## Cybercriminaliteit: aansprakelijkheid (II)

In de hedendaagse digitale wereld vormen cyberincidenten een steeds grotere bedreiging voor ondernemingen. De versnelde digitalisering, aangewakkerd door de COVID-19-pandemie, heeft ondernemingen kwetsbaar gemaakt voor zware, georganiseerde cybercriminaliteit. Een dergelijk incident kan leiden tot uitval van digitale systemen. Dat dit enorme gevolgen kan hebben, bleek onlangs nog uit de ICT-storing die werd veroorzaakt door een fout in een update van cyberbeveiligingsbedrijf CrowdStrike. Dit leidde wereldwijd tot chaos, verstoringen en hinder, zo ook in Nederland: vluchten werden geschrapt, ziekenhuisoperaties werden uitgesteld en noodnummers vielen uit.

Als een onderneming door een cyberincident wordt getroffen, kan deze aansprakelijk worden gesteld voor de daaruit voortvloeiende schade. In een eerdere bijdrage is aandacht besteed aan de problematiek rondom de normschending. In dit deel belichten Robert Pessers en Annevi Etienne een aantal juridische uitdagingen die hierbij een rol kunnen spelen: Welke instrumenten biedt het bewijsrecht bij het vaststellen van het vereiste causaal verband? Aan welke vereisten moet worden voldaan voor toekenning van schadevergoeding? En de mogelijkheid om geleden schade te verhalen op de IT-leverancier: wanneer is sprake van een schending van de (bijzondere) zorgplicht van de IT-leverancier?

### 1. Inleiding

Tegenwoordig is vrijwel iedere organisatie in hoge mate gedigitaliseerd, er zijn nog amper processen zonder digitale component. De COVID-19-pandemie heeft dit proces verder versneld. Dit heeft ook een keerzijde: de afhankelijkheid van digitale processen maakt organisaties kwetsbaar voor cybercriminaliteit. Zware, georganiseerde criminaliteit is sterk toegenomen en maakt daardoor de afgelopen jaren meer slachtoffers, meer schade en is voor criminelen lucratiever dan ooit. Dit blijkt uit het door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gepubliceerde 'Cybersecuritybeeld Nederland 2023'.[1] Daarmee neemt de kans op cyberaanvallen steeds meer toe.

In het geval dat een onderneming getroffen wordt door een cyberincident, dan rijst de vraag in hoeverre het aansprakelijkheidsrecht mogelijkheden biedt om de door betrokkenen geleden schade op de onderneming te verhalen. Cyberincidenten kunnen immers tot schade bij de organisatie zelf leiden, maar ook bij klanten of derden. Dit kan zich vertalen in een vordering tot vergoeding van de geleden materiële en immateriële schade.

Om aanspraak te kunnen maken op schadevergoeding is vereist dat vast komt te staan dat er een grondslag voor de aansprakelijkheid is, dat sprake is van schade én dat er een causaal verband bestaat tussen de aansprakelijkheidsvestigende gebeurtenis en de schade. De grondslag voor aansprakelijkheid kan onder meer gebaseerd worden op wanprestatie (art. 6:74 BW) of onrechtmatige daad (art. 6:162 BW). In geval van een daarop gebaseerde schadevergoedingsvordering kan een schadelijdende partij tegen diverse obstakels aanlopen als het gaat om het bewijzen van de normschending, causaal verband en schade. In een eerder bijdrage is aandacht besteed aan de problematiek rondom de normschending. In deze bijdrage zal eerst worden ingegaan op de juridische barrières ten aanzien van het causaal verband en de schade.[2] Wij zullen met name aandacht besteden aan cyberaanvallen waarbij persoonsgegevens worden gestolen of gelekt. Hierbij zal eerst het toepasselijke juridische kader worden geschetst, waarna een concreet zal worden gegeven.

Indien een onderneming aansprakelijk kan worden gehouden, kan deze trachten regres te nemen op de IT-leverancier. Veel ondernemingen besteden immers hun IT uit aan een IT-leverancier. In die gevallen kan de vraag opkomen of sprake is van een schending van de (bijzondere) zorgplicht van de IT-leverancier. In het laatste deel van deze

[1] NCTV, *Cybersecuritybeeld Nederland 2023*, juni 2023, Den Haag: NCTV. Te raadplegen op https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023.
[2] https://www.vantraa.nl/nl/kennis/cybercriminaliteit-aansprakelijkheid-deel-1-van-2/.

bijdrage zal hieraan aandacht worden besteed, aan de hand van recente jurisprudentie.

