Contractuele aansprakelijkheid voor digitale onveiligheid in B2B relaties[1]

Mr.dr.ir. B.F.H. Nieuwesteeg,[2] prof.mr.dr. L.T. Visscher,[3] prof.dr. M.G. Faure[4] en mr. N. Brouwer[5]

1 Inleiding

Als een organisatie in een business to businessrelatie (hierna B2B-relatie) schade lijdt door digitale onveiligheid, dan rijst de vraag in hoeverre het aansprakelijkheidsrecht mogelijkheden biedt om deze schade op een ander te verhalen. In deze bijdrage betogen wij dat die mogelijkheden zeer beperkt zijn vanwege het bestaan van diverse juridische barrières (de zorgplicht, het vaststellen van de schade, de causaliteit en de bewijslast) en economische barrières (onderhandelingsmacht, toegang tot de rechter en faillissement van de leverancier). Op andere terreinen kunnen deze weliswaar eveneens een rol spelen, maar bij digitale onveiligheid resulteert de combinatie van barrières erin dat verhaal in verreweg de meeste gevallen niet loont. Het mes van het aansprakelijkheidsrecht is dus bot.

Er worden talloze contracten afgesloten tussen afnemers en leveranciers van producten en diensten die een cybersecuritycomponent hebben. Er kunnen minstens vier verschillende partijen bij digitale onveiligheid betrokken zijn: A: de leverancier van producten of diensten met een cybersecuritycomponent; B: de afnemer van die producten of diensten die schade kan lijden; C: een derde die schade kan lijden en D: een derde die intentioneel schade heeft veroorzaakt (zoals een hacker). Onze bijdrage betreft situaties waarin afnemer B leverancier A wil aanspreken, ongeacht of de cyberonveiligheid door een hacker (D) of door A zelf wordt veroorzaakt.[6]
Onze bijdrage analyseert situaties waarin een contractuele relatie tussen partijen in een B2B-relatie bestaat. Het regime van productaansprakelijkheid is hier dus niet van toepassing, evenmin als privacy-gerelateerde aansprakelijkheid.[7] Vanwege de regels van samenloop biedt het

[1] Deze bijdrage is een verkorte en geüpdatete versie van een onderzoek dat in opdracht van het Ministerie van Economische Zaken en Klimaat is verricht. Het volledige rapport is beschikbaar via https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/24/aansprakelijkheid-voor-digitale-onveiligheid-in-b2b-relaties/CLECS+-+Aansprakelijkheid+voor+digitale+onveiligheid+in+b2b-relaties.pdf.
[2] Mr.dr.ir. B.F.H. Nieuwesteeg is directeur van het Centre for the Law and Economics of Cyber Security aan de Erasmus Universiteit Rotterdam.
[3] Prof. mr. dr. L.T. Visscher is bijzonder hoogleraar Legal Economic Analysis of Tort and Damages aan het Rotterdam Institute of Law and Economics (RILE) van de Erasmus Universiteit Rotterdam.
[4] Prof.dr. M.G. Faure is hoogleraar Comparative Private Law and Economics aan het Rotterdam Institute of Law and Economics (RILE) van de Erasmus Universiteit Rotterdam en hoogleraar Comparative and International Environmental Law aan de Universiteit Maastricht.
[5] Mr. N.M. Brouwer is advocaat bij Dirkzwager legal & tax en buitenpromovenda aan het Onderzoekcentrum voor Onderneming & Recht van de Radboud Universiteit Nijmegen.
[6] Wij gaan er van uit dat (vanwege bijvoorbeeld onvindbaarheid of insolventie) op D geen verhaal kan worden genomen.
[7] Krachtens artikel 82 van de Algemene Verordening Gegevensbescherming (Verordening 2016/679, in werking getreden op 25 mei 2018) heeft eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk

onrechtmatigedaadsrecht evenmin soelaas.[8] Bestuurdersaansprakelijkheid vereist een persoonlijk ernstig verwijt, hetgeen niet snel het geval zal zijn.[9] Er zijn, naar ons beste weten, dan ook nog geen gevallen van bestuurdersaansprakelijkheid voor digitale onveiligheid in B2B-relaties. Contractuele aansprakelijkheid voor wanprestatie is derhalve in verreweg de meeste gevallen de aangewezen route voor verhaal.

Onze bijdrage is als volgt opgebouwd. In paragraaf 2 bespreken wij de juridische barrières en in paragraaf 3 de economische. In paragraaf 4 laten wij aan de hand van enkele scenario's zien dat de combinatie van barrières verhaal via het contractuele aansprakelijkheidsrecht vrijwel altijd illusoir maakt. In paragraaf 5 doen wij enkele aanbevelingen om het geschetste probleem aan te pakken en concluderen wij.

2 Juridische barrières

2.1 Woord vooraf over contractsvrijheid

In deze paragraaf bespreken wij vier juridische barrières bij het verhalen van schade als gevolg van cyberonveiligheid en in de volgende paragraaf richten wij onze aandacht op drie economische barrières. Tezamen zorgen deze belemmeringen ervoor dat, ook als een claim in beginsel gegrond is, het zeer de vraag is of zo'n claim succesvol zal zijn. Illustratief is dat er in de jurisprudentie vrijwel geen aansprakelijkheidsclaims te vinden zijn betreffende gebrekkige cybersecurity bij die leverancier.[10]

---

op deze Verordening, het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. Het debat over de vraag of 'eenieder' in art. 82 AVG ook van toepassing is op rechtspersonen valt buiten de reikwijdte van deze bijdrage. Zie voor een uitgebreide beschouwing op dat punt T.F. Walree en P.T.J. Wolters, 'Het recht op schadevergoeding van een concurrent bij een schending van de AVG', *SEW* 2020/1, p. 2-10.

