts

Inzicht in procescontrol

Drs. J.J. van Beek RE RA en drs. A.R.J. Basten

3 25e jaargang 98/3

Accountantscontrole en ICT

Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?

Prof. A.W. Neisingh RE RA

ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking

J.C. Boer RE RA

EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties

W. de Korte RE RA

Het beheersen van risico's op het gebied van informatiebeveiliging: de visie van een klant

Mr. P. van Dijken

Accountantscontrole, COSO en CobiT

Mw. drs. A.J.M. Koopman

4 25e jaargang 98/4

Electronic commerce

Stand van zaken en ontwikkelingen rond electronic commerce

Drs. A.J. Biesheuvel RA RE en drs. C.F. Olde Olthof

Oplossingen voor veilige electronic commerce over Internet

R.L. Moonen

Als u dan hier even wilt tekenen, op de stippellijn?

Enkele juridische aspecten van electronic commerce

Mw. mr. A.M.Ch. Kemna MBA

De Trusted Third Party als enabler voor electronic commerce

Mw. mr. drs. A.W. Duthler en mw. mr. M.J. Dontje

Electronic commerce en TTP-dienstverlening, een praktijkvoorbeeld uit de bouwbranche

Ing. J.A.M. Hermans en A. Bruggeman

5 25e jaargang 98/5

Informatie(beveiligings)beleid

Hoe helpen we de probleemeigenaar?

Drs. C.J. Coumou en drs. J.W.R. Schoemaker

Corporate Information Security

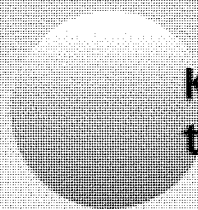
Dr. E.E.O. Roos Lindgreen RE

Informatiebeveiliging voor topmanagers

Drs. A.M. Buren, drs. B. van der Meer, ing. A. Shahim M.Sc., W. Barnhoorn, dr. E.E.O. Roos Lindgreen

Een vertrouwensbasis voor informatiebeveiliging

Dr. ir. P.L. Overbeek



**KPMG EDP Auditors
ten Hagen & Stam Uitgevers**