## 2. Causaal verband

Zowel art. 6:74 BW als art. 6:162 BW stelt het bestaan van causaal verband tussen het normschendend gedrag en de schade als voorwaarde voor een recht op schadevergoeding. Dit betekent dat de schadelijdende partij voldoende feiten en omstandigheden moet stellen waaruit afgeleid kan worden dat de schade niet zou zijn ontstaan indien de desbetreffende gebeurtenis niet zou hebben plaatsgevonden. Met andere woorden: zou ook schade zijn ingetreden zonder inadequate beveiligingsmaatregelen? Wil de schadelijdende partij zijn schade op de schadeveroorzaker verhalen, dan moet dus worden aangetoond dat zijn schade door de cyberonveiligheid van de betrokken onderneming is veroorzaakt.

In de literatuur wordt gesteld dat het aantonen van het causaal verband één van de grootste barrières vormt voor het vestigen van aansprakelijkheid op het gebied van cyber.[3] Zo achten Tjong Tjin Tai en Koops een "*claim door een derde niet kansrijk aangezien hij zou moeten bewijzen dat er causaal verband is tussen een concrete veiligheidsfout, en de cybercrime waar hij slachtoffer van is. Bewezen zal moeten worden dat de concrete geïnfecteerde computers betrokken waren bij de cybercrime, en dat deze met malware geïnfecteerd zijn geraakt als gevolg van die concrete veiligheidsfout. Dat laatste lijkt onmogelijk aan te tonen*."[4]

Hoofdregel is dat de stelplicht en de bewijslast ter zake van het condicio sine qua non-verband op de schadelijdende partij rust (art. 150 Rv). Zoals gezegd, is het voor de schadelijdende partij niet altijd mogelijk om dit aan te tonen. Nu vrijwel iedere organisatie gebruik maakt van digitale processen, is er een groot aantal mogelijke schadeveroorzakers. Dat bemoeilijkt het leveren van het benodigde bewijs. Het is immers mogelijk dat de gegevens langs andere weg bekend zijn geworden of uitgelekt, mogelijk zelfs door het handelen van de schadelijdende partij zelf.[5]

In de jurisprudentie zijn verschillende 'instrumenten' – ook wel: bewijsrechtelijke tegemoetkomingen – ontwikkeld om aan de bewijsnood van de schadelijdende partij tegemoet te komen. De volgende instrumenten zullen hieronder in een vogelvlucht worden besproken:

(i) de omkering van de bewijslast;
(ii) het voorshands bewijsoordeel;
(iii) de verzwaarde (stel/)motiveringsplicht;
(iv) proportionele aansprakelijkheid.

### *i. De omkering van de bewijslast*

De meest vergaande stap is het omkeren van de bewijslast. Art. 150 Rv biedt de ruimte om de bewijslast op grond van redelijkheid en billijkheid om te keren. Het is dan aan de organisatie die het slachtoffer is geworden van cybercriminaliteit om te bewijzen dat géén causaal verband bestaat tussen de cybercrime en de schade. Het volledige bewijsrisico komt dan op de organisatie te rusten. Een dergelijke vergaande stap zal slechts bij uitzondering worden genomen.

Voor toepassing van de omkeringsregel is alleen plaats als het gaat om een (geschreven of ongeschreven) norm die ertoe strekt een specifiek gevaar ter zake van het ontstaan van schade bij een ander te voorkomen, en dit specifieke gevaar zich heeft verwezenlijkt. De geschonden norm moet dus een specifiek gevaar beogen te voorkomen. Hierbij zou gedacht kunnen worden aan specifieke normen in de regelgeving op het gebied van cybersecurity, zoals Europese regelgeving (NIB-richtlijn en Cybersecurity Act) of een wet in formele zin (Wbni). Deze zijn immers opgesteld om een specifiek gevaar te voorkomen, namelijk het beschermen van de ICT-systemen van aanbieders en het verkleinen van de gevolgen van incidenten, hetgeen zich vervolgens verwezenlijkt.

