Studie:

Aansprakelijkheid voor digitale onveiligheid in b2b-relaties

Bernold Nieuwesteeg [1]
Michael Faure [2]
Louis Visscher [3]

[1] Mr. dr. ir. Bernold Nieuwesteeg is directeur van het Centre for the Law and Economics of Cyber Security aan de Erasmus Universiteit Rotterdam.
[2] Prof. dr. Michael Faure is hoogleraar rechtseconomie aan de Erasmus universiteit Rotterdam en Maastricht University en is haiwaimingshi (bijzonder buitenlands hoogleraar) aan het Centre for Law and Economics van de China University of Political Science and Law.
[3] Prof. dr. Louis Visscher is bijzonder hoogleraar rechtseconomie aan de Erasmus Universiteit Rotterdam

2020

Dit onderzoek is in opdracht van het Ministerie van Economische Zaken en Klimaat verricht door Bernold Nieuwesteeg, Michael Faure en Louis Visscher van de Erasmus Universiteit Rotterdam, Centre for the Law and Economics of Cyber Security (CLECS). De auteurs bedanken Ghyslaine Krebbekx, Nelly Ghaoui, Maartje Beltman, Anne Marie Načinovič en Matthijs Balder voor hun waardevolle feedback op eerdere conceptversies. Ook danken de auteurs de gesproken experts voor hun waardevolle inzichten en opmerkingen.

Management-samenvatting

In deze studie is onderzocht of het Nederlandse aansprakelijkheidsrecht voldoende mogelijkheden biedt om in een b2b-relatie cybersecurityschade te verhalen. Voorbeeld hiervan is een bedrijf dat gehackt wordt omdat het gebruik maakt van onveilige software van een leverancier en daardoor schade lijdt.

Onze conclusie is dat de juridische en economische barrières vaak te groot zijn om verhaal praktisch mogelijk te maken. Deze barrières zijn:

- De zorgplicht. Schade kan alleen worden verhaald als er een schending is van een 'norm'. In het geval van aansprakelijkheid voor cybersecurity zijn dit minimumvereisten voor cybersecurity. Deze vereisten zijn bijvoorbeeld in het contract vastgelegd of komen door de aard van de b2b-relatie tot uitdrukking
- Schade. Uiteraard moet er schade zijn om een mogelijkheid te hebben om deze te verhalen
- Causaliteit. Er dient een causaal verband te zijn tussen de geschonden norm, in casu de cyberonveiligheid van de leverende partij, en de geleden schade van de afnemende partij.
- 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 enorm omdat de afnemende partij niet in de IT-systemen van de leverende partij kan kijken en dus ook niet kan identificeren of de zorgplicht is geschonden en er een causaal verband is tussen de geschonden zorgplicht en de geleden schade.
- Onderhandelingsmacht. Grote partijen sluiten in het algemeen aansprakelijkheid volledig uit en beperken ook hun zorgplicht. Hier valt, in ieder geval in de perceptie van MKB partijen, niet of nauwelijks over te onderhandelen.
- Toegang tot de rechter als de juridische kosten hoog zijn en de succesverwachting laag, bijvoorbeeld in het geval van het halen van verhaal bij een Amerikaanse leverancier.
- Faillissement. De waarde van een claim wordt gemaximeerd door een eventueel faillissement van de leverende partij.

Er zijn daarom ook voor zover wij weten geen rechtszaken rondom dit thema. Kan beleid deze juridische en economische barrières deels wegnemen? Een bijkomende uitdaging: de beleidsopties dienen de contractvrijheid zo veel mogelijk in stand te laten, want contractvrijheid zorgt in de meeste gevallen voor welvaart. In dit onderzoek doen wij enkele suggesties voor verder onderzoek naar beleidsopties. Deze strekken ertoe:

- Afspraken over cybersecurity te verduidelijken zodat ook duidelijker wordt wanneer een leverancier zich niet aan de afspraken met betrekking tot cybersecurity houdt. (de zogenaamde 'zorgplicht').
- De bewijslast te vereenvoudigen door het eenvoudiger te maken de zowel schade als het verband tussen de schade en de gebrekkige cybersecurity te bewijzen.

