Cybercriminaliteit: aansprakelijkheid (I)

Cyber vormt één van de grootste risico's waarmee overheden, ondernemingen en burgers anno 2022 worden geconfronteerd. Cyber leidt niet alleen tot bijvoorbeeld operationele en privacy risico's, maar ook tot aansprakelijkheidsrisco's. In deze derde bijdrage worden deze aansprakelijkheidsrisico's verkend. Kunnen ondernemingen die worden getroffen door een cyberincident aansprakelijk zijn voor de schade die hieruit voortvloeit? Denk hierbij aan aansprakelijkheden die uit wet voortvloeien (zoals onrechtmatige daad), maar ook aan contractuele aansprakelijkheden. Daarnaast gaan Robert Pessers en Annevi Etienne in dit deel in op de rol van bestuurders en commissarissen. In een dit najaar te verschijnen vervolg zal ook worden ingegaan op andere aspecten, zoals onder meer causaliteit en schade.

1. Inleiding

Met de komst van de coronaepidemie en het daaraan verbonden thuiswerken, is een online bedrijfsvoering niet meer weg te denken. Tegelijkertijd brengt de afhankelijkheid van IT ook nieuwe risico's met zich mee. Zoals in eerdere bijdragen uiteengezet, vormt cyber inmiddels één van de grootste risico's waarmee overheden, ondernemingen en burgers worden geconfronteerd.[1] De omvang en ernst van cyberrisico's zijn het afgelopen jaar opnieuw sterk toegenomen.[2]

Cyberincidenten kunnen op verschillende manieren worden veroorzaakt en tot niet alleen omvangrijke, maar ook verschillende soorten schade leiden. Denk hierbij aan het stilvallen van de productie door een hack, het verlies van bedrijfsinformatie door diefstal of de enorme boetes door privacyschendingen. Die schade kan bij een organisatie zelf ontstaan, maar ook bij klanten, leveranciers en derden, hetgeen tot schadeclaims jegens de organisatie kan leiden.[3] Denk bijvoorbeeld aan de cyberaanval op de VDL Groep, die in een eerder artikel reeds werd aangehaald.[4] Als reactie op de cyberaanval besloot de VDL Groep alle IT-systemen te ontkoppelen en zich van de buitenwereld te isoleren.[5] Als gevolg hiervan viel de VDL Groep min of meer stil en konden de VDL-ondernemingen niet meer aan hun leveringsverplichtingen voldoen.

In deze bijdrage wordt beoogd enig inzicht te geven in de mogelijke aansprakelijkheden van ondernemingen, bestuurders en commissarissen indien zij worden geconfronteerd met een cyberincident. In onze eerst volgende bijdrage zal worden ingegaan op causaliteit, schade en regresmogelijkheden.

Zoals hierna zal blijken, is veelal sprake van open normen en bestaat er nog betrekkelijk weinig rechtspraak en literatuur waarin daaraan concrete invulling wordt gegeven. Cyber is ook in het recht in ontwikkeling. Vandaar dat dit een eerste verkenning is, die wij in de komende jaren regelmatig zullen aanvullen op basis van de ontwikkelingen.

2. Aansprakelijkheid onderneming voor cyberrisico's

Zoals we eerder hebben toegelicht, zijn cyberincidenten veelal terug te voeren op een van de volgende oorzaken: (i) moedwillig handelen van buitenaf door bijvoorbeeld hackers, (ii) een menselijke fout en (iii) technisch falen.[6] In het geval dat een dergelijk incident zich voordoet, kunnen de volgende vragen aan de orde komen:

- Is een onderneming die als gevolg van een dergelijk cyberincident niet aan haar contractuele verplichtingen kan voldoen in beginsel aansprakelijk uit hoofde van overeenkomst?

- Is een onderneming die getroffen wordt door een cyberincident tevens mogelijk aansprakelijk uit onrechtmatige daad?

2.1 Aansprakelijkheid o.g.v. 'wanprestatie' ex art. 6:74 BW

De eerste vraag is of een niet-nakoming van een overeenkomst door een cyberincident een toerekenbare tekortkoming in de nakoming ('wanprestatie') oplevert. Allereerst zullen we de situatie in kaart brengen waarbij hierover in de overeenkomst niets is geregeld. Op de mogelijkheden om dat wel te doen, zullen we daarna in gaan.