### *ii. Het voorshands bewijsoordeel*

Er is ook minder vergaande stap mogelijk dan de regelrechte omkering, het voorshandse bewijsoordeel. In dat geval wordt het bewijs van

[3] B.F.H. Nieuwesteeg, L.T. Visscher, M.G. Faure & N.M. Brouwer, 'Contractuele aansprakelijkheid voor digitale onveiligheid in B2B relaties', *AV&S* 2020/22, afl. 4.
[4] T.F.E. Tjong Tjin Tai & B.J. Koops, 'Zorgplichten tegen cybercrime', *Nederlands Juristenblad* 2015, p. 1068.
[5] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 462.

het causaal verband op basis van de door de schadelijdende partij aangevoerde bewijsmiddelen 'voorshands' als geleverd beschouwd. Een condicio sine qua non-verband kan met behulp van een wettelijk vermoeden of een rechterlijk (ook wel genoemd feitelijk) vermoeden worden aanvaard. De partij in wiens voordeel dat is geschied hoeft dan geen nader bewijs te leveren.[6]

Het is dan aan de tegenpartij om tegen dit vermoeden tegenbewijs te leveren. Hiervoor is voldoende dat het bewijs dat voorshands geleverd was, erdoor wordt ontzenuwd.[7] Of, in de woorden van Asser: strikt genomen is al voldoende dat door de tegenbewijslevering zoveel twijfel wordt gezaaid dat die vaststelling onhoudbaar wordt.[8]

Hiervoor kan plaats zijn indien de rechter redenen aanwezig acht om 'voorshands' uit te gaan van de aanwezigheid van een condicio sine qua non-verband. Denkbaar is dat het onwenselijk wordt geacht als de schadelijdende partij met zijn eigen schade achterblijft, omdat het causaal verband niet aangetoond kan worden terwijl de organisatie wel bekend heeft gemaakt dat sprake was van een cyberaanval waarbij mogelijk persoonsgegevens zijn gelekt.

Illustratief in dit verband is de cyberaanval op ruim 120 tandartsparktijken in Nederland die hierdoor hun deuren moesten sluiten.[9] Colosseum Dental Benelux, het bedrijf waarbij de praktijken aangesloten zijn, heeft twee miljoen euro moeten betalen om weer toegang tot de patiëntgegevens te krijgen. "*Met direct betrokkenen zoeken wij contact zodra daarvoor voldoende feiten zijn en aanleiding is. […] Wij betreuren ten zeerste dat met deze cyberaanval onze zorgplicht voor onze patiënten zo ernstig verstoord werd. In onze praktijken worden ook persoonlijk excuses aangeboden bij patiënten die ongemak ondervonden*", aldus Colosseum Dental Benelux.[10] In een dergelijk geval – waarin de organisatie bekendmaakt dat patiëntgegevens zijn buitgemaakt – ligt het voor de hand dat het causaal verband voorshands als bewezen wordt geacht.

*iii. De verzwaarde motiveringsplicht*

Daarnaast kan de verzwaarde motiveringsplicht (ook wel de verzwaarde stelplicht) een oplossing kunnen bieden voor de bewijsnood van de schadelijdende partij.[11] Dit houdt in dat van de partij op wie niet de bewijslast rust verwacht wordt dat deze zijn stellingen extra motiveert. Dat betekent dat de wederpartij bij zijn betwisting van de stellingen voldoende feitelijke gegevens moet verstrekken. Die gegevens moeten de partij met de bewijslast in staat stellen daaraan te voldoen.[12] In andere woorden: de partij op wie de verzwaarde motiveringsplicht rust, dient zijn wederpartij tot op zekere hoogte te helpen met het voldoen aan diens bewijslast.[13] De bewijslast wordt daarmee niet verschoven, maar de bewijsvoeringslast van de schadelijdende partij wordt verlicht.[14]