Binnen een b2b-relatie is de contractvrijheid niet problematisch, tenzij er bijvoorbeeld sprake is van een zodanig verschil in onderhandelingsmacht dat de sterke partij hiervan misbruik kan maken. Daartoe strekken ook een aantal aanbevelingen tot verder onderzoek, zoals onderzoek naar:

- Het verplichten van meer pluraliteit in aansprakelijkheidsvormen bij grote software-aanbieders, zodat niet alle aansprakelijkheid standaard wordt uitgesloten door die partijen.
- Toegang tot de rechter wanneer men schade wil verhalen bij grote internationale partijen.

Concluderend: het mes van het aansprakelijkheidsregime is bot. Zelfs indien beleidsopties worden doorgevoerd blijft de balans houden tussen het stimuleren van verhaalsmogelijkheden en het in stand houden van contractsvrijheid een uitdagende opgave voor de overheid. De vraag is of het aansprakelijkheidsregime in een b2b-relatie een effectief middel is om schade te verhalen en prikkels goed te leggen. Men zou ook alternatieven voor aansprakelijkheidsstelling kunnen onderzoeken en/of stimuleren, zoals het risico afdekken door middel van bijvoorbeeld een cyberverzekering of een risicospreidingsovereenkomst. Voor een afnemende partij kan dat een laagdrempelig alternatief zijn voor aansprakelijkheidsstelling van de leverancier die bemoeilijkt wordt door de grote juridische en economische barrières voor verhaal.

Inhoudsopgave

1. Inleiding

Het ministerie van Economische Zaken en Klimaat wil cybersecurity in Nederland versterken. Aansprakelijkheid voor schade die voortkomt uit cyberonveiligheid is in dat kader een belangrijk thema.[1] Het civiele aansprakelijkheidsrecht biedt juridische mogelijkheden om verhaal te zoeken voor geleden schade. Desondanks is er door het ministerie van Economische Zaken en Klimaat geconstateerd dat er vanuit het werkveld beginnende geluiden zijn dat aansprakelijkheden op het gebied van cybersecurity beter geregeld moeten worden.[2] Het lijkt er op dat in Nederland in de huidige praktijk de geleden schade niet systematisch wordt verhaald.[3]

Aansprakelijkheid voor cybersecurity kan twee primaire doelstellingen dienen:

1. Ten eerste kan aansprakelijkheid voor cybersecurity compensatie bieden voor een partij die schade lijdt op basis van de gemaakte contractuele afspraken tussen partijen. Als er schade ontstaat, kan het maatschappelijk wenselijk zijn dat de schade wordt gecompenseerd door de partij die de schade heeft veroorzaakt.[4]

2. Ten tweede kan een aansprakelijkheidsregime maatschappelijk nuttige prikkels voor optimale cybersecurityniveaus geven.[5] Compensatie kan tevens tot een maatschappelijk gewenste prikkel leiden bij de leverende partij om te investeren in optimale cybersecurity. Dat is bijvoorbeeld het geval wanneer deze leverancier zich er contractueel toe verbonden heeft dat hij eventuele schade als gevolg van zijn eigen suboptimale cybersecurityniveaus zal vergoeden. Als partijen gemakkelijker verhaal kunnen halen bij een leverancier, kan dit leiden tot verhoogde prikkels om voor afdoende cyberveiligheid te zorgen bij de leverancier.

De studie richt zich primair op de vraag of het eerste doel via het huidige aansprakelijkheidsregime en de toepassing daarvan in Nederland in voldoende mate kan worden bereikt. De studie onderzoekt de mogelijkheden die een organisatie heeft in een business to businessrelatie (hierna: b2b-relatie) om het privaatrecht in te zetten wanneer zij schade lijdt door digitale onveiligheid, alsmede haar motivaties voor het wel of niet inzetten van dit middel.