---

[1] https://www.vantraa.nl/nl/kennis/cybercriminaliteit-2022/; https://www.vantraa.nl/nl/kennis/cybercriminaleit-regelgeving/.
[2] OVV, *Kwetsbaarheid door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix, 16 december 2021*, Den Haag: OVV. Te raadplegen op https://www.rijksoverheid.nl/documenten/rapporten/2021/12/16/tk-bijlage-ovv-rapport-kwetsbaar-door-software-lessen-naar-aanleiding-van-beveiligingslekken-door-software-van-citrix.
[3] W.T.C. Weterings, 'Persoonlijke aansprakelijkheid bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, afl. 6.
[4] https://www.vantraa.nl/nl/kennis/cybercriminaleit-regelgeving/.
[5] 'VDL Groep weer in bedrijf na cyberaanval', vdlgroep.com.
[6] https://www.vantraa.nl/nl/kennis/cybercriminaliteit-2022/.

Toerekenbare tekortkoming

Op grond van art. 6:74 BW is de schuldenaar verplicht om de schade die de schuldeiser lijdt door iedere tekortkoming in de nakoming van een verbintenis te vergoeden, tenzij de tekortkoming de schuldenaar niet kan worden toegerekend. Een tekortkoming is niet toerekenbaar in geval van overmacht, dat wil zeggen "indien zij niet te wijten is aan zijn schuld, noch krachtens de wet, rechtshandeling of in het verkeer geldende opvattingen voor zijn rekening komt".

Wanneer een cyberincident door een fout van een medewerker is veroorzaakt, dan is in beginsel geen sprake van overmacht. Wanneer de fout echter gemaakt is door een hulppersoon, dan kan dat anders liggen. Art. 6:76 BW bepaalt immers dat een schuldenaar voor hulppersonen op gelijke wijze als voor eigen gedragingen aansprakelijk is als hij daarvan "bij de uitvoering van een verbintenis" gebruik maakt. In het *Geldnet/Kwantum*-arrest heeft de Hoge Raad dit criterium eng uitgelegd. Deze bepaling is alleen van toepassing "voor personen van wie de hulp wordt gebruikt bij de uitvoering van de verbintenis ten aanzien waarvan de aansprakelijkheid in het geding is".[7]

Het betrof in *Geldnet/Kwantum* een gewapende overval die was gepleegd met hulp van een medewerker, een geldtransporteur die op de avond van de overval ook aan het werk was bij Geldnet maar niet bij het betrokken transport. Volgens de Hoge Raad was hij niet aan te merken als een hulppersoon in de zin van art. 6:76 BW. Gelet hierop ligt het voor de hand dat hetzelfde geldt voor de medewerker van een IT-leverancier, die voor een klant algemene IT-werkzaamheden verricht en daarbij een fout maakt die een cyberincident tot gevolg heeft. In een dergelijk geval is aansprakelijkheid op grond van art. 6:76 BW dus niet aannemelijk. Dit betekent echter nog niet dat de tekortkoming richting de klant van de getroffen onderneming per definitie niet-toerekenbaar is. Dat hangt van de overige omstandigheden van het geval af.

Illustratief in dit verband is de Citrix-casus waarover de Onderzoeksraad voor Veiligheid (OVV) in 2021 rapporteerde.[8] Het Citrix-programma werd door vele overheidsinstanties gebruikt. Eind 2019 bleek dat het systeem niet (meer) waterdicht was. In verband daarmee werd dringend geadviseerd de Citrix-servers uit te zetten. Verschillende overheidsinstanties kozen er echter om hen moverende redenen voor om dat niet te doen. Voorbeeld daarvan is het Ministerie van Economische Zaken, dat meende tijdig voldoende maatregelen te hebben genomen.[9] Wanneer een dergelijke inschatting wordt gemaakt en die onjuist blijkt te zijn of een veiligheidswaarschuwing niet met gepaste spoed wordt opgepakt, is een beroep op overmacht niet aan de orde wanneer het cyberincident daarop is terug te voeren. Overmacht kan daarentegen wel aan de orde zijn wanneer bijvoorbeeld een onderneming slachtoffer van een DDoS-aanval wordt, waardoor de systemen overbelast raken.