Deze methode is al op verschillende gebieden ingezet om de bewijspositie tussen partijen met elkaar in evenwicht te brengen, waaronder bij aansprakelijkheid van artsen, notarissen en bestuurders.[15] In deze gevallen liggen de relevante feiten om het causaal verband aan te tonen in het domein van de partij die niet de bewijslast draagt. Zo bevindt de informatie over het verloop van de operatie zich bij de arts, terwijl het aan de patiënt is om te bewijzen dat tijdens de ingreep een fout is gemaakt. De patiënt is echter doorgaans onwetend over de wijze waarop de behandeling bij hem heeft plaatsgevonden, bijvoorbeeld omdat hij onder narcose was.[16] In dat geval wordt het onacceptabel

[6] R.J.B. Boonekamp & W.L. Valk (red.), Stelplicht & Bewijslast, Deventer: Wolters Kluwer, par. 4.3.1.
[7] N. van Tiggele-van der Velde, *Bewijsrechtelijke verhoudingen in het verzekeringsrecht(Verzekeringsrecht) (diss. Rotterdam)*, Deventer: Kluwer 2008/1.2.2.1.
[8] W.D.H. Asser, *Bewijslastverdeling*, Deventer: Kluwer 2004, nr. 46.
[9] 'Zo'n 120 Nederlandse tandartspraktijken komende dagen dicht door cyberaanval', nu.nl; 'Tandartsbedrijf betaalt internetcriminelen losgeld na ransomware-aanval', nos.nl.
[10] https://www.colosseumdental.nl/mededeling-cyberincident/.
[11] De verzwaarde motiveringsplicht vloeit voort uit de eisen van redelijkheid en billijkheid.
[12] N. van Tiggele-van der Velde, *Bewijsrechtelijke verhoudingen in het verzekeringsrecht(Verzekeringsrecht) (diss. Rotterdam)*, Deventer: Kluwer 2008/1.2.2.2.
[13] T. Holsbrink & V.R. Pool, 'De verzwaarde motiveringsplicht in het wegvervoer', *NTHR* 2022-1, p. 9. Te raadplegen op: https://www.vantraa.nl/nl/kennis/de-verzwaarde-motiveringsplicht-in-het-wegvervoer/.
[14] R.P. Wijne, 'De verzwaarde motiveringsplicht', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer.
[15] Zie voor een uiteenzetting van de jurisprudentie: T. Holsbrink & V.R. Pool, 'De verzwaarde motiveringsplicht in het wegvervoer', *NTHR* 2022-1, p. 9. Zie bijvoorbeeld: HR 15 december 2006, ECLI:NL:HR:2006:AZ1083, *NJ* 2007/203, m.nt. M.R. Mok (*NNEK/Mourik*) en HR 11 januari 2019, ECLI:NL:HR:2019:3, *NJ* 2019/48 (*Notaris*).
[16] *GS Bijzondere overeenkomsten*, art. 7:454 BW, aant. 9.

gevonden als de arts zijn kaarten tegen de borst kan houden en de patiënt daardoor het bewijs niet rond kan krijgen. Om te voorkomen dat de partij die de bewijslast draagt – in dit geval de patiënt – hierdoor met een onevenredig zware bewijslast wordt opgezadeld, wordt in dit soort gevallen de verzwaarde motiveringsplicht toegepast.[17]

Eenzelfde redenering kan worden gevolgd wanneer zich een cyberincident voordoet. De informatie over het eventuele tekortschieten van de getroffen onderneming bevindt zich immers in het domein van die onderneming, in plaats van bij de derde partij die daardoor schade lijdt. Indien in een dergelijk geval de verzwaarde motiveringsplicht wordt toegepast, zal de getroffen onderneming bijvoorbeeld de benodigde logs van het cybersecurityincident aan de betrokkene moeten verschaffen.

*iv. Proportionele aansprakelijkheid*

Indien één van de mogelijke oorzaken van de schade binnen de risicosfeer van de schadelijdende derde valt, kan het leerstuk van proportionele aansprakelijkheid toepassing vinden. Hoewel het leerstuk veelal uitwerking vindt in geval van multicausale beroepsziekten, kan dit wellicht ook in de context van cyber worden geplaatst.