De studie is een verkennend onderzoek en poogt een bijdrage te leveren aan het dichten van de kloof die bestaat tussen enerzijds het technische werkveld van cybersecurity en anderzijds de

1. Zie bijvoorbeeld de Roadmap Digitaal Veilige Hard- en Software.
2. Opdrachtomschrijving Ministerie van Economische Zaken en Klimaat.
3. Opdrachtomschrijving Ministerie van Economische Zaken en Klimaat.
4. Er zijn verschillende redenen te geven waarom vergoeding van schade door de schadeveroorzaker wenselijk wordt geacht, bijvoorbeeld preventie, rechtvaardigheid, kostenallocatie, handhaving van rechten of vergoeding van geleden nadeel. Zie o.a. Priest (1988); Blomquist (1988) voor een discussie over de verschillende doelen van het aansprakelijkheidsrecht. Dit verkennende onderzoek gaat verder niet in op deze onderliggende redenen van de verschillende aspecten van het aansprakelijkheidsrecht. Zie ook Lindenbergh (2014).
5. Dat wordt dan omschreven als het punt waar de marginale kosten (van investeringen in cybersecurity) gelijk zijn aan de marginale opbrengsten (in verbetering van de veiligheid van het systeem), zie ook Nieuwesteeg (2018).

juridische mogelijkheden op het gebied van aansprakelijkheid. We onderzoeken de mate van scherpte van het aansprakelijkheidsinstrument in een b2b-relatie op het gebied van cybersecurity. Met andere woorden: kan er effectief gebruik worden gemaakt van het aansprakelijkheidsrecht? We zullen in deze inleiding kort ingaan op de reikwijdte, methode en structuur van het onderzoek.

1.1 Reikwijdte

We hanteren enkele uitgangspunten ten aanzien van de reikwijdte van dit verkennende onderzoek.[6] Allereerst betreft het onderzoek een juridische en rechtseconomische analyse van de Nederlandse regels en mogelijkheden op het gebied van aansprakelijkheid voor cybersecurity in een b2b-relatie. Hierbij bespreken we voorbeelden van Nederlandse jurisprudentie op het terrein van cybersecurityaansprakelijkheid in een b2b-relatie, waarbij aangetekend dient te worden dat die jurisprudentie (nog) schaars is. In sectie 3 gaan we tevens kort in op het Europese raamwerk met betrekking tot productaansprakelijkheid. We komen tot de conclusie dat dit raamwerk voor dit onderzoek minder relevant is omdat productaansprakelijkheid een bescherming biedt aan consumenten en zich richt op fysiek letsel, iets dat zich in een b2b-relatie op het gebied van cybersecurity niet voordoet. Ten tweede richt de analyse zich op partijen die reeds een b2b-relatie hebben. De juridische mogelijkheden die wij analyseren gaan dus uit van een reeds bestaande contractuele relatie tussen een afnemende en een leverende partij. Ten derde maakt het onderzoek gebruik van openbare bronnen. We analyseren dus geen informatie uit specifieke contracten tussen partijen. Ten vierde beschouwt het onderzoek geen privacygerelateerde aansprakelijkheid. Dit heeft te maken met de constatering dat de Algemene Verordening Gegevensbescherming (hierna: AVG) in beginsel de gegevens beschermt van natuurlijke personen en niet van rechtspersonen.[7] Er is discussie denkbaar over de vraag of 'eenieder' in art. 82 AVG ook van toepassing is op rechtspersonen, maar dit debat valt buiten de reikwijdte van dit onderzoek. Ten vijfde vatten wij 'cybersecurityschade' op als schade bij een afnemende partij die voortvloeit uit intentionele gedragingen vanuit een kwaadwillende derde (een cyberaanval, zoals ook beschreven in de opdrachtomschrijving) ten gevolge van acties van de leverende partij zoals bijvoorbeeld een onvoldoende niveau van cybersecurity. We beschouwen onder meer aansprakelijkheidszaken waarbij bijvoorbeeld een softwaretoeleverancier aansprakelijk kan worden gesteld door een cyberaanval die resulteert in een onderbreking van de continuïteit, integriteit of beschikbaarheid van een systeem.[8]

In het technische werkveld van cybersecurity worden talloze contracten afgesloten tussen afnemers en leveranciers van producten en diensten die een cybersecuritycomponent hebben. Hierbij kan gedacht worden aan een overeenkomst tussen een cybersecurityleverancier en een lokale overheid voor een serie van penetratietesten om haar systemen op kwetsbaarheden te testen. Maar denk ook aan een contract tussen diezelfde cybersecurityleverancier en een grote