Een andere vraag die in dit verband aan de orde is, is in hoeverre een beroep op art. 6:77 BW kan worden gedaan. Dit artikel bepaalt dat indien een tekortkoming veroorzaakt wordt door een bij de uitvoering van de verbintenis gebruikte zaak die daartoe ongeschikt is, de tekortkoming als regel aan de schuldenaar kan worden toegerekend. Dit artikel roept tenminste twee vragen op, namelijk enerzijds of software een "zaak" is in de zin van dit artikel en anderzijds of die bij de uitvoering van de verbintenis wordt gebruikt. Wat dat laatste betreft is de vraag of de Hoge Raad zal opteren voor een even stringente uitleg als hiervoor toegelicht ten aanzien van art. 6:76 BW in *Geldnet/Kwantum*-arrest.

> *Als dat het geval is, dan zou een onderneming tekortschieten in de nakoming van een verbintenis indien zij bij de uitvoering ervan gebruik maakt van IT-systemen die voor de toepassing ervan ongeschikt zijn.*

Voor wat betreft de eerste vraag, bestaat discussie of software als een 'zaak' in de zin van art. 3:2 BW kan worden aangemerkt. Onder 'zaak' wordt verstaan een voor menselijke beheersing vatbaar stoffelijk object (art. 3:2 BW). Software is dat strikt genomen niet. Uit de Parlementaire Geschiedenis blijkt bijvoorbeeld ook dat energie niet als zaak kan worden gekwalificeerd.[10] De Hoge Raad heeft echter geoordeeld dat het wenselijk is

[7] HR 14 juni 2002, *NJ* 2002/495, r.o. 3.4.
[8] OVV, *Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix, 16 december 2021*, Den Haag; OVV. Te raadplegen op https://www.rijksoverheid.nl/documenten/rapporten/2021/12/16/tk-bijlage-ovv-rapport-kwetsbaar-door-software-lessen-naar-aanleiding-van-beveiligingslekken-door-software-van-citrix.
[9] OVV, *Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix, 16 december 2021*, p. 55.
[10] Parl. Gesch. Boek 3, p. 64-65.

dat de aanschaf van software onder de titel koop valt en daarmee als een zaak moet worden gekwalificeerd. Onder ander Advocaat-Generaal Wuisman is ook die mening toegedaan.[11] Op basis hiervan kan verdedigd worden dat een beroep op art. 6:77 BW mogelijk is. Als dat het geval is, dan zou een onderneming tekortschieten in de nakoming van een verbintenis indien zij bij de uitvoering ervan gebruik maakt van IT-systemen die voor de toepassing ervan ongeschikt zijn. Denk daarbij aan een onderneming die gebruik maakt van een niet deugdelijk beveiligd programma om informatie te delen.

Uit het voorgaande volgt dat contractuele aansprakelijkheden goed denkbaar zijn. Het is daarom verstandig een specifieke regeling ten aanzien van Cyber in overeenkomsten op te nemen. Hierop gaan wij hierna nader in voor zover het zakelijke relaties (B2B) betreft.

Cyber bepalingen

Het is mogelijk om op verschillende manieren de uit overeenkomsten voortvloeiende 'exposure' die cyberrisico's met zich brengen, te managen. Allereerst kan daarbij gedacht worden aan de omschrijving van de verplichtingen van een partij, waardoor de op de betrokken onderneming rustende verplichtingen en zorgplichten behapbaar gemaakt kunnen worden. Tevens kan worden gedacht aan het opnemen van een contractuele definitie van overmacht die ruimer is dan de wettelijke. Ten slotte kan een contractuele aansprakelijkheidsregeling uitkomst bieden.

Vanzelfsprekend kan met een dergelijke contractuele regeling niet per definitie aansprakelijkheid buiten de deur worden gehouden. Een beding waarbij het belang van de ene partij verregaand wordt opgeofferd aan dat van de andere partij, kan nietig zijn wegens strijd met de goede zeden of vernietigbaar wegens misbruik van omstandigheden. Een gebalanceerde regeling is daarom verstandiger dan een totaal eenzijdige.