[8] Zie bijvoorbeeld C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Wolters Kluwer 2019, nr. 10. Alleen als er, onafhankelijk van de wanprestatie, een onrechtmatige daad is gepleegd die wel verband houdt met de contractuele verhouding, zou buitencontractuele aansprakelijkheid aangewezen kunnen zijn. Hierbij geldt echter dat de contractuele afspraken (ook over exoneratie) de inhoud van de buitencontractuele aansprakelijkheid beïnvloeden, zodat dezelfde beperkingen van aansprakelijkheid kunnen gelden. In de rechtspraak wordt in het algemeen aangenomen dat exoneraties zowel op contractuele als op buitencontractuele aansprakelijkheid zien, maar Sieburgh (2019), nr. 10 en 12 stelt dat ter bescherming van de benadeelde partij mag worden verwacht dat een exoneratiebeding duidelijk moet aangeven of het ook op buitencontractuele aansprakelijkheid betrekking heeft.

[9] HR 10 januari 1997, NJ 1997/360 (Staleman/Van de Ven); HR 20 juni 2008, NJ 2009/21 (Willemsen/NOM); HR 5 september 2014, ECLI:NL:HR:2014:2628 (Hezemans Air); HR 5 september 2014, ECLI:NL:HR:2014:2627 (RCI).

[10] Afgezien van het vonnis van de rechtbank Amsterdam uit 2018, dat pas begin juni 2020 is gepubliceerd (Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124) en in paragraaf 2.2 besproken wordt. Ook zijn we aanpalende zaken tegengekomen en zaken die zich op een ander terrein bevinden dan cybersecurity maar waar we wel barrières voor verhaal uit kunnen afleiden. Zo speelde in 2014 de zaak Ratonigid/Vasco (ECLI:NL:RBAMS:2014:4888). Het ging daar niet om een B2B-relatie waarin een cybersecurityproduct of -dienst wordt geleverd, maar om de verkoop van een geheel cybersecuritybedrijf, te weten DigiNotar. In deze zaak moesten de voormalige eigenaren van de Nederlandse commerciële certificaatautoriteit DigiNotar miljoenen euro's betalen aan het bedrijf VASCO Data Security International, dat in januari 2011 de aandelen DigiNotar overnam. Ratonigid (de

Partijen in een B2B-relatie hebben een grote mate van vrijheid om afspraken te maken over hoe om te gaan met risico's betreffende cyberveiligheid. De afnemer kan bijvoorbeeld proberen te bedingen dat de leverancier het risico draagt of hij kan het risico zelf dragen (en het al dan niet verzekeren) en proberen een lagere prijs overeen te komen. Door deze contractsvrijheid kunnen partijen de afspraken maken die hun voorkeuren zo goed mogelijk weergeven. Hierbij is o.a. de risicohouding van partijen relevant, maar ook hun mate van solvabiliteit, of ze voldoende informatie hebben om de risico's goed in te kunnen schatten, en of ze het risico middels verzekeringen kunnen afdekken. In de ene situatie kan het wenselijk zijn dat de leverancier de aansprakelijkheid geheel uitsluit en een lagere prijs vraag (waarna de afnemer het risico draagt of zich ertegen verzekert) terwijl het in een andere B2B-relatie beter kan zijn dat juist de leverancier het risico draagt en daar een hogere prijs voor vraagt. Contractuele risicoverdelingen (via bijvoorbeeld exoneraties) moeten dus in beginsel gerespecteerd worden, omdat ze de voorkeuren van de betrokken partijen reflecteren. Dit kan anders zijn als er bijvoorbeeld sprake is van een zodanig verschil in onderhandelingsmacht dat de sterke partij hiervan misbruik kan maken. Denk hierbij aan een situatie waarbij een leverancier met marktmacht zijn aansprakelijkheid geheel uitsluit, maar de afnemer vanwege gebrek aan concurrentie geen lagere prijs kan bedingen.

2.2 Juridische barrière 1: vage zorgplicht[11] en exoneratie van aansprakelijkheid

In een B2B-relatie worden minimumvereisten voor cybersecurity in het contract vastgelegd of volgen uit de aard van de B2B-relatie.[12] Als het gaat om de beveiliging van staatsgeheimen zal de cybersecuritynorm strenger zijn dan als het gaat om een kwetsbaarheidsscan van de plaatselijke voetbalclub. De leverende partij heeft de plicht om aan de norm te voldoen. Deze zorgplicht hangt mede af van het type aansprakelijkheid, i.c. aansprakelijkheid voor wanprestatie of bestuurdersaansprakelijkheid.

2.2.1 Zorgplicht bij toerekenbare tekortkoming (wanprestatie)

In beginsel kunnen partijen in het contract afspreken wat er ter zake van cyberveiligheid van de leverancier wordt verwacht. Enerzijds rust op de afnemer een informatieplicht (zo dient hij de

holding achter DigiNotar) had DigiNotar verkocht aan Vasco. Met de verkoop waren garantiebepalingen gemoeid, waarin specifieke veiligheidseisen waren opgenomen. Bedongen was tevens dat in geval van een schending Ratonigid aan Vasco een bedrag zou moeten betalen waardoor Vasco wederom in de positie zou komen waarin zij had verkeerd als de garantieschending niet had plaatsgevonden. Ten gevolge van de garantieschendingen heeft in de zomer van 2011 een hack kunnen plaatsvinden en deze heeft zodanige gevolgen gehad dat DigiNotar daaraan failliet is gegaan. Er is in deze zaak sprake van een heldere zorgplicht (de garantiebepaling), zeer duidelijke schade (namelijk het faillissement van DigiNotar), en een grote hoeveelheid extern onderzoek die het bewijzen van de causaliteit mogelijk maakte. Het faillissement leidde in dit geval niet tot insolventie, omdat het ging om de verkoop van DigiNotar door de bovenliggende holding.

[11] Het begrip 'zorgplicht' wordt veel gebruikt in wet- en regelgeving rondom cybersecurity. De contractuele zorgplicht moet niet verward worden met zorgplichten die voortvloeien uit wetgeving, zoals bijvoorbeeld de zorgplicht die voortvloeit uit de Algemene Verordening Gegevensbescherming.