6. Deze uitgangspunten zijn tot stand gekomen in overleg tussen opdrachtgever en opdrachtnemer voorafgaand aan het starten van het onderzoek, en zijn onder andere besproken in de opdrachtomschrijving en de offerte die de basis vormen van dit onderzoek. Zo spreekt de opdrachtomschrijving binnen het kopje aanpak bijvoorbeeld van 'een rechtseconomische analyse, waarin er met een economische blik naar de inzet van het civiele aansprakelijkheidsrecht ter stimulans voor digitale veiligheid wordt gekeken. De scope richt zich op het civiele aansprakelijkheidsrecht in een business-to-businessrelatie. Het onderzoek is gericht op de praktijk binnen Nederland en zal gebruik maken van openbare bronnen.' Opdrachtomschrijving Ministerie van Economische Zaken en Klimaat.
7. Algemene Verordening Gegevensbescherming - Verordening 2016/679. 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 op deze Verordening, het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.
8. Er zijn bijvoorbeeld zaken waarbij een derde partij back-ups beheerde en die per ongeluk overschreef met het gevolg een verlies aan data. Hierop volgde een aansprakelijkheidszaak, maar dergelijke zaken vallen dus buiten de reikwijdte van het onderzoek. Zie voor de continuïteit, integriteit of beschikbaarheidsdrie-eenheid ook Pfleeger (2003) p. 504.

cloudleverancier voor dataopslag en rekenkracht. Veel clausules in contracten worden na opstelling ervan niet ingeroepen. Deze contracten regelen immers veel zaken die vaak niet misgaan, zoals de consequenties bij wanprestatie (bijvoorbeeld een niet tijdige levering), een concurrentiebeding en het intellectueel eigendom van het product of dienst. De vergoeding van de schade die voortvloeit uit onvoldoende cybersecurity vanuit de leverende partij valt ook onder de categorie clausules die, wanneer er zich geen cybersecurityincidenten voordoen, niet zal worden ingeroepen.[9]

Uit het bovenstaande blijkt dat er minstens vier verschillende partijen bij digitale onveiligheid betrokken kunnen zijn: A: de leverancier van de cybersecurity; B: de afnemer van producten of diensten met een cybersecuritycomponent die schade kan lijden; C: een derde die schade kan lijden en D: een derde die intentioneel schade veroorzaakt (de hacker). In dit rapport staat de (contractuele) relatie tussen A en B centraal. We zullen in bijlage 1 de mogelijkheid voor derden (C) om A (met wie ze geen contractuele relatie hebben) aansprakelijk te stellen op basis van onrechtmatige daad bespreken, daar dit buiten de reikwijdte van het rapport valt.[10] We gaan ervanuit dat D (de kwade genius die een zwakheid in het cybersecuritysysteem heeft ontdekt) onvindbaar, dan wel onvermogend is, en dat tegen D derhalve geen verhaal kan worden uitgeoefend. In sommige gevallen kan de leverancier A ook zelf digitale onveiligheid veroorzaken, bijvoorbeeld doordat hij schade aanricht door een penetratietest uit te voeren op reeds operationele systemen. In dat geval is er geen sprake van een hacker en kan de leverancier A direct worden aangesproken.

1.2 Methode

Voor dit onderzoek wordt voornamelijk gebruik gemaakt van deskresearch binnen de rechtseconomie van cybersecurity. Daartoe zal gebruik worden gemaakt van de rechtseconomische methode met aandacht voor de invloed van verschillende financiële en andere prikkels op het gedrag van partijen. De rechtseconomie kan aangeven of en in welke mate een aansprakelijkstelling van de leverancier diezelfde leverancier prikkels kan geven tot het bevorderen van optimale cybersecurity. Een voorbeeld: een grote kans op aansprakelijkheid bij slechte cybersecurity van de leverancier kan bijvoorbeeld leiden tot meer investeringen in cybersecurity door de leverancier terwijl een kleine kans op aansprakelijkheid minder reden geeft voor een leverancier om goede cybersecurity in zijn producten in te bouwen. Ook kan de rechtseconomie door de economische blik op het juridische, praktische barrières voor verhaal analyseren, iets dat we in dit onderzoek ook zullen doen. Binnen de rechtseconomie wordt ook veel aandacht besteed aan kosten-batenanalyses. Vandaar dat voor een rechtseconoom het verwerven van *optimale* cybersecurity het maatschappelijk doel is, hetgeen geen *maximale* cybersecurity (als dat al mogelijk zou zijn) hoeft te betekenen.[11] Naast deskresearch naar rechtseconomische bronnen wordt ook gebruik gemaakt van een analyse van jurisprudentie. Bedoeling is niet een uitgebreide analyse van het Nederlands privaatrecht en de toepasselijke regels te geven, maar om aan de