Daarnaast is het mogelijk dat het beding weliswaar toelaatbaar is, maar dat het inroepen daarvan naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is.[12] Juist om die reden blijft het van belang dat iedere onderneming cybermaatregelen neemt en deze maatregelen periodiek tegen het licht houdt en waar nodig bijstelt. Een onderneming die bijvoorbeeld bewust gebruik maakt van sterk verouderde software en geen maatregelen neemt om haar computers en netwerken te beveiligen, kan zich waarschijnlijk niet beroepen op een clausule die aansprakelijkheid uitsluit of beperkt als het gebrek aan beveiliging tot schade leidt.[13]

Aansprakelijkheid voor eigen opzettelijk handelen van de (bestuurders van) de onderneming of dat van ondergeschikten, kan in elk geval niet worden beperkt of uitgesloten. Of aansprakelijkheid voor grove schuld of bewuste roekeloosheid van (bestuurders van) de onderneming kan worden uitgesloten is onduidelijk. De rechtspraak biedt daarover geen uitsluitstel en in de literatuur bestaat daarover verschil van mening.[14] Aansprakelijkheid voor grove schuld of bewuste roekeloosheid van medewerkers kan wel worden uitgesloten en beperkt.[15]

Een onderneming die bewust gebruik maakt van sterk verouderde software en geen maatregelen neemt om haar computers en netwerken te beveiligen, kan zich waarschijnlijk niet beroepen op een clausule die aansprakelijkheid uitsluit of beperkt als het gebrek aan beveiliging tot schade leidt.

2.2 Aansprakelijkheid o.g.v. 'onrechtmatige daad' ex art. 6:162 BW

Vanzelfsprekend kan een onderneming ook uit onrechtmatige daad worden aangesproken.

Onrechtmatigheid

Niet elke gedraging die schade veroorzaakt, levert een onrechtmatige daad op. Hiervoor dient voldaan te zijn aan een vijftal vereisten, die in art. 6:162 en 6:163 BW worden omschreven. We richten ons in deze bijdrage met name op het vereiste dat een gedraging of nalaten onrechtmatig dient te zijn. Er bestaan drie onrechtmatigheidscategorieën: onrechtmatigheid kan worden gebaseerd op (i) een

[11] HR 27 april 2012, *NJ* 2012/293, par. 3.8; HR 27 april 2012, *NJ* 2012/294; Zie voor een uiteenzetting van de literatuur: B.J. Broekema-Engelen, '(Tekortkoming ten gevolge van) gebruik van een zaak', in: R.J.Q. Klomp & H.N. Schelhaas (red.), *Groene Serie Verbintenissenrecht*, Deventer: Wolters Kluwer.
[12] Asser/Sieburgh 6-I 2020/364.
[13] P.T.J. Wolters & C.J.H. Jansen, *Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity*, Den Haag: Cyber Security Raad 2017, p. 13.
[14] Asser/Sieburgh 6-I 2020/365.
[15] Zie bijvoorbeeld HR 26 maart 1920, *NJ* 1920, 476. Zie ook Handboek Personenschade 2080.3.1 Algemeen.

inbreuk op een recht, (ii) een doen of nalaten in strijd met een wettelijke plicht en (iii) een doen of nalaten in strijd met het ongeschreven recht.

De eerste onrechtmatigheidscategorie betreft de 'inbreuk op een recht'. In het algemeen wordt aangenomen dat het bij een rechtsinbreuk gaat om een inbreuk op een subjectief recht. Dit wordt doorgaans onderscheiden in absolute rechten en zakelijke rechten. Het gaat enerzijds om persoonlijkheidsrechten, zoals het recht op lichamelijke integriteit, privéleven en het recht op privacy, en anderzijds om zakelijke vermogensrechten, zoals het eigendomsrecht en intellectuele eigendomsrechten. Indien bij een cyberincident persoonsgegevens openbaar worden gemaakt, dan levert dat een inbreuk op de privacy van de betrokkenen op en is dus de onrechtmatigheid gegeven. In een B2B-relatie kan bijvoorbeeld sprake zijn van inbreuk op (intellectuele) eigendomsrechten wanneer aldus bijvoorbeeld bedrijfsgeheimen openbaar worden.