[12] T.F.E. Tjong Tjin Tai & B.J. Koops, 'Zorgplichten tegen cybercrime', *Nederlands Juristenblad* 2015, p. 1065-1072.

leverancier correct te informeren over de aard van zijn werkzaamheden, bedrijvigheden en noden op het terrein van cyberveiligheid). Anderzijds heeft de leverancier een onderzoeksplicht en dient deze er zich dus van te vergewissen dat het door hem aangeboden beveiligingssysteem ook adequaat is, gelet op de wensen van de afnemer. Bepaalde normen kunnen contractspartijen te hulp komen om te verduidelijken wat er specifiek van de leverancier kan worden verwacht. Zo kunnen partijen bijvoorbeeld afspreken dat de leverancier zich aan bepaalde cybersecuritystandaarden moet houden zoals ISO27001 en jaarlijks een cybersecurityaudit dient te laten uitvoeren.[13] Als de leverancier zich niet aan de in het contract vastgelegde zorgplicht heeft gehouden, bijvoorbeeld doordat deze geen audit heeft laten uitvoeren, dan kan sprake zijn van een schending van een norm en dus van wanprestatie.

Belangrijk hierbij is dat cyberveiligheid (onder andere vanwege hoge kosten) doorgaans niet als een resultaatsverplichting kan worden gekwalificeerd, dus absolute cyberveiligheid kan niet worden gegarandeerd. In de praktijk rust op een leverancier een inspanningsverplichting, welke vaag geformuleerd kan zijn. Een leverancier zal liever met relatief vage en algemene inspanningsverbintenissen werken omdat de schending daarvan moeilijker is aan te tonen dan de schending van een strenge en zeer specifieke norm. De afnemer heeft juist voorkeur voor specifieke cybersecuritynormen zoals een ISO-norm, omdat schending van de zorgplicht dan eenvoudiger is aan te tonen.

In de praktijk is de zorgplicht moeilijk vast te stellen omdat er geen standaarden zijn waaraan partijen zich dienen te houden en er vrijwel geen Nederlandse jurisprudentie is.[14] Een voorbeeld uit de schaarse rechtspraak is het vonnis van de rechtbank Amsterdam uit 2018, dat pas begin juni 2020 is gepubliceerd.[15] Die zaak laat zien dat op de IT-leverancier die een totaalpakket levert ook de verplichting rust om zorg te dragen voor adequate beveiligingsmaatregelen. Die zorgplicht gaat volgens de rechtbank Amsterdam zelfs zo ver dat, zou de afnemer de voorgestelde beveiligingsmaatregelen van de hand wijzen, het op de weg van de IT-leverancier ligt om de opdracht te weigeren wegens onuitvoerbaarheid, alternatieven aan te dragen of op zijn minst indringend en herhaaldelijk te waarschuwen voor de risico's die het achterwege laten van de voorgestelde beveiligingsmaatregelen met zich brengen (r.o. 1.1). Beveiliging was dus een kernelement van de zorgplicht van deze IT-leverancier.

2.2.2 Zorgplicht bij bestuurdersaansprakelijkheid

[13] Vergelijk ook de garantiebepalingen in de Share Purchase Agreement in de zaak Ratonigid/Vasco (ECLI:NL:RBAMS:2014:4888).

[14] Zie onder andere de verplichting tot het bijwerken van onveilige software en de zaak van de consumentenbond tegen Samsung (Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175). Zie ook P. Verbruggen & P.T.J. Wolters, 'Consument en cybersecurity: Een agenda voor Europese harmonisatie van zorgplichten', *Tijdschrift voor consumentenrecht & handelspraktijken* 2017, p. 20-29. Voor consumenten ontwikkelt de discussie over de zorgplicht van partijen zich waarschijnlijk sneller dan in B2B-relaties, omdat de recente Europese Richtlijnen 2019/770 en 2019/771 de verwachtingen inkleuren die een consument van een leverancier mag hebben op het gebied van de levering van digitale goederen en diensten. De zorgplicht van de leverancier jegens de consument wordt dus verduidelijkt. Artikel 7 lid 3 van Richtlijn 2019/771 spreekt bijvoorbeeld over verplichte beveiligingsupdates voor een bepaalde periode.

[15] Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124.

Bij bestuurdersaansprakelijkheid is de barrière flink hoger,[16] omdat hiervoor aan een bestuurder van een vennootschap een persoonlijk ernstig verwijt moet kunnen worden gemaakt. Ook deze normen zijn in het geval van cybersecurity niet glashelder. Maar in de exceptionele gevallen waarin wel een ernstig persoonlijk verwijt kan worden gemaakt, zou dus sprake kunnen zijn van bestuurdersaansprakelijkheid.

2.2.3 Uitsluiting van aansprakelijkheid

Contractspartijen in een B2B-relatie hebben de vrijheid om afspraken te maken over de risicoverdeling en ze kunnen dus ook exoneratieclausules opnemen.[17] Naar onze verwachting zullen leveranciers (doorgaans via hun algemene voorwaarden) elke vorm van aansprakelijkheid trachten uit te sluiten of te beperken.[18] Een beroep op een exoneratiebeding dat op zichzelf beschouwd geldig is, kan in zeer uitzonderlijke gevallen echter vanwege de omstandigheden van het geval onredelijk bewarend of naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zijn. Relevante factoren hierbij zijn o.a. de zwaarte van de schuld maar ook de 'maatschappelijke positie en onderlinge verhouding van partijen'.[19] In B2B-relaties zal hier veel minder ruimte voor zijn dan in B2C-relaties. Naarmate een 'business' meer het karakter van een consument heeft, bijvoorbeeld een ZZP'er, heeft deze echter een grotere kans om via de reflexwerking een beroep te kunnen doen op de bescherming die geldt voor consumenten.[20]

Schade die is ontstaan door *opzet of bewuste roekeloosheid* is niet uit te sluiten, omdat zo'n beding strijdig is met de goede zeden.[21] Er is in de wetenschap en de rechtspraak grote onduidelijkheid over wat opzet of bewuste roekeloosheid inhoudt in het geval van aansprakelijkheid voor cybersecurityschade in B2B-relaties. De volgende twee voorbeelden worden aangehaald in een CSR-advies over zorgplichten:[22]

---

[16] Zie bijvoorbeeld M.W.A. Westenbroek, 'Externe bestuurdersaansprakelijkheid, rechtspersoonlijkheid en toerekening', *Ondernemingsrecht* 2016, p. 112-119.

[17] Hof Arnhem-Leeuwarden, 17 december 2013 (Staalservice Zuidbroek) [NL:GHARL:2013:9644]; zie ook o.a.: 6:233A BW; 6:248 lid 2 BW. Het ging hier om de vraag of een beding in de algemene voorwaarden onredelijk bezwarend was. Het hof ging hier niet in mee. Zie in het kader van automatiseringswerkzaamheden bijvoorbeeld ook Hof Den Haag 27 september 2016, ECLI:NL:GHDHA:2016:2690.

[18] Deze verwachting baseren wij op de constatering dat *ceteris paribus* de leverancier beter af is als hij of zij de aansprakelijkheid uitsluit. De ICT-office voorwaarden (vroeger de Fenit-voorwaarden, opgesteld door de brancheorganisatie van IT-leveranciers) zijn hiervan een goed voorbeeld. Uiteraard kan de afnemende partij in de onderhandeling trachten om de aansprakelijkheid van de leverancier niet uit te sluiten, maar dit doet niet af aan de prikkel van de leverancier om de contractsonderhandelingen te beginnen met een voorstel tot beperking en uitsluiting van de aansprakelijkheid. Zie ook Tjong Tjin Tai & Koops 2015; T.F.E. Tjong Tjin Tai, 'Zorgplichten van banken tegen DDoS-aanvallen', *Nederlands Juristenblad*.2013, p. 2196-2200; P.H. Blok (red.), 'Overeenkomsten inzake informatietechnologie', Den Haag: SDU Uitgevers 2010, p. 112, 113; T.J. de Graaf & C. Stuurman, 'ICT-contracten', in: S. van der Hof e.a. (red.), *Recht en Computer*, Deventer: Wolters Kluwer 2014, p. 79.

[19] Zie bijvoorbeeld HR 11 februari 2000, *NJ* 2000, 294; HR 20 februari 1976, *NJ* 1976, 486; HR 19 mei 1967, *NJ* 1967, 261

[20] Zie bijvoorbeeld Rb. Den Haag 28 mei 2014, ECLI:NL:RBDHA:2014:6526.

[21] Zie C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel I. De verbintenis in het algemeen, eerste gedeelte*, Deventer: Wolters Kluwer 2016, nr. 365.

[22] 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 en 22.

> ‘Door een beveiligingslek in een computerprogramma is een hacker op eenvoudige wijze in staat om de computer van de gebruiker over te nemen. De kennis van dit gebrek is wijdverbreid. De verkoper die dit product verkoopt ondanks kennis van de onveiligheid, kan zich niet beroepen op een clausule die aansprakelijkheid uitsluit. Dit geldt in het bijzonder als het beveiligingslek niet is bekend gemaakt aan de afnemer waardoor de afnemer geen schadebeperkende maatregelen heeft kunnen treffen.’

> ‘Het [bedrijf] blijft aansprakelijk als het bijvoorbeeld, met medeweten van de bedrijfsleiding, bewust (‘opzettelijk of bewust roekeloos’) gebruik maakt van ICT waarvan de cybersecurity sterk tekortschiet. Een bedrijf dat bewust gebruik maakt van sterk verouderde software en geen maatregelen neemt om zijn computers en netwerken te beveiligen, kan zich waarschijnlijk niet beroepen op een clausule die aansprakelijkheid uitsluit als het gebrek aan beveiliging tot schade leidt.’

Het eerste voorbeeld kan inderdaad een casus zijn waarin de leverancier zich niet op de exoneratie kan beroepen, maar de rechter zal moeten toetsen of, gegeven de omstandigheden van het specifieke geval, er sprake is van opzet of roekeloosheid. In het tweede voorbeeld is het o.a. de vraag wanneer een organisatie ‘bewust gebruik maakt van sterk tekortschietende ICT’.
Beide voorbeelden maken duidelijk dat in de meeste gevallen de exoneratie inderdaad tot limitering of uitsluiting van de aansprakelijkheid van de leverancier zal leiden, omdat er vaak geen sprake zal zijn van opzet of bewuste roekeloosheid. Waar de grens precies ligt, zal in de praktijk vaak moeilijk te bepalen zijn. De rechter zal van geval tot geval moeten bepalen wat opzet of bewuste roekeloosheid inhoudt,[23] maar er is niet veel jurisprudentie op dit terrein. Uitgangspunt in het Nederlandse recht blijft echter dat bedrijven in een B2B-relatie zelf kunnen onderhandelen over de mate van aansprakelijkheid die zij willen aanvaarden en dat exoneratieclausules in beginsel door de rechter worden gerespecteerd.

2.3 Juridische barrière 2: schade

In gevallen van cyberonveiligheid is de schade vaak moeilijk kwantificeerbaar, bijvoorbeeld wanneer de afnemer gedurende twee weken zijn emailsysteem niet kon gebruiken. Dit geldt temeer nu er vaak sprake zal zijn van ‘zuivere vermogensschade’, zoals gederfde inkomsten omdat de afnemer zijn bedrijf tijdelijk niet kan uitoefenen,[24] die veelal moeilijker vast te stellen is dan zaakschade of letselschade.

---

[23] Een voorbeeld waarin grove schuld werd aangenomen is de uitspraak van Rb. Overijssel 9 maart 2016, ECLI:NL:RBOVE:2016:1113 (r.o. 5.12-5.14).