Gedacht kan worden aan het voorbeeld waarin de getroffen onderneming nalatig is geweest bij het treffen van adequate beveiligingsmaatregelen, maar ook de schadelijdende derde onzorgvuldig is geweest bij het beheren van een kopie van zijn identiteitsbewijs. In dat geval kan de rechter de aansprakelijkheid vaststellen naar rato van waarschijnlijkheid dat de schade is veroorzaakt door het lekken van de kopie door de organisatie. Deze benadering is passend als het causaal verband tussen de normschending en de schade zich niet of nauwelijks laat vaststellen, en de kans dat de schade is veroorzaakt door het lek niet zeer klein of zeer groot is.[18] Hierbij dient men zich te realiseren dat de Hoge Raad van oordeel is dat de proportionele benadering met terughoudendheid moet worden toegepast.[19]

[17] T. Holsbrink & V.R. Pool, 'De verzwaarde motiveringsplicht in het wegvervoer', *NTHR* 2022-1, p. 9.
[18] HR 31 maart 2006, ECLI:NL:HR:2006:AU6092, *NJ* 2011/250, m.nt. Tjong Tjin Tain (*Nefalit/Karamus*).
[19] HR 24 december 2010, ECLI:NL:HR:2010:BO1799, *NJ* 2011/251, m.nt. Tjong Tjin Tai (*Fortis/Bourgonje*).

## 3. Schade

Indien zich een cyberincident bij een onderneming voordoet, kan schade aan derden worden veroorzaakt. Indien de derde een particulier is kunnen vertrouwelijke persoonsgegevens worden gelekt, waarmee bankrekeningen kunnen worden leeggetrokken[20] of kunnen die gegevens worden gebruikt om toegang te krijgen tot andere systemen. In het geval dat de derde een onderneming is en privacygevoelige gegevens over de bedrijfsvoering worden gelekt, kunnen schades zoals bedrijfsstilstand, winstderving en kosten van crisismanagement optreden. Ook kunnen gegevens openbaar worden gemaakt, waardoor de derde reputatieschade lijdt. Daar komt bij dat dergelijke gegevens, als zij eenmaal gelekt zijn, langdurig bewaard kunnen blijven en veel later alsnog of nogmaals kunnen worden gebruikt.

De derde heeft in dat geval recht op vergoeding van zijn vermogensschade (art. 6:96 BW). Daarnaast komen de buitengerechtelijke kosten voor vergoeding in aanmerking op grond van art. 6:96 lid 2 sub a BW, voor zover deze kosten de 'dubbele redelijkheidstoets' doorstaan: het maken van de kosten moet redelijk zijn geweest en de omvang van de kosten moet redelijk zijn.[21]

Een cyberincident kan ook immateriële schade opleveren, bijvoorbeeld gevoelens van angst of controleverlies. Voor zover de getroffen onderneming kwalificeert als een dataverwerker, biedt artikel 82 lid 1 AVG in dat geval een grond voor vergoeding van deze schade. Op 4 mei 2023 heeft het HvJ EU zich uitgelaten over de invulling van dit artikel.[22] Daaruit blijkt dat een enkele inbreuk op de AVG onvoldoende is voor een vordering tot schadevergoeding, er moet daadwerkelijk schade zijn geleden, aldus het HvJ EU.[23] Tegelijkertijd mag het nationale recht echter geen drempel hanteren ten aanzien van de ernst

[20] Men kan contact opnemen met de bank door zich telefonisch vals te identificeren op basis van de persoonsgegevens.
[21] HR 16 oktober 1998, ECLI:NL:HR:1998:ZC2740, *NJ* 1999/196, m.nt. A.R. Bloembergen (*AMEV/Staat*), r.o. 3.6.
[22] HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, nr. C-300/21. Concl. A-G. Campos Sánchez-Bordona bij HvJEU 6 oktober 2022, ECLI:EU:C2022:756, C-300/21 (*UI/Österreichische Post AG*).
[23] Art. 82 AVG heeft dus geen punitief karakter.

van die schade.[24] De nationale rechters moeten bij de vaststelling van de hoogte van de schadevergoeding de interne regels van elke lidstaat over de omvang van de schadevergoeding toepassen, mits de Unierechtelijke beginselen van gelijkwaardigheid en doeltreffendheid in acht worden genomen.[25]