De tweede onrechtmatigheidscategorie ziet op "een doen of nalaten in strijd met een wettelijke plicht". Onder wettelijke normen vallen alle denkbare wettelijke bepalingen, zowel internationaal, nationaal als lokaal. In geval van een cyberincident kunnen deze wettelijke normen variëren van een bepaling in Europese regelgeving (NIB-richtlijn en Cybersecurity Act) tot een bepaling in een wet in formele zin (Wbni).[16] Zoals toegelicht in een van onze eerdere artikelen, geldt bijvoorbeeld volgens art. 7 van de Wbni voor 'aanbieders van een essentiële dienst' en 'andere aangewezen vitale aanbieders' een zorg- en een meldplicht. Deze zorgplicht houdt in dat de aanbieders "passende en evenredige technische en organisatorische maatregelen" moeten nemen om hun ICT-systemen te beheersen en de gevolgen van incidenten te verkleinen. Daarnaast houdt de meldplicht in dat de aanbieders verplicht zijn om alle incidenten met aanzienlijke gevolgen onverwijld te melden bij Agentschap Telecom en bij een Computer Security incident Response Team. Met het overtreden van een dergelijke wettelijke norm is de onrechtmatigheid in beginsel gegeven, aldus art. 6:162 lid 2 BW.

De hiervoor aangehaalde meldplicht die in art. 7 van de Wbni is neergelegd, is betrekkelijk concreet. Dat geldt echter niet voor de daarin eveneens neergelegde zorgplicht. Deze is niet verder ingevuld. De invulling moet van geval tot geval geschieden en regelmatig worden geactualiseerd. In geval van cyberincidenten zal achteraf bepaald moeten worden of de betrokken onderneming aan deze zorgplicht heeft voldaan. De tijd zal leren of dat tot jurisprudentie zal leiden die een zodanige invulling geeft aan deze zorgplicht dat daaruit een aantal algemene lessen getrokken kunnen worden. Op dit moment is dat niet het geval.

Daar komt bij dat het relativiteitsvereiste bij de categorie 'strijd met de wettelijke plicht' een belangrijke rol speelt. De enkele schending van een wettelijke norm is immers niet voldoende voor aansprakelijkheid op grond van art. 6:162 BW. Blijkens art. 6:163 BW is ook vereist dat de geschonden norm 'strekt tot bescherming tegen de schade zoals de benadeelde die heeft geleden.' In de parlementaire geschiedenis is uitgelegd dat de relativiteit betrekking heeft op drie aspecten: (a) de norm moet de benadeelde beschermen, (b) hij moet beschermen tegen de aard van de geleden schade en (c) hij moet beschermen tegen de manier waarop schade is ontstaan.[17]

Duwbak Linda illustreert deze drie aspecten in één arrest.[18] Een duwbak genaamd Linda zonk in een grindgat in de Maas en beschadigde daardoor andere vaartuigen waaraan de duwbak was vastgelegd.[19] Vaststond dat de Staat onzorgvuldig was geweest toen het de Linda een jaar daarvoor had goedgekeurd, maar had de Staat daarmee ook onrechtmatig gehandeld jegens de eigenaar van een ander vaartuig? De Hoge Raad overwoog dat het door de Staat geschonden Reglement niet strekte tot bescherming van andere vaartuigen, maar de veiligheid van het scheepvaartverkeer in algemene zin beoogde te bevorderen. Nu het Reglement niet zag op bescherming van de belangen van de eigenaar van een ander vaartuig, was geen sprake van een onrechtmatige daad jegens de eigenaren van andere vaartuigen.

De vraag is of bij de hiervoor aangehaalde Cyberregelgeving voldaan is aan het relativiteitsvereiste. Dat zal de komende tijd moeten blijken. Daarbij is van belang dat deze regelgeving ook in ontwikkeling is. De reikwijdte daarvan kan zich dus ook ontwikkelen.