[24] Vergelijk ook de zaak Ratonigid/Vasco (ECLI:NL:RBAMS:2014:4888). De schade was in deze uitzonderlijke zaak juist heel duidelijk. De rechtbank zegt: ‘Op grond van artikel 7.4 van de SPA zal Ratonigid aan Vasco alle schade moeten vergoeden die Vasco ten gevolge van de inbreuk(en) op de garantie heeft geleden, waarbij voor de definitie van schade (‘Damages’) in de SPA aansluiting wordt gezocht bij de artikelen 6:95 en 6:96 BW met de aanvulling dat in geval van een schending van de garanties, Ratonigid aan Vasco een bedrag moet betalen waardoor Vasco in de positie komt waarin zij had verkeerd als de garantieschending niet had plaatsgevonden. Aangezien als gevolg van de garantieschending(en) – waardoor de hack heeft kunnen plaatsvinden en ten gevolge waarvan DigiNotar failliet is gegaan – de aandelen in DigiNotar waardeloos zijn geworden, zal Ratonigid aan Vasco in ieder geval de (gehele) verkoopprijs voor de aandelen terug moeten betalen.’

Daarnaast kan een securitybreuk bij een afnemer ook reputatieschade veroorzaken. Hier is er vaak een groot verschil tussen werkelijke en gepercipieerde schade. Vaak is de reputatieschade niet of nauwelijks te kwantificeren.[25] Schade ten gevolge van bedrijfsonderbreking gerelateerd aan de cyberonveiligheid van de afnemende partij is wellicht gemakkelijker te kwantificeren, maar ook daar rijzen vragen ten aanzien van de precieze omvang van de schade. Als bijvoorbeeld een afnemende partij een dag niet kan leveren maar de dag daarop dubbel zoveel omzet heeft, kan een leverende partij betogen dat er geen of slechts een kleine schade is.
Materiële schade aan systemen en processen is het meest eenvoudig te kwantificeren doordat hier in algemene zin directe kosten worden gemaakt zoals bijvoorbeeld herstel van systemen en de inhuur van forensische IT-diensten zoals bijvoorbeeld bij de ransomware-aanval op Maersk in juni 2017.
Samenvattend is schade bij cyberonveiligheid vanwege deze uiteenlopende redenen vaak moeilijk te kwantificeren. De kosten en mogelijkheden van het aantonen van de schade kunnen derhalve een hoge barrière vormen.

2.4 Juridische barrière 3: causaliteit

Als, ondanks de bovenstaande problemen, schade kan worden aangetoond, dan moet nog worden bewezen dat deze schade door de cyberonveiligheid bij de leverancier is veroorzaakt. Het aantonen van dit causale verband is wellicht een van de grootste barrières voor aansprakelijkheid. 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.’[26] Daarbij komt dat de eiser moet aantonen dat hij de beveiliging van de computersystemen geheel op orde heeft omdat hij anders zelf ook een aandeel kan hebben in de door hem geleden schade.[27] Een extra complicerende factor is dat producten met een cybersecuritycomponent (voor zover deze niet onderdeel zijn van *Software as a Service*) waarschijnlijk worden onderworpen aan updates die niet noodzakelijkerwijs door de oorspronkelijke leverende partij worden verstrekt. Met het bepalen welk deel van de cyberonveiligheid in de code vanaf het begin fout was of tijdens een update werd gecreëerd, zijn

[25] F. Bisogni, H. Asghari & M.J.G. van Eeten ‘Estimating the size of the iceberg from its tip. An investigation into unreported data breach notifications’, *Proceedings of 16th Annual Workshop on the Economics of Information Security* 2017 en B.F.H. Nieuwesteeg & M.G. Faure, ‘An Analysis of the Effectiveness of the EU Data Breach Notification Law’, *Computer Law & Security Review* 2018, p. 1232-1246 geven een analyse en overzicht van het onderzoek dat is gedaan naar reputatieschade aan de hand van cybersecurityaanvallen zoals datalekken.
[26] Tjong Tjin Tai & Koops 2015. Vergelijk ook de zaak Ratonigid/Vasco, waarin door het uitvoerige onderzoek van Fox-IT en de onderzoeksraad voor de veiligheid de verhalende partij veel munitie had om causaliteit aan te tonen. Door deze (extern gefinancierde) bewijsvoering kon de rechtbank oordelen dat elk van de drie vastgestelde beveiligingsgebreken een garantieschending (i.e. schending van de norm) opleverde.
[27] Eigen schuld bij cybersecurity wordt o.a. besproken door M.L. Rustad & T.H. Koenig, ‘The Tort of Negligent Enablement of Cybercrime’, *Berkeley Technology Law Journal* 2005, p. 1553-1611.

hoge expertkosten gemoeid, maar dit is essentieel om te bepalen welk deel van de schade verhaald kan worden op de initieel leverende partij.[28]

2.5 Juridische barrière 4: bewijslast

De afnemer die schadevergoeding vordert van de leverancier, zal moeten bewijzen dat de zorgplicht is geschonden en dat die schending schade heeft veroorzaakt. In gevallen van cyberschade is dit een zeer belangrijke barrière, omdat de afnemer niet in de IT-systemen van de leverancier kan kijken. Hij kan dus niet vaststellen of de zorgplicht (die een inspanningsverplichting inhoudt en niet een resultaatsverplichting) is geschonden en of er een causaal verband is tussen de geschonden zorgplicht en de geleden schade. Bovendien kan de leverancier eenvoudig eventueel bewijs laten verdwijnen, door bijvoorbeeld logbestanden te verwijderen.[29] Hier kunnen natuurlijk wel contractuele afspraken over worden gemaakt, bijvoorbeeld het vereiste om logbestanden voor een bepaalde periode te bewaren. De *Expert Group on Liability and New Technologies – New Technologies Formation* van de Europese Commissie stelt daarom op basis van verschillende Europese uitspraken uit verschillende jurisdicties een beleidsoptie voor om de bewijslast in een aantal gevallen te verschuiven, bijvoorbeeld vanwege de aannemelijkheid dat de technologie in de schade voorzag, de informatieasymmetrie tussen leverende en afnemende partij en de bekendheid van het defect in het product.[30]

2.6 Conclusie

In deze paragraaf zijn enkele omstandigheden geschetst die specifiek in de context van schade door cyberonveiligheid het verhaal van die schade bemoeilijken. De zorgplicht is vaak niet duidelijk geformuleerd en bestaat in elk geval uit een inspanningsverplichting in plaats van een resultaatsverplichting; aansprakelijkheid wordt vaak contractueel uitgesloten; de schade is moeilijk kwantificeerbaar; het causaal verband tussen normschending en schade is moeilijk aantoonbaar en sowieso is het voor de afnemer moeilijk om bewijs te leveren omdat de benodigde informatie zich vaak in de invloedssfeer van de leverancier bevindt. De kans op een succesvolle claim is dus zeer beperkt. De economische barrières die wij in de volgende paragraaf kort bespreken, versterken deze conclusie.

---

[28] European Union, *Liability for Artificial Intelligence and other emerging digital technologies* 2019.

[29] Procesrechtelijke middelen zoals bewijsbeslag (artikel 730 jo 843a Rv, zie ook HR 13 september 2013, ECLI:NL:HR:2013:BZ9958) bieden in deze gevallen mogelijk niet altijd de gewenste snelheid.

[30] Deze expertgroep adviseert de Europese Commissie (Directoraat-generaal Justitie en Consumentenzaken (JUST)) bij het opstellen van nieuwe wetgeving en nieuw beleid. Expertgroepen zijn samengesteld uit deskundigen van nationale overheden, vertegenwoordigers van belangenorganisaties en/of experts uit het bedrijfsleven. Zie EU 2019, p 26.

3 Economische barrières

3.1 Economische barrière 1: onderhandelingsmacht

Grote partijen zoals Google, Microsoft en Amazon sluiten in het algemeen aansprakelijkheid volledig uit en beperken ook hun zorgplicht. Het is ook vaak niet mogelijk om naar een andere partij over te stappen omdat alle grote partijen dezelfde exoneratiebedingen hanteren en er op het gebied van veel internetdiensten een *de facto* mono- of oligopolie is, zoals Microsoft met Microsoft Office.[31] De onderhandelingsmacht kan zich ook aan de zijde van de afnemer voordoen, bijvoorbeeld de overheid die ook standaardvoorwaarden hanteert. Asymmetrische onderhandelingsmacht zonder keuzevrijheid beperkt de contractvrijheid en kan verkeerde prikkels ten aanzien van cybersecurity geven. Grote partijen kunnen bijvoorbeeld aansprakelijkheid voor de cybersecurity van hun producten uitsluiten, terwijl deze partijen wellicht ook tegen de laagste kosten cyberaanvallen kunnen voorkomen of beter in staat zijn de schade te dragen en/of te spreiden.

3.2 Economische barrière 2: toegang tot de rechter

Als een leverancier in beginsel aansprakelijk is, maar de kosten en/of risico's van een rechtszaak voor de afnemers te hoog zijn om een zaak tegen de leverancier te beginnen, dan blijft de schade bij de afnemers blijft liggen. Zulke 'rationele apathie' van de potentiële eiser(s) kan vooral relevant zijn bij gespreide schade, waar de totale schade weliswaar heel groot kan zijn, maar de schade voor individuele partijen te klein kan zijn om individuele zaken te starten. Deze barrière wordt nog verder verhoogd als een (kleine) afnemer uit land A moet procederen tegen een (grote) leverancier uit land B.

3.3 Economische barrière 3: faillissement

Vanwege onderlinge afhankelijkheid van softwaresystemen kunnen er bij cyberonveiligheid 'cascade-effecten' optreden en kan de totale schade snel heel groot worden, ook als de aangesproken leverancier zelf een relatief klein bedrijf is. De waarde van een claim wordt gemaximeerd door een eventueel faillissement van de leverende partij. In het geval dat een leverende partij (of een bestuurder daarbinnen) een verzekering heeft voor cybersecurityschade, dan wordt de maximaal verhaalbare claim vergroot door het maximale bedrag dat een verzekering

[31] Er zijn wel enkele alternatieven voor Microsoft Office, zoals OpenOffice en G-Suite, maar deze bieden niet dezelfde functionaliteit van en compatibiliteit met Microsoft Office, al zijn op dit vlak de afgelopen jaren, door bijvoorbeeld Google, wel verbeteringen gemaakt. Voor een deel van de bedrijven zal er dus een de facto monopolie van Microsoft zijn omdat deze bedrijven reeds in het ecosysteem van Microsoft zitten en de overstapkosten te hoog zijn. Voor andere bedrijven met lagere overstapkosten zal er meer sprake zijn van een oligopolie met beperkte keuzevrijheid.

kan uitkeren. Leveranciers zouden deze barrière kunnen benutten door het oprichten van aparte BVs voor risicovolle cybersecurityprojecten, die vervolgens failliet mogen gaan als er teveel schade geclaimd dreigt te worden.

4 Drie scenario's

Er zijn vele verschillende situaties van digitale onveiligheid denkbaar, waarin de hierboven geschetste barrières steeds op andere manieren tot uiting komen. In deze paragraaf schetsen wij drie verschillende scenario's en geven aan hoe belangrijk de verschillende barrières in die drie scenario's zijn. De conclusie is dat er steeds een of meer barrières zó belemmerend zijn dat contractuele aansprakelijkheid in geen van de scenario's een vruchtbare route biedt voor schadeverhaal op de leverancier.

Scenario 1: reputatieschade
Deze situatie betreft twee kleine bedrijven in Nederland. Als gevolg van een aantoonbare kwetsbaarheid in de IT-systemen van de leverende partij vindt er een aantoonbare cyberaanval plaats bij de afnemende partij, die eveneens cybersecuritydiensten levert. De aanval kan in de kiem worden gesmoord maar wordt wel publiekelijk bekend gemaakt door de hackers. De afnemende partij heeft geen materiële schade maar heeft de perceptie forse reputatieschade te lijden. De leverancier heeft zijn aansprakelijkheid beperkt tot drie keer de contractwaarde.
In dit scenario vormt het aantonen van de reputatieschade alsmede van het causale verband tussen die schade en de geschonden norm de grootste barrière. Verschillende zeer grondige en tijdrovende academische studies kunnen vaak geen langdurige reputatieschade aantonen bij grote bedrijven die slachtoffer zijn geworden van zeer omvangrijke cyberaanvallen.[32] Het aantonen van een schending van de zorgplicht kan ook moeilijk zijn, en een eventueel faillissement beperkt de waarde van de claim. Ongelijke onderhandelingsmacht en toegang tot de rechter lijken hier geen probleem.