Een schadevergoeding voor immateriële schade wordt naar Nederlands recht gebaseerd op artikel 6:106 sub b BW. Dit artikel vereist dat de derde door de gebeurtenis in zijn 'eer of goede naam is geschaad' of 'in zijn persoon is aangetast'. Vooral de persoonsaantasting speelt een rol bij een privacy-inbreuk. Beslissend of sprake is van een persoonsaantasting, zijn de aard en de ernst van de normschending en de gevolgen daarvan.[26] De schadelijdende partij dient de immateriële gevolgen van de normschending concreet te onderbouwen. Geestelijk letsel is niet vereist.[27] Uit de Nederlandse rechtspraak volgt dat de schadevergoeding voor immateriële schade door een datalek beperkt is: de smartengeldbedragen schommelen over het algemeen onder de EUR 1.000.[28]

*Illustratief in dit verband is de cyberaanval op ruim 120 tandartsparktijken in Nederland die hierdoor hun deuren moesten sluiten. Colosseum Dental Benelux, het bedrijf waarbij de praktijken aangesloten zijn, heeft twee miljoen euro moeten betalen om weer toegang tot de patiëntgegevens te krijgen*

[24] Prof. mr. S.D. Lindenbergh en mr. drs. M.C. Samson, 'Smartengeld wegens AVG-inbreuken na 'Österreichische Post', *NJB* 2023, afl. 23.
[25] *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 82 AVG.
[26] HR 15 maart 2019, ECLI:NL:HR:2019:376, *NJ* 2019/162, m.nt. S.D. Lindenbergh (*EBI*).
[27] HR 15 maart 2019, ECLI:NL:HR:2019:376, *NJ* 2019/162, m.nt. S.D. Lindenbergh (*EBI*).
[28] Rb. Gelderland 4 oktober 2023, ECLI:NL:RBGEL:2023:5435, r.o. 4.5-4.8, waarin een schadevergoeding van € 300,00 is toegewezen; Rb. Noord-Nederland 12 januari 2021, ECLI:NL:RBNNE:2021:106, r.o. 4.28, waarin een schadebedrag van € 500 is toegewezen; Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490, schadevergoeding van € 250,00 is toegewezen; Zie voor een afwijzend oordeel de uitspraak van de Rb. Gelderland van 7 april 2021, ECLI:NL:RBGEL:2021:1888.

## 4. Aansprakelijkheid IT-leveranciers

Veel ondernemingen besteden hun IT geheel of gedeeltelijk uit aan een IT-leverancier. Door de kenniskloof tussen de klant en de IT-leverancier, zijn de meeste ondernemingen in grote mate afhankelijk van de IT-diensten die worden geleverd en de adviezen van de IT-leveranciers. Indien deze systemen niet deugdelijk werken, kan de onderneming zijn IT-leverancier aanspreken langs de band van de (bijzondere) zorgplicht. Deze zorgplicht kan voortvloeien uit de met de IT-leverancier gesloten overeenkomst of uit onrechtmatige daad.

*Zorgplicht uit overeenkomst*

In beginsel kunnen partijen overeenkomen wat van de IT-leverancier ter zake van cyberveiligheid wordt verwacht. In de praktijk komt het echter veelal voor dat IT-leveranciers trachten de risico's bij de minst machtige partij (veelal de afnemer) te leggen. Denk bijvoorbeeld aan het formuleren van vage en algemene inspanningsverbintenissen, omdat de schending daarvan moeilijker is aan te tonen dan de schending van een strenge en zeer specifieke norm. Of denk aan het uitsluiten van verantwoordelijkheid en/of aansprakelijkheid in de algemene voorwaarden.[29]

Inmiddels groeit de aandacht voor deze praktijken en wordt gewerkt aan adequate zorgplichten voor IT-dienstverleners. Wanneer die ontbreken, kan worden teruggevallen op art. 7:401 lid 1 BW.[30] Dit artikel bepaalt dat een opdrachtnemer bij zijn werkzaamheden de zorg van een goed opdrachtnemer in acht moet nemen. Dit wordt uitgelegd als "de zorg die van een redelijk bekwaam en redelijk handelend vakgenoot – de maatman – mag worden verwacht". Afgevraagd kan worden wat van een redelijke handelende en bekwame IT-leverancier, de maatman, verwacht mag worden. In de rechtspraak zijn hiervan veel voorbeelden te vinden, die zijn toegesneden op de omstandigheden van het geval.[31]