De derde onrechtmatigheidscategorie is 'strijd met het ongeschreven recht'. In dit kader kan bijvoorbeeld de vraag worden gesteld of het gebruik maken van een bepaald ICT-systeem onder omstandigheden kwalificeert als een gedraging die

[16] Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen), Stb. 2018, 387. Te raadplegen op https://wetten.overheid.nl/BWBR0041515/2021-08-01.

[17] Parl. Gesch. Boek 6, p. 637.
[18] HR 7 mei 2004, *NJ* 2006/281, m.nt. J. Hijma (*Duwbak Linda*); zie bijvoorbeeld ook HR 13 april 2007, *NJ* 2008/576, m.nt. J.B.M. Vranken (*Iraanse vluchtelinge*) of HR 10 november 2006, *NJ* 2008/491, m.nt. J.B.M. Vranken (*Astrazeneca c.a./Menzis*).
[19] C. van Dam, *Aansprakelijkheidsrecht*, Den Haag: Boom juridisch 2020, p. 231 e.v.

in strijd is met de maatschappelijke betamelijkheid. Denk bijvoorbeeld aan het eerder genoemde Citrix systeem. Goed verdedigd zou kunnen worden dat het gebruik blijven maken van dit systeem zonder de benodigde patches uit te voeren en/of andere adequate maatregelen te treffen, in strijd is met de maatschappelijke betamelijkheid en dus onrechtmatig is. Hierbij zou aansluiting gezocht kunnen worden bij het leerstuk van de gevaarzetting.

In het Kelderluik-arrest heeft de Hoge Raad een aantal criteria geformuleerd aan de hand waarvan kan worden beoordeeld of een bepaalde gevaarzettende situatie als onrechtmatig dient te worden aangemerkt.[20] De criteria luiden als volgt: (i) de waarschijnlijkheid van onoplettend of onvoorzichtig gedrag van de potentiele slachtoffers, (ii) de kans dat daardoor ongevallen ontstaan, (iii) de ernst van de mogelijke gevolgen van zulke ongevallen en (iv) de bezwaarlijkheid van te nemen veiligheidsmaatregelen. Wij kunnen ons voorstellen dat hierbij de focus vaak zal liggen op de bezwaarlijkheid van het nemen van voorzorgsmaatregelen (o.a. alternatieven). Neem het eerdergenoemde voorbeeld ten aanzien van Citrix-servers. Het Ministerie van Economische Zaken meende dat zij niet anders kon handelen. Anders zou dit er volgens het Ministerie toe hebben geleid dat de NVWA geen inspecties en de douane geen controles meer uit had kunnen voeren, waardoor onder meer de vleesproductie en –handel stil zou komen te liggen. Dat is een zwaarwegend belang dat vermoedelijk het nemen van serieuze risico's rechtvaardigt. Dat zal mogelijk echter niet in alle gevallen zo zijn geweest, zodat voor andere instanties die geen maatregelen hebben genomen zeer wel een andere uitkomst denkbaar is.

Naast de Kelderluik-criteria kunnen ook wettelijke bepalingen van belang zijn bij de invulling van de maatschappelijke betamelijkheid. Dit is mogelijk door 'reflexwerking'. Reflexwerking houdt in dat de rechter bij invulling van de maatschappelijke betamelijkheid inhoudelijke inspiratie put uit een bepaling die strikt genomen niet (of nog niet) van toepassing is.[21] Dit betekent dat naast de bestaande wetgeving, ook de komende wetgeving (o.a. NIB 2-richtlijn) hierbij van betekenis zou kunnen zijn.

[20] HR 5 november 1965, *NJ* 1966/136 (*Kelderluik*); Zie voor uiteenzetting van de verschillende factoren: C. van Dam, *Aansprakelijkheidsrecht*, Den Haag: Boom juridisch 2020, p. 207 e.v.
[21] Zie bijvoorbeeld: Rb. 's Hertogenbosch 10 juni 2014, ECLI:NL:GHSHE:2014:1734, *JA* 2015/164; Rb. Amsterdam 30 september 2009, *JA* 2010/36, LJN BK0988.