Scenario 2: bedrijfsonderbreking
Het betreft hier een contract tussen een Nederlandse MKB-er en een grote internationale leverancier van clouddiensten. Door een cyberaanval bij de leverancier ontstaat er storing in enkele datacentra in de Amerikaanse westkust waardoor de Nederlandse MKB-er gedurende een week niet van de clouddiensten van leverancier gebruik kan maken en er dus een interruptie in de levering ontstaat. In het contract is de aansprakelijkheid maximaal geëxonereerd.[33]

[32] Bisogni, Asghari & Van Eeten 2017 en Nieuwesteeg & Faure 2018. Vaak kunnen er wel directe kosten aangetoond worden zoals de kosten van forensisch onderzoek en het herstel van data.
[33] Dit scenario is geïnspireerd op een recente interruptie van Microsoft Azure in het westen van de Verenigde Staten, zie o.a. <https://tweakers.net/nieuws/142981/hitteprobleem-in-datacentrum-microsoft-azure-veroorzaakt-storingen.html> (geraadpleegd 22 januari 2020).

In dit scenario gooit vooral de exoneratie roet in het eten. Door de grote verschillen in onderhandelingsmacht tussen de internationale leverancier van clouddiensten en een Nederlandse MKB-er is er waarschijnlijk weinig tot geen ruimte om enige vorm van aansprakelijkheid te behouden bij de leverende partij. Volgens Nederlands recht zal een beroep op een exoneratieclausule vaak slagen, tenzij de Nederlandse MKB-er bewijst dat door opzet of bewuste roekeloosheid de veiligheid van de systemen niet op orde was. De MKB-er heeft geen toegang tot de interne systemen van de cloudleverancier om hiervoor bewijs te vinden. Voorts bestaat de kans dat de procedure in Amerika moet worden gevoerd, waardoor de kosten voor verhaal nog verder stijgen.

Scenario 3: materiële schade
Hier doet een cybersecurityleverancier zaken met de overheid. De cybersecurityleverancier heeft willens en wetens grove fouten gemaakt in de eigen beveiliging waardoor er aantoonbare materiële schade ontstaat aan systemen en processen van de overheid, maar ook bij vrijwel alle haar andere klanten.[34]
In dit scenario is er weliswaar overduidelijk een normoverschrijding (want: opzettelijk handelen), maar de kans op faillissement van de leverancier is zeer groot, enerzijds omdat andere klanten van de leverancier ook hun schade zullen proberen te verhalen en anderzijds omdat het vertrouwen in de leverancier zodanig is beschadigd dat toekomstige inkomsten die de kosten kunnen dragen onwaarschijnlijk zijn. Een claim op basis van bestuurdersaansprakelijkheid kan zinvol zijn, en de maximale waarde van die claim is dan gebaseerd op het vermogen van de bestuurder en eventueel het verzekerde bedrag van de bestuurdersaansprakelijkheidsverzekering, voor zover deze cybersecurity niet uitsluit.[35]

5 Conclusies en aanbevelingen

Uit onze analyse blijkt dat de combinatie van juridische en economische barrières voor verhaal van schade door cyberonveiligheid zo belemmerend is, dat schadeverhaal in verreweg de meeste gevallen niet loont. Het stimuleren van verhaal zal een uitdagende opgave zijn als men de contractvrijheid zoveel mogelijk in stand wil houden. Desalniettemin doen wij een aantal aanbevelingen, waarbij aangetekend moet worden dat nader onderzoek nodig is naar mogelijke (neven)effecten voordat ze geïmplementeerd worden.

[34] Dit scenario is geïnspireerd op de DigiNotar affaire, waarbij een hacker inbrak bij het bedrijf DigiNotar, dat beveiligingscertificaten verzorgde, zie bijvoorbeeld N.S. van der Meulen, 'DigiNotar: Dissecting the First Dutch Digital Disaster', *Journal of Strategic Security* 2013, p. 46-58.
[35] Er moet dan sprake zijn van een persoonlijk ernstig verwijt. Zie o.a. P.D. Olden, 'Koester de maatstaf 'ernstig verwijt': beter hebben we niet', *Ondernemingsrecht* 2015, p. 367-369.; Westenbroek 2016 en het arrest Ontvanger/Roelofsen (ECLI:NL:HR:2006:AZ0758).

1. *Vergroot duidelijkheid over de contractuele zorgplicht.* Meer duidelijkheid over de zorgplicht verlaagt de onzekerheid over de vraag of een partij zijn verplichtingen heeft geschonden. De overheid kan hier een informerende rol kunnen innemen, bijvoorbeeld adviseren over normen in contracten. De zorgplicht kan worden verduidelijkt bijvoorbeeld door te stimuleren dat concrete cybersecuritystandaarden worden opgenomen in contracten. Men zou zelfs in het contract kunnen vastleggen wat men onder opzet of bewuste roekeloosheid verstaat. Standaarden, bijvoorbeeld keurmerken, hebben ook zelf weer nadelen, die voor deze specifieke context verder dienen te worden onderzocht. Zo moet men standaarden continu onderhouden en aanpassen aan de veranderlijke aard van cybersecurity en moet de partij die de standaarden vaststelt snel toegang hebben tot de informatie op basis waarvan kan worden bepaald of standaarden moeten worden aangepast. Bovendien zouden standaarden een negatieve invloed kunnen hebben op de alertheid van cybersecuritymedewerkers op nieuwe cybersecurityrisico's die niet afgedekt worden door standaarden, juist als deze medewerkers zich aan de gestelde standaarden houden. Meer onderzoek naar het effect van standaarden op het gebied van cybersecurity is dus noodzakelijk.
2. *Stimuleer vergemakkelijken van bewijsvoering (en onderzoek verzwaren verweerplicht of omkeren bewijslast).* De bewijslast ligt in beginsel bij de partij die de schade wil verhalen, tenzij anders overeengekomen. Dit beginsel bemoeilijkt de mogelijkheid om schade te verhalen omdat de afnemer niet de IT-systemen van de leverancier kan analyseren en dus ook niet kan identificeren of de zorgplicht is geschonden en of er een causaal verband is tussen de geschonden zorgplicht en de geleden schade. Het is wenselijk dat degene die tegen de laagste kosten de informatie kan leveren, de bewijslast krijgt opgelegd. De leverancier kan bijvoorbeeld door logs waarschijnlijk beter aantonen dat bepaalde stappen wél gezet zijn, dan dat de afnemer kan aantonen dat die stappen niet zijn gezet. Een verzwaarde motiveringsplicht,[36] zoals de verplichting tot het bewaren en desgewenst verstrekken van de logs van een cybersecurityincident, het aannemen van bewijsvermoedens, of zelfs omkering van de bewijslast voor de leverancier kunnen de barrières tot verhaal verlagen. In een lichtere variant kan de overheid partijen informeren om naast afspraken over de zorgplicht ook afspraken over bewijsvoering in (standaard)contracten op te nemen, bijvoorbeeld via de modellen voor algemene voorwaarden die brancheorganisaties aan hun leden ter beschikking stellen.
3. *Stimuleer of dwing meerdere opties voor aansprakelijkheid af bij grote partijen.* Dit kan de keuzeoptie voor kleinere- en middelgrote partijen vergroten en prikkels vergroten bij grote partijen om hun cybersecurity op orde te hebben en hun aansprakelijkheid niet af te schuiven op kleine partijen. Grote partijen zoals Google, Microsoft en Amazon sluiten in het algemeen aansprakelijkheid volledig uit. Wij bevelen aan om te onderzoeken of gestimuleerd of afgedwongen kan worden dat deze partijen ook een optie bieden waarin aansprakelijkheid voor digitale onveiligheid niet wordt uitgesloten. Ook kan worden onderzocht of (dwingend) consumentenrecht reflexwerking kan krijgen (of al heeft) voor kleine ondernemers in B2B-

[36] Artsen hebben bijvoorbeeld een verzwaarde motiveringsplicht bij medische fouten, zie o.a. HR 15-06-2007, ECLI:NL:PHR:2007:BA3587.

situaties waarin er grote verschillen in macht, informatie en andere facetten van de onderhandeling bestaan.[37] Uiteraard zal een uitbreiding van aansprakelijkheid van de leverancier wel tot gevolg hebben dat deze de prijs van het product of de dienst zal verhogen.

4. *Onderzoek de toegang tot de rechter en vergroot deze waar mogelijk.* Als een afnemer een internationale leverancier kan aanklagen in Nederland in plaats van in het land waar de leverancier gevestigd is, dan kan deze gemakkelijker verhaal halen. Verder internationaal privaatrechtelijk onderzoek is nodig naar de toegankelijkheid van de rechter met betrekking tot relaties met grote internationale (veelal Amerikaanse) cloudleveranciers. Een alternatieve beleidsroute is het stimuleren van ADR. Dat is vaak goedkoper, eenvoudiger en sneller en kan ook gebeuren zonder tussenkomst van een advocaat. Voordeel is ook dat er dan mogelijk minder reputatieschade optreedt en dat zelfs claims met een relatief lage verwachte opbrengst misschien toch kunnen worden beslecht.
5. *Alternatief voor aansprakelijkheid: stimuleer het afdekken van het risico.* Zowel voor de afnemende als voor de leverende partij kan een cyberverzekering een alternatief compensatiemechanisme vormen. De afnemende partij kan de geleden schade vanuit zijn verzekering vergoed krijgen en hoeft daardoor niet de mogelijk ingewikkelde – en daarmee inefficiënte – route van aansprakelijkheid te volgen. Dit geldt met name als de premie van de cyberverzekering een accurate weerspiegeling is van het schaderisico dat wordt overgedragen aan de verzekeraar. Hiervoor is het wel noodzakelijk dat de cyberverzekeringsmarkt verder volwassen wordt dan nu het geval is. Nader onderzoek naar de precieze inhoud en werking van de cyberverzekering is daarom aanbevolen.[38] Ook voor een leverende partij kan een cyberverzekering meerwaarde hebben doordat een van de belangrijkste dekkingselementen ‘incident response’ is. Dit is een georganiseerde aanpak en beheer van de nasleep van een beveiligingslek of cyberaanval. Het doel is om met de situatie om te gaan op een manier die schade beperkt en de hersteltijd en -kosten vermindert. Dat kan de kans dat het bedrijf wordt geconfronteerd met een aansprakelijkheidsclaim verkleinen. Incident response heeft namelijk een mitigerend effect op de schade richting afnemende partijen.

[37] Ook in het consumentenrecht is het echter niet geheel duidelijk wat de zorgplicht van cybersecurityleverancier inhoudt. Zou er dus reflexwerking zijn, dan loopt een bedrijf mogelijk alsnog tegen die horde aan. Zie bijv. de zaak tussen de Consumentenbond en Samsung (Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175 (Consumentenbond/Samsung) en P.W.J. Verbruggen, ‘Consumentenrecht en cybersecurity’ (redactioneel), TvC 2016, afl. 3, p. 97-98; P.T.J. Wolters & P.W.J. Verbruggen, ‘De verplichting tot het bijwerken van onveilige software’, WPNR 2016, afl. 7123, p. 832-839.

[38] Zie bijvoorbeeld reeds N.M. Brouwer, ‘Cyberverzekeringen vanuit rechtsvergelijkend perspectief: privacyregelgeving in de VS en de Europese AVG’, *AV&S* 2018/19, p. 92-104 en N.M. Brouwer, ‘‘Vlijt en naarstigheid’ in een digitale wereld: eigen schuld en beredding in de context van de cyberverzekering’, *AV&S* 2019/23, p. 119-128; N.M. Brouwer, ‘Cyberverzekeringen en de zorgplicht van de assurantietussenpersoon’, *WPNR* 2017/7160, p. 568-576; W.C.T. Weterings, ‘Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?’, *AV&S* 2015/2, p. 4-14.