9. Dit beeld komt ook naar voren uit de interviews met Erik Rutkens en Maarten Wegdam.
10. In bijlage 1 doen wij ook een korte aanzet of het privaatrecht kan worden ingezet om maatschappelijk nuttige prikkels voor optimale cybersecurityniveaus aan alle partijen te geven. Het is belangrijk aan te stippen dat binnen het privaatrecht twee verschillende instrumenten ter beschikking staan om schade op een leverancier te verhalen. In de eerste plaats is dat het contractenrecht dat van toepassing zal zijn in de contractuele relatie tussen de leverancier en de afnemer en dat bij wanprestatie door de leverancier tot compensatie zou kunnen leiden. Het contractenrecht vormt de kern van onze analyse. In de tweede plaats is er het buitencontractuele aansprakelijkheidsrecht (aansprakelijkheid uit onrechtmatige daad) dat ertoe leidt dat leveranciers (of anderen) aansprakelijk kunnen worden gesteld voor de door hen veroorzaakte schade, ook als er geen contractuele relatie bestaat.
11. Dat wordt dan omschreven als het punt waar de marginale kosten (i.c. dus de kosten van extra investeringen in cybersecurity) gelijk zijn aan de marginale opbrengsten daarvan (dus de resulterende verbetering van de veiligheid van het systeem), zie ook Nieuwesteeg (2018).

hand van de beperkte jurisprudentie op terrein van cybersecurity te analyseren hoe de verhaalsmogelijkheden van verschillende scenario's van digitale onveiligheid in de praktijk uitwerken. Ten slotte zal ook van een empirische component gebruik worden gemaakt teneinde te verifiëren in welke mate binnen b2b-relaties van beperking of uitsluiting van aansprakelijkheid gebruik wordt gemaakt en in welke mate leveranciers van cybersecurity in Nederland daadwerkelijk met aansprakelijkstellingen worden geconfronteerd. Daartoe zal binnen de reikwijdte van het onderzoek met een beperkt aantal stakeholders explorerend worden gesproken ter kleuring van de scenario's en de praktijk van cybersecurity. Dit laat een 'reality check' van het veeleer theoretisch rechtseconomische perspectief toe. Sectie 6 biedt een overzicht van de geraadpleegde respondenten.

1.3 Structuur van het onderzoek

Het onderzoek is als volgt gestructureerd. Allereerst bestuderen we de doelen van het aansprakelijkheidsregime voor cybersecurity in een b2b-relatie (2). Vervolgens zullen we de belemmeringen die het privaatrecht biedt om schade ten gevolge van digitale onveiligheid te verhalen, bespreken (3). Daarna zullen we enkele scenario's schetsen en deze scenario's koppelen aan de doelen van een aansprakelijkheidsregime en de handvatten die het aansprakelijkheidsrecht op dit moment biedt (4). In deze sectie komen ook de interviews aan bod die dienen ter kleuring van de praktijk van de civiele aansprakelijkheid. Tenslotte zullen we concluderen en richtingen aangeven voor de identificatie van beleidsinstrumenten (5).

2. Het belang van contractvrijheid

Als een partij die diensten met een cybersecuritycomponent afneemt een risico waarneemt op mogelijke schade ten gevolge van digitale onveiligheid, dan zal deze partij een afweging willen maken hoe deze met dat risico wil omgaan. Die afweging zal afhankelijk zijn van de risicobereidheid, het type opdracht, de eigen solvabiliteit; kortom met de omstandigheden van het geval die maken dat elke actor in het economische systeem eigen voorkeuren heeft.