Risicoaansprakelijkheid voor gebrekkige zaak

Voorts kan in dit verband van belang zijn of de onderneming aansprakelijk kan worden gehouden voor het gebruik van gebrekkige IT-systemen. Op grond van art. 6:173 BW is de *bezitter* van een roerende zaak risicoaansprakelijk als deze gebrekkig is. In geval van bedrijfsmatig gebruik van een zaak kan sprake zijn van een 'verlegging' van de aansprakelijkheid naar de bedrijfsmatige gebruiker.[22]

De eerste vraag die in dit verband rijst is of software kwalificeert als een (gebrekkige) roerende zaak. Zoals hiervoor toegelicht, is dat verdedigbaar ondanks dat niet aan de wettelijke omschrijving van het begrip 'zaak' is voldaan.

Als deze horde wordt genomen, volgt de volgende, namelijk het vereiste dat de roerende zaak gebrekkig moet zijn. Een zaak is pas gebrekkig als deze niet voldoet aan de eisen die men hieraan in de gegeven omstandigheden mag stellen.[23] Dit wordt veelal aangeduid als het 'gebrekscriterium' en het gaat daarbij om de eisen die men uit het oogpunt van veiligheid aan de desbetreffende roerende zaak mag stellen. Daarbij spelen zowel gedragsnormen als veiligheidsvoorschriften en in het algemeen aan de bezitter of bedrijfsmatig gebruiker te stellen zorgvuldigheidsnormen een belangrijke rol.[24]

Gelet op de snelheid waarmee de wereldwijde digitalisering verloopt en de daarmee verbonden toenemende risico's op het gebied van cyber, wordt verdedigd dat van ondernemingen een hoge mate van cybersecurity mag worden verwacht.[25] Daar komt bij dat het bedrijfsmatig gebruik van een roerende zaak kan meebrengen dat nog hogere veiligheidseisen aan de zaak mogen worden gesteld.[26] Tegen deze achtergrond is dus mogelijk dat een beroep kan worden gedaan op art. 6:173 BW wanneer bijvoorbeeld een onderneming niet adequaat reageert op veiligheidswaarschuwingen van de producent van de software waarvan zij

[22] HR 1 april 2011, *NJ* 2011/405 (*Loretta*); A. Kolder, 'Kwalitatieve aansprakelijkheid voor gebrekkige zaken, gevaarlijke stoffen en dieren: het bedrijfsbegrip van art. 6:181 BW', *AV&S* 2019/17.
[23] Voor aansprakelijkheid op grond van art. 6:173 BW is voorts vereist dat (i) sprake is van een bijzonder gevaar en (ii) bekend moet zijn dat het gebrek een gevaar voor personen of zaken oplevert.
[24] Parl. Gesch. Boek 6 (Inv. Boek 3,5 en 6), p. 1380; zie ook HR 17 december 2010, *NJ* 2012/155, m.nt. T. Hartlief (*Wilnis*); C. van Dam, *Aansprakelijkheidsrecht*, Den Haag: Boom juridisch 2020, p. 630 e.v.
[25] Zie hiervoor onder meer P.T.J. Wolters & C.J.H. Jansen, *Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity*, Den Haag: Cyber Security Raad 2017.
[26] T.E. van der Linden, 'De invloed van bedrijfsmatig gebruik op het gebrekscriterium', *NTBR* 2020/39, afl. 9.

gebruik maakt of niet met de nodige voortvarendheid patches uitvoert.

Daarbij is van belang dat de onderneming zich in dat geval niet kan verschuilen achter de oorzaak van het gebrek. Zelfs als de zaak door een derde (zoals een hacker) is gesaboteerd, blijft de bezitter of bedrijfsmatig gebruiker wanneer dit artikel van toepassing is (risico)aansprakelijk.

3. Aansprakelijkheid bestuurders en commissarissen voor cyberrisico's

Naast de organisatie kunnen ook de bestuurders en commissarissen geconfronteerd worden met de gevolgen van een cyberincident. Zo zijn in de Verenigde Staten in 2016 de eerste bestuurders persoonlijk aansprakelijk gesteld voor de gevolgen van "the second biggest data breach in retail history".[27] Dat de verplichtingen op het gebied van digitale veiligheid een verzwaring van de taak van bestuurders en commissarissen meebrengt, volgde reeds uit de in 2017 verschenen handreiking "Cyber security-guide for boardroom members" die door de Cyber Security Raad is uitgebracht.[28]

Het bestuur is belast met het bepalen van het beleid en de strategie van de vennootschap. In het verlengde daarvan ligt de verantwoordelijkheid voor het opstellen van een beleid inzake de risico's en het systeem ter beheersing en controle van deze risico's. Een effectieve aanpak van cyberrisico's binnen het bedrijf behoort daarmee tot de taak van bestuurders. Hoewel zij zelf geen IT-specialisten behoeven te worden, zijn zij wel gehouden om direct betrokken te zijn bij het adresseren en aanpakken van cyberrisico's en hierop toezicht te houden. Een behoorlijke taakvervulling brengt immers met zich dat het bestuur het beleid ter zake van cyberveiligheid – gelet op de snelle ontwikkelingen op digitaal gebied – regelmatig monitort en aanscherpt. Het is vervolgens aan de raad van commissarissen om toezicht te houden op het beleid van het bestuur en het bestuur hierover te adviseren.[29] Meer dan ooit moet een commissaris zich (pro)actief opstellen en het bestuur bevragen over het cybersecuritybeleid.

Daarmee kan op het moment dat een cyberrisico zich verwezenlijkt de vraag worden gesteld wat de rol van het bestuur en commissarissen is geweest met betrekking tot de beheersing van cyberrisico's.[30] Was de onderneming voldoende voorbereid op een cyberincident? Waren de juiste standaarden voor beveiliging binnen de onderneming ingevoerd? Hebben de bestuurders en commissarissen voldoende verantwoordelijkheid genomen voor de wijze waarop het bedrijf cyberrisico's benadert? Bij een tekortschieten daarvan kan het zijn dat de bestuurders en de commissarissen hun taak onbehoorlijk hebben vervuld en hen een (persoonlijk) ernstig verwijt kan worden gemaakt vanwege onvoldoende cybersecurity.

Vooralsnog zijn er geen gevallen bekend van bestuurdersaansprakelijkheid voor digitale onveiligheid in B2B-relaties. Het lijkt echter een kwestie van tijd dat hierin verandering komt.

4. Meer informatie en contact

In deze bijdrage is beoogd inzicht te geven in de positie van ondernemingen, bestuurders en commissarissen indien de cybersecurity van de door hen aangeschafte ICT-toepassingen tekortschiet.

In onze volgende bijdrage zal aandacht worden besteed aan de problematiek rondom de causaliteit, de schade en de mogelijkheid van regres op de IT-leverancier door de onderneming.

Wilt u meer weten over cyber, dan kunt u contact opnemen met Robert Pessers of Annevi Etienne.

Robert Pessers
pessers@vantraa.nl
+31 6 50 51 26 62
+31 10 22 45 502

Annevi Etienne
etienne@vantraa.nl
+31 6 82 06 69 96
+31 10 22 45 520

[27] W.C.T. Weterings, 'Persoonlijke aansprakelijkheid van bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, afl. 6; C.D.J. Bulten, B.P.F. Jacobs & C.J.H. Jansen, 'Cybersecurity: Chefsache?!', *Ondernemingsrecht* 2021/79, afl. 12.
[28] CSR, *Cybersecurity-guide for boardroom members*, Den Haag 2019. Te raadplegen op: https://www.cybersecuritycouncil.nl/documents/cybersecurity-guides/2019/10/01/cybersecurity-guide_boardroom-members.
[29] C. Bulten & C. Jansen, 'De taak van de commissaris in een digitale wereld: de noodzaak van awareness van cyber security', *Ondernemingsrecht* 2016/74, afl. 9.
[30] W.C.T. Weterings, 'Persoonlijke aansprakelijkheid van bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, afl. 6; C. Bulten & C. Jansen, 'De taak van de commissaris in een digitale wereld: de noodzaak van awareness van cyber security', *Ondernemingsrecht* 2016/74, afl. 9, p. 358.