Wet- en regelgeving rond het betrouwbaarheidsaspect *beschikbaarheid*.

Vanuit het oogpunt van de millenniumproblematiek is recent veel aandacht geweest voor de juridische aansprakelijkheid van organisaties indien de bedrijfsvoering van henzelf dan wel van partners in gevaar komt door datumfouten in soft- en/of hardware. In het onderstaande artikel wordt de wet- en regelgeving met betrekking tot continuïteit van de onderneming in een ruimer verband geschetst.

door Ernst J. Oud

Relevante wetgeving

Beschikbaarheid van bedrijfsprocessen (en dus van de ondersteunende ICT systemen) wordt in enkele wetten en regelgevingen direct en in andere indirect genoemd. Enkele voorbeelden zijn:

- **"Het Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen" van De Nederlandsche Bank**
- **De Wet Toezicht Verzekeringsbedrijf (uitvoering door De Verzekeringskamer)**
- **Het Burgerlijk Wetboek**
- **De Wet Computercriminaliteit**
- **De Archiefwet**
- **De Wet Persoonsregistraties**
- **De Regeling gemeentelijke basis administratie persoonsgegevens (Art. 30)**
- **De Code voor Informatiebeveiliging**
- **Het Voorschrift Informatiebeveiliging Rijksdienst**

Uiteraard zijn niet alle genoemde documenten van toepassing voor iedere organisatie.

Bancaire industrie en overheid

Vanuit haar rol als toezichthouder voor het bankwezen heeft DNB reeds in 1988 eisen gesteld m.b.t. continuïteit aan financiële instellingen. Niet voldoen aan die eisen kan in het ernstigste geval leiden tot het intrekken van de bankvergunning.

Voor de nationale overheid stelt het Voorschrift Informatiebeveiliging Rijksdienst (VIR '94) verplicht dat middels een A&K-analyse maatregelen gekozen moeten worden die o.a. de beschikbaarheid waarborgen en voor lokale overheden is in de GBA wetgeving calamiteitenplanning, inclusief uitwijk, dwingend voorgeschreven.

Bedrijfsleven

Voor overige rechtspersonen blijft uiteraard het in de normale wetboeken gestelde altijd van toepassing. Zo stelt de Wet Persoonsregistraties (WPR) in artikel 8: *"De houder draagt zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of aantasting van de gegevens …"*[1]. De toekomstige Wet Bescherming Persoonsgegevens verklaart waarom een organisatie dit zou moeten doen: *"Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen."*

De bewindsvoerder van een organisatie draagt verantwoordelijkheid voor de continuïteit van de onderneming richting debiteuren, aandeelhouders, personeel, belastingdienst en sociale partners.

[1] In het Advies Beveiliging Persoonsregistraties van de Rekenkamer staan de te treffen maatregelen beschreven.

Business Continuity Management richt zich dan ook op bescherming van mensen, middelen en informatie. Hoe ver wordt deze verantwoordelijkheid door het management echter ook daadwerkelijk genomen? Wordt deze verantwoordelijkheid slechts in woorden neergelegd (elk jaarverslag zal de aandeelhouders en de vakbonden geruststellen dat de onderneming continuïteit nastreeft) of onderneemt het management ook daadwerkelijk actie?

Dit laatste lijkt steeds belangrijker te worden want bijvoorbeeld bij de recente aanpassingen van het Burgerlijk Wetboek (met name in Boek 6, artikel 162) wordt met betrekking tot 'onrechtmatige daad' gesteld dat:

1. *Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.*
2. *Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.*

Ongeschreven recht

De cruciale zinsnede in het BW is 'ongeschreven recht'. Informatiebeveiliging, en daarvan afgeleid het treffen van beschikbaarheidsmaatregelen, is reeds een lang bekend vakgebied. Dan mag toch verondersteld worden dat bestuurders zich als een goed huisvader gedragen en maatregelen treffen. Vooralsnog lijkt het echter geen sinecure een onderneming bij geleden schade aansprakelijk te stellen na een calamiteit indien die onderneming de bedrijfsvoering moest staken, bijvoorbeeld omdat geen beschikbaarheidsmaatregelen, zoals een continuïteitsvoorziening, getroffen waren.

Los van wettelijke beveiligingsvoorschriften legt ons burgerlijke recht iedereen een maatschappelijke verplichting tot zorgvuldigheid op, ook ten aanzien van de toepassing van informatietechnologie en de verwerking van persoonsgegevens. Wie niet beveiligt kan dus alleen al op grond van het civiele recht worden aangesproken, bijvoorbeeld om schade te vergoeden.

Op een andere plaats in boek 6 van het Burgerlijk Wetboek meldt artikel 248: *"Een overeenkomst heeft niet alleen de door partijen overeengekomen rechtsgevolgen, maar ook die welke, naar de aard van de overeenkomst, uit de wet, de gewoonte of de eisen van redelijkheid en billijkheid voortvloeien."* Het bewust bezig zijn met informatiebeveiliging en bedrijfscontinuïteit wordt door de rechter echter waarschijnlijk niet in elke bedrijfstak als 'gewoon' beschouwd.

Onbehoorlijk bestuur

Continuïteitsplanning wordt door de Code voor Informatiebeveiliging als een essentiële en fundamentele maatregel omschreven en is dus van toepassing op elke organisatie en omgeving. Is sprake van mismanagement – onbehoorlijk bestuur dus - als aantoonbaar is dat een onderneming vervolgens geen continuïteitsplanning uitvoert? En zo ja; is daar bij de rechtbank recht voor te behalen? De Code is immers geen wet maar wel een defacto standaard. Goed huisvaderschap vereist voldoen aan 'ongeschreven recht in het maatschappelijk verkeer' volgens het BW; valt de Code daar dan niet expliciet onder? Er is helaas nog geen jurisprudentie op dit specifieke gebied.

Meer opening geeft de wetgeving bij faillissementen. Europese regelgeving (antimisbruikwetgeving) geeft aan, dat in geval de rechtspersoon in gebreke is aan zijn betalingsverplichtingen te voldoen, de bestuurders in persoon, naast de rechtspersoon, aansprakelijk kunnen worden gesteld. Dit geldt indien aannemelijk is dat bestuurder kennelijk onbehoorlijk bestuur is te wijten waaronder onder andere wordt verstaan *"het niet tijdig indekken tegen duidelijk voorzienbare risico's"*. Recent oordeelde de Hoge Raad dat van kennelijk onbehoorlijk bestuur in de regel pas sprake is wanneer een bestuurder heeft gehandeld zoals geen "redelijk denkend bestuurder" zou hebben gedaan.

Bij Getronics Business Continuity worden gemiddeld 3% van de 1500 klanten jaarlijks getroffen door een calamiteit welke de bedrijfsprocessen stillegt; voorwaar een duidelijk voorzienbaar risico waartegen elk redelijk denkende bestuurder toch maatregelen zou moeten treffen.

Een groot deel van de ondernemingen welke getroffen wordt door een calamiteit, gaat failliet binnen de eerste maanden[2]. De curator kan ook volgens Nederlandse wetgeving in het faillissement van een onderneming de bestuurder persoonlijk aansprakelijk stellen indien er in de drie jaren voorafgaand aan het faillissement sprake is geweest van onbehoorlijk bestuur en dat onbehoorlijk bestuur een belangrijke oorzaak is van het faillissement[3]. Ondernemers realiseren zich dikwijls niet dat het niet juist bijhouden en bewaren van hun boekhouding al kan leiden tot de vaststelling dat er kennelijk sprake is van een onbehoorlijke taakvervulling[4].

Verantwoordelijkheid van de handelspartner

Openstaande vraag blijft wat de verantwoordelijkheden zijn van de andere partij. Als die verzuimd heeft te informeren (in contract en leveringsvoorwaarden e.d.) naar de continuïteit van zijn partner is continuïteit dan impliciet? Welk risico zal een belanghebbende als afgedekt aannemen en welke geleden schade na een calamiteit bij zijn handelspartner zal deze vervolgens niet accepteren? Bij de grote stroomstoring in 1995 in het midden van het land hebben bedrijven wel geprobeerd de NUON aansprakelijk te stellen voor de geleden schade maar voor zover bekend hebben bedrijven welke van elkaar afhankelijk waren dat onderling niet gedaan. Klaarblijkelijk had men toch begrip voor de ontstane calamiteit ondanks het feit dat duidelijk was dat veel organisaties eigenlijk een noodstroomvoorziening hadden moeten hebben. Waar stopt de verantwoordelijkheid?

Verstoring van het bedrijfsproces schaadt altijd het product van dat bedrijfsproces (in kwaliteit of kwantiteit) of de verstoring schaadt de omgeving (de mens of het milieu). Productaansprakelijkheid neemt toe; wat als de kwaliteit van het geproduceerde (product of dienst) leidt tot claims bijvoorbeeld als IT systemen bij uitval de arbeidsomstandigheden verslechteren of de milieuwetgeving passeren? Met betrekking tot kwantiteit; wat als bij een calamiteit niet voldaan wordt aan de eisen in contracten met afnemers? Leveringscontracten zijn vaak bindend en het niet nakomen ervan bij calamiteiten zal niet altijd door een rechter als overmacht gezien worden.

Overmacht

Overmacht is volgens van Dale: *"niet toerekenbare onmogelijkheid om zijn verplichting na te komen"* hetgeen de vraag doet rijzen wat 'niet toerekenbaar' is. Het is dus raadzaam in de algemene leveringsvoorwaarden toe te lichten wat men tot overmacht rekent, in de trant van: *"Niet toerekenbare tekortkomingen omvatten, maar zijn niet beperkt tot de volgende gebeurtenissen en/of situaties: besluiten en maatregelen van enige overheid, het uitblijven van vereiste vergunningen of andere formaliteiten van overheden van welke aard ook, arbeidsconflicten, gebrek aan personeel, tekort aan grondstoffen of onderdelen, gebrek aan of vertragingen in vervoer, diefstal, bezitsverlies of vernietiging c.q. beschadiging van bedrijfsmiddelen of -gegevens, niet, niet goed of niet tijdig presteren van leveranciers, rechthebbenden en andere contractanten van ..."*

Mr. W.Th.A. Schermer is advocaat bij Benthem en Keulen Advocaten in Utrecht en houdt zich bezig met de juridische aspecten rond de informatietechnologie.

Hij stelde onlangs, gevraagd naar de gevolgen van de millenniumproblematiek[5]: *"Een bedrijf kan geraakt worden in de continuïteit van zijn bedrijfsvoering. Dat kan gevolgen hebben voor zijn verplichtingen jegens zijn afnemers. Het zal niet gemakkelijk zijn om je te verschuilen achter overmacht. De rechter zal ongetwijfeld oordelen dat de schade behoort tot het risico van degene die tegen het probleem aanloopt. Ik sluit echter niet uit dat de rechter bij het vaststellen van de te betalen schadevergoeding zal uitgaan van de aantoonbare maatregelen die zijn genomen om te proberen de problemen te voorkomen"*.

Met betrekking tot verzekering van bedrijven tegen aansprakelijkheden voortkomende uit de millenniumproblematiek wordt gesproken van zorgplicht. Is die zorgplicht er eigenlijk niet altijd? 'De kwestie van 'onbehoorlijk bestuur' speelt al jaren. Als bestuurders verzuimen om tijdig maatregelen te nemen waardoor een onderneming in ernstige moeilijkheden raakt of failliet gaat, dan kunnen zij daarvoor dus persoonlijk aansprakelijk worden gesteld.

---

[2] Driekwart van die ondernemingen bestaat na drie jaar niet meer.
[3] Voor sommige rechtspersonen (zoals verenigingen, stichtingen) is deze aansprakelijkheid deels te verzekeren.
[4] Artikel 10 Titel 1 Boek 2 van het Burgerlijk Wetboek.
[5] Millenniumprobleem loopt in de papieren - Cok de Zwart - PolyTechnisch tijdschrift - juli 1998.

Rol van de accountant

Wat is de rol van de (EDP-)accountant hierin? Uiteraard zal de accountant het conformeren aan de wet- en regelgeving op ICT gebied dienen te auditen; CobiT Control Objective 8.1 bevat immers de zinsnede *"Legal, government or other external requirements related to information technology practices and controls should be reviewed."*

Het is niet ondenkbaar dat de accountant in toenemende mate verantwoordelijkheid zal nemen en gezien de bestuurders- en productaansprakelijkheid dus steeds meer eisen zal stellen aan waarborgen met betrekking tot de beschikbaarheid van de onderneming.

Met de komst van de Wet Computercriminaliteit (1993) werd reeds aan het vierde lid van artikel 393 van boek 2 van het Burgerlijk Wetboek toegevoegd *"Hij (de controlerende accountant) maakt daarbij (bij de controle van de jaarrekening) ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking."*

Dit laatste leidde tot Nivra studierapport 34[6] waarin een zeer hoog gewicht toegekend is aan de maatregel *"De implementatie van back-up, recovery en uitwijkbeleid, … dient de beschikbaarheid in voldoende mate te waarborgen."* [7] Dit gewicht zal met de toenemende afhankelijkheid van informatiesystemen, bestuurders- en productverantwoordelijkheid alleen maar toenemen.

Ernst J. Oud (e.j.oud@getronics.nl) is senior consultant bij Getronics Business Continuity BV te Lelystad.

[6] Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole – NIVRA 1995.
[7] De NIVRA is van mening dat de kwaliteitsdoelstelling 'continuïteit' niet tot de reikwijdte van de jaarrekening edp-audit behoort.