De afnemende partij heeft in een vrije markt verschillende alternatieven, zoals:

1. pogen het risico op schade en de gevolgen daarvan contractueel geheel bij de leverende partij te leggen,
2. het risico op schade (deels) zelf dragen en een lagere prijs bedingen,
3. het risico op schade (deels) zelf dragen, een lagere prijs bedingen en dit risico (deels) verzekeren.

Een van de basisprincipes binnen een marktecono-mie is dat partijen verschillende voorkeuren hebben en dat de vrijheid om naar die voorkeuren te (onder)handelen de maatschappelijke welvaart vergroot. Daarom is contractvrijheid een wenselijk uitgangspunt. Immers, als de overheid via het privaatrecht of anderszins een verplichting zou inbouwen om bijvoorbeeld het risico bij de leverende partij te leggen, met een relatief hogere prijs tot gevolg, dan verhoogt het recht de prijs van het product voor iedereen, ook voor de partijen die het risico beter zelf hadden kunnen dragen of verzekeren, met economisch verlies als resultaat. Juist omdat de preferenties van partijen verschillen, zullen bepaalde partijen met een dergelijk overheidsingrijpen in de markt niet gediend zijn en zal een vermindering van de keuzevrijheid de maatschappelijke welvaart reduceren.

De ene partij zal bijvoorbeeld alle risico's op cybersecurityschade zelf willen dragen en een lagere prijs willen bedingen, terwijl een andere partij alle risico's bij de leverende partij wil houden. De redenen voor die onderscheiden keuzes kunnen met verschillende elementen samenhangen zoals:

- de houding ten aanzien van risico van beide partijen;
- het eigen vermogen van de afnemer en diens mogelijkheden om het risico eventueel zelf te dragen;
- informatie en de mogelijkheden van beide partijen om het risico correct in te schatten en
- de mogelijkheid om het cybersecurityrisico te dekken ofwel via een aansprakelijkheids-verzekering (voor de leverancier) dan wel een zogenaamde first party verzekering (voor de afnemer).

We benadrukken dat in de contractuele sfeer de vrijheid om risico's te verdelen in deze b2b-relatie doorgaans niet problematisch is, tenzij er bij-voorbeeld sprake is van een zodanig verschil in onderhandelingsmacht dat de sterke partij hiervan

misbruik kan maken. Wel kan een probleem rijzen wanneer derden ook schade lijden en die trachten te verhalen op de leverende partij. Precies die door derden geleden schade kan ook maatschappelijke schade vormen. Dit fenomeen bespreken we kort in bijlage 1. Zoals in sectie 3 verder zal worden uitgewerkt zijn er zowel juridische als economische barrières die een aansprakelijkheidsstelling kunnen bemoeilijken.

3. Barrières om schade te verhalen in een contractuele relatie

In deze paragraaf gaan we nader in op de mogelijkheden die het privaatrecht biedt voor een aansprakelijkheidsstelling ten gevolge van gebrekkige cybersecurity bij de leverancier. Het gaat, het zij nogmaals gezegd voor de duidelijkheid, daarbij om gebrekkige digitale veiligheid van ICT producten en diensten in een b2b-relatie.[12]

3.1 Vormen van aansprakelijkheid

We richten onze analyse voornamelijk op de contractuele aansprakelijkheid voor wanprestatie omdat dit in verreweg de meeste gevallen de route voor verhaal is voor een partij die een contract heeft met een andere partij. Een voorbeeld hiervan is de levering van een penetratietest door een cybersecurityleverancier aan de gemeente die schade veroorzaakt omdat onverhoopt een niet van het internet afgesloten systeem wordt getest.

Een andere route voor verhaal is aansprakelijkheid uit onrechtmatige daad. Voor deze route is het noodzakelijk dat er schade bij andere partijen (derden) ten gevolge van gedragingen bij de leverende partij ontstaat.[13] Deze derden mogen geen contractuele relatie hebben met de leverende partij. In het geval van een contractuele