[29] B. Nieuwesteeg e.a. 'Contractuele aansprakelijkheid voor digitale onveiligheid in B2B-relaties, *AV&S* 2020/22, p. 130.
[30] Doorgaans zal een IT-overeenkomst kwalificeren als een overeenkomst van opdracht, waarbij de IT-leverancier de opdrachtnemer is.
[31] P.G. van der Putt & C.A.M. van de Bunt, 'Update Nederlandse zorgplicht-jurisprudentie', *Computerrecht* 2021/207, p. 404.

Inmiddels is uitdrukkelijk aangenomen dat op IT-leveranciers een bijzondere zorgplicht kan rusten.[32] Illustratief in dit verband is de volgende zaak. Een onderneming heeft het netwerk- en systeembeheer neergelegd bij IT-dienstverlener A. Zij besluit over te gaan naar B. De overeenkomst eindigt op 21 juni 2016. Op 19 juli 2016 wordt de onderneming getroffen door een ransomware-aanval.[33] Doordat de voormalig IT-leverancier geen back-ups had gemaakt, stelt de klant dat het systeem niet kon worden hersteld en dat daarom het geëiste losgeld ter waarde van € 17.000,- moest worden betaald. De voormalig ICT-leverancier kon hiervoor aansprakelijk worden gehouden, omdat de tekortkoming ertoe heeft geleid dat de klant niet adequaat kon acteren tegen de ransomware-aanval.

Dat de zorgplicht van de IT-leverancier ver strekt, volgt eveneens uit een uitspraak van de rechtbank Amsterdam. Hierin werd geoordeeld dat op de IT-leverancier die een totaalpakket levert ook de verplichting rust om zorg te dragen voor adeq beveiligingsmaatregelen.[34] Indien een IT-leverancier door toedoen van de klant de beveiligingsmaatregelen niet kan treffen, "*brengt de zorgplicht mee dat de IT-leverander de opdracht wegens onuitvoerbaarheid dient te weigeren, alternatieven dient aan te dragen, of indringend en herhaaldelijk dient te waarschuwen over risico's*". De IT-leverancier werd op deze grond medeverantwoordelijk gehouden voor het ontstaan van de ransomware aanval en werd in dit geval aansprakelijk gehouden voor twee derde van de schade die de klant als gevolg daarvan heeft geleden.

Ook kunnen de eigen gedragingen van de getroffen onderneming een rol spelen bij de beoordeling van de aansprakelijkheid van de IT-leverancier, zo blijkt uit een uitspraak van de rechtbank Overijssel.[35] De casus was al volgt: eind 2020 heeft bij de gemeente Hof van Twente een cyberaanval plaatsgevonden. Daarbij zijn de systemen van het netwerk van de gemeente en de back-up versleuteld en ontoegankelijk gemaakt en vele virtuele servers verwijderd. De gemeente stelt dat haar ICT-beheerder is tekortgeschoten in de nakoming van zijn verplichtingen, althans zijn zorgplicht heeft geschonden, althans onrechtmatig heeft gehandeld. De rechtbank wijst de vorderingen af. Daarbij wordt overwogen dat de gemeente zelf steken heeft laten vallen, door onder andere een eigen internetverbinding te willen hebben met de back-up, een account met de hoogste rechten te beheren, het wachtwoord 'Welkom 2020' te gebruiken en (kennelijk uit kostenoverwegingen) niet in te gaan op een voorstel tot verbetering van de beveiliging dat de ICT-beheerder had gedaan.[36]

Zoals uit bovenstaande uitspraken valt op te maken, blijft de zorgplicht van IT-leveranciers voor cybersecurity een casuïstische aangelegenheid. Gelet op de toename van de omvang en ernst van de cyberrisico's, is het de vraag of dit wenselijk is.[37] Om hieraan tegemoet te komen wordt gepleit voor het vormgeven van een cybersecuritystandaard die in de contracten van B2B-relaties kan worden opgenomen.[38] Vaststaat in ieder geval dat organisaties duidelijke, afdwingbare verplichtingen overeen moeten komen met een IT-leverancier om deze met succes aan te kunnen spreken.[39]

*Zorgplicht uit onrechtmatige daad*

Een IT-leverancier zou, onder omstandigheden, ook op grond van onrechtmatige daad kunnen worden aangesproken. Zo kan de zorgplicht van de IT-leverancier tevens voortvloeien uit de regels van het maatschappelijk verkeer.[40] De zorgplicht uit hoofde van de onrechtmatige daad wordt

[32] P.G. van der Putt & C.A.M. van de Bunt, 'Update Nederlandse zorgplicht-jurisprudentie', *Computerrecht* 2021/207, p. 403; Rb. Amsterdam 18 augustus 2020, ECLI:NL:RBAMS:2020:4059 (*Uniface/PinkRoccade*), r.o. 4.5.
[33] Hof Amsterdam 16 februari 2021, ECLI:NL:GHAMS:2021:508, m.nt. N.M. Brouwer, *JOR* 2021/197.
[34] Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124, *Computerrecht* 2020/225, m.nt. C.A.M. van de Bunt (*O'Cliance*).
[35] Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731, *NJF* 2023/295.
[36] Rb. Overijssel 10-05-2023, ECLI:NL:RBOVE:2023:1731, *NJF* 2023/295.
[37] N.M. Brouwer, annotatie bij hof Amsterdam 14 april 2020, ECLI:NL:GHAMS:2020:1308 en 16 februari 2021, ECLI:NL:GHAMS:2021:508, *JOR* 2021, afl. 7-8.
[38] B. Nieuwesteeg e.a., 'Op naar een zorgplichtstandaard voor cybersecurity', Nationaal Cyber Security Lab, Labsessie #1, Position paper 23 april 2021; B. Nieuwesteeg e.a. 'Contractuele aansprakelijkheid voor digitale onveiligheid in B2B-relaties, *AV&S* 2020/22, p. 129-135.
[39] D.A. Korteweg, 'Cybersecurity: overzicht huidig regelgevend kader', *Bb* 2015/52, p. 182.
[40] P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2018/160, p. 194.

doorgaans gebaseerd op het bekende *Kelderluik*-arrest.[41] Uit dit arrest volgt dat iemand onrechtmatig kan handelen indien hij voorziet dat een ander een reële kans heeft om schade te leiden, welke kans door eenvoudig optreden kan worden voorkomen, en die persoon nalaat om die handelingen te treffen.[42] Te denken valt aan de situatie waarin de IT-leverancier nalaat om een risicovolle situatie op te heffen of hierover te waarschuwen.

Het bovenstaande laat onverlet dat de rechter het eigen handelen van de klant als opdrachtgever in zijn oordeel meeweegt, ook al is er sprake van een (bijzondere) zorgplicht van de ICT-leverancier.[43] 'Slecht' opdrachtgeverschap kan er zelfs toe leiden dat de zorgplichtschending van de ICT-leverancier niet wordt aangenomen.[44] Bovendien kan het niet tijdig aangeven van de gebrekkige dienstverlening door de klant een schending van de klachtplicht opleveren (art. 6:89 BW). In dat geval heeft de klant zijn recht verwerkt om de leverancier nog op de gebrekkige prestatie aan te spreken.

## 5. Meer informatie

In deze bijdrage is beoogd inzicht te geven in de problematiek rondom de causaliteit, de schade en de mogelijkheid van regres op de IT-leverancier door de onderneming. In onze volgende bijdrage zal aandacht worden besteed aan de mogelijkheid tot het verzekeren van aansprakelijkheidsrisico's onder de cyberverzekering.

[41] P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2021/207, p. 406. HR 5 november 1965, ECLI:NL:PHR:1965:AB7079, m.nt. G.J. Scholten (*Coca Cola/Duchateau (Kelderluik)*).
[42] P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2018/160, p. 195.
[43] Vgl. de uitspraak zoals genoemd in par. 3.6: Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731, *NJF* 2023/295.
[44] P.G. van der Putt & C.A.M. van de Bunt, 'Update Nederlandse zorgplicht-jurisprudentie', *Computerrecht* 2021/207, p. 406 e.v.