12. Een korte verkenning van de aansprakelijkheidsroute in de ons omringende landen vertelt ons dat ook in die landen bij contractuele aansprakelijkheid zal moeten worden aangetoond dat de tegenpartij wanprestatie heeft begaan en uiteindelijk verloopt de route tot verhaal niet structureel anders dan in Nederland. We laten in dit rapport derhalve verdere rechtsvergelijking buiten beschouwing.
13. Uitzonderlijke situaties daargelaten. In de meeste gevallen zal de onrechtmatige daadsactie (buitencontractuele aansprakelijkheid) geen mogelijkheden bieden ten opzichte van contractuele aansprakelijkheid in een b2b-relatie. Deze zogenaamde samenloop tussen contractuele aansprakelijkheid en aansprakelijkheid uit onrechtmatige daad is een complexe materie die buiten de reikwijdte van het onderzoek valt. Zie Asser/Hartkamp & Sieburgh (2015), nr. 10. Volgens Hartkamp en Sieburgh brengt de strekking van de contractuele aansprakelijkheid uit art. 6:74 BW mee dat bij wanprestatie de contractuele regeling toepasselijk is, en niet de regeling van de onrechtmatige daad uit art. 6:162 BW. 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 Hartkamp en Sieburgh stellen dat ter bescherming van de schadelijder mag worden verwacht dat een exoneratiebeding duidelijk moet aangeven of het ook op buitencontractuele aansprakelijkheid betrekking heeft. Asser/Hartkamp & Sieburgh (2015), nr. 10 en 12. Het belang van deze vraag is ook beperkt omdat de regeling voor schadevergoeding bij contractuele en buitencontractuele aansprakelijkheid dezelfde is. De noodzakelijke invulling van de open normen kan echter wel enigszins verschillen. In de praktijk zal er in een b2b-relatie allereerst naar de mogelijkheden van contractuele aansprakelijkheid wegens wanprestatie worden gekeken omdat daar de normen duidelijker zijn dan in het geval van de route van de aansprakelijkheid uit onrechtmatige daad.

relatie dient men namelijk in beginsel de route van wanprestatie te belopen. Derhalve valt deze situatie buiten de reikwijdte van het rapport. Desalniettemin wijdt bijlage 1 kort uit over de barrières voor verhaal voor derden.[14] Een voorbeeld is dat hackers een e-mailsysteem van een bedrijf kraken, en vanuit die e-mailserver phishingmails sturen naar een derde partij die geen zaken doet met het bedrijf.

Wel is er nog een bijzondere aansprakelijkheid mogelijk voor bestuurders, de zogenaamde bestuurdersaansprakelijkheid. Hoewel deze ook als relatief uitzonderlijk kan worden gekwalificeerd, is theoretisch denkbaar dat een bestuurder van een vennootschap die gebrekkige cybersecurity levert, persoonlijk aansprakelijk kan worden gehouden, maar de voorwaarden ter zake zijn bijzonder streng. In het geval van bestuurdersaansprakelijkheid moet een bestuurder van een vennootschap een persoonlijk ernstig verwijt kunnen worden gemaakt. Dit zijn zeer specifieke gevallen.

Voor de volledigheid melden we dat er, mede ter implementatie van de Europese Richtlijn Productaansprakelijkheid van 25 juli 1985 ook een specifiek regime bestaat voor productaansprakelijkheid. Echter, dat regime is gericht op gevallen waarbij door een gebrek in een product letselschade wordt veroorzaakt. Daarnaast is dit regime specifiek gericht op een bescherming van consumenten. Door bedrijven geleden schade valt buiten het regime van de Richtlijn Productaansprakelijkheid en wordt derhalve hier ook niet verder besproken.

In dit gedeelte worden de voorwaarden voor aansprakelijkheid verder uitgediept en wordt verduidelijkt waarom contractuele aansprakelijkheid voor gebrekkige cybersecurity op belangrijke juridische en economische barrières zal kunnen stuiten. Het uitgangspunt hierbij is dat wanneer bedrijven onderhandeld hebben er vanzelfsprekend wel een grond voor een claim ontstaat als zich schade voordoet bij de afnemende partij. Desalniettemin hebben wij in een analyse van de jurisprudentie en explorerende interviews met experts en leiders van cybersecuritybedrijven geen zaken kunnen vinden die tot aansprakelijkheidsclaims tegen leveranciers hebben geleid ten gevolge van gebrekkige cybersecurity bij die leverancier.[15] Dat komt naar alle waarschijnlijkheid door juridische en economische barrières voor verhaal die wij in deze sectie zullen bespreken.

Wij bespreken de voor de huidige Nederlandse praktijk meest relevante juridische barrières op basis van een rechtseconomische analyse. Het gaat daarbij in de context van cybersecurity in een b2b-relatie om de zorgplicht, het vaststellen van de schade, de causaliteit en de bewijslast.

Daarnaast zijn in de contractuele relatie omtrent cybersecurity vaak economische barrières waardoor de mogelijkheden voor partijen om goede afspraken te maken of verhaal te halen (bijvoorbeeld over de gewenste reikwijdte van de aansprakelijkheid van een leverancier) in de praktijk niet altijd uit de verf komen. We bespreken de onderhandelingsmacht, de toegang tot de rechter en het faillissement van de leverancier.

14. Binnen de reikwijdte van dit rapport focussen wij op de b2b-relatie. Hier gaat het in eerste instantie om de contractuele aansprakelijkheid voor wanprestatie, maar zoals in bijlage 1 worden geschetst, rijzen deze barrières evenzeer bij de aansprakelijkheid uit onrechtmatige daad.
15. We zijn wel aanpalende zaken tegengekomen en zaken die zich op een ander terrein bevinden dan cybersecurity maar waar we wel barrières voor verhaal uit kunnen afleiden. Deze zaken worden in dit rapport waar toepasselijk benoemd. Zo speelde in 2014 de zaak Ratonigid/Vasco (NL:RBAMS:2014:4888). Het gaat hier niet om een b2b-relatie waarin een cybersecurity product of dienst wordt geleverd, maar 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 dienden te betalen aan het bedrijf VASCO Data Security International, dat in januari 2011 de aandelen DigiNotar overnam. Ratonigid (de holding achter DigiNotar) had DigiNotar verkocht aan Vasco. Met de verkoop waren garantiebepalingen gemoeid waarin veiligheidseisen stonden. Ratonigid moest aan Vasco een bedrag moet betalen waardoor Vasco in de positie komt waarin zij had verkeerd als de garantieschending niet had plaatsgevonden. Als gevolg van de garantieschendingen had de hack in de zomer van 2011 kunnen plaatsvinden en daarom is DigiNotar failliet is gegaan. Er is in deze zaak een 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. Ook faillissement speelde hier geen rol, omdat het ging om de verkoop van DigiNotar door de bovenliggende holding.

3.2 Juridische barrière 1: de zorgplicht.[16]

Schade kan alleen worden verhaald als er een schending is van een 'norm'. In het geval van aansprakelijkheid voor cybersecurity zijn dit minimumvereisten voor cybersecurity. Deze vereisten zijn bijvoorbeeld in het contract vastgelegd of komen door de aard van de b2b-relatie tot uitdrukking.[17] Deze norm verschilt dus van geval tot geval. Als het gaat om de beveiliging van staatsgeheimen zal de cybersecuritynorm uiteraard strenger zijn dan als het gaat om een kwetsbaarheidsscan van de plaatselijke voetbalclub. De leverende partij heeft vervolgens een zorgplicht om aan de norm te voldoen. De invulling van de zorgplicht is afhankelijk van de omstandigheden van het geval. De zorgplicht om aan de norm te voldoen verschilt ook voor de verschillende aansprakelijkheidsroutes die genomen worden om schade te kunnen verhalen.

Ten eerste is daar de overtreding van de norm met betrekking tot contractuele aansprakelijkheid, ook wel wanprestatie of toerekenbare tekortkoming genoemd. In beginsel kunnen partijen contractueel afspreken wat er ter zake van cyberveiligheid van de leverancier wordt verwacht.[18] Bepaalde normen kunnen contractspartijen daarbij te hulp komen om te verduidelijken wat er specifiek van de leverancier kan worden verwacht.[19] Zo kunnen partijen bijvoorbeeld de volgende zorgplicht afspreken: de leverancier moet zich aan bepaalde cybersecuritystandaarden houden zoals ISO27001 en moet jaarlijks een cybersecurityaudit laten doen om extern te laten controleren of de leverancier zich inderdaad aan de standaarden houdt.[20] 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 is dat cyberveiligheid doorgaans niet als een zogenaamde resultaatsverplichting kan worden gekwalificeerd. Dat betekent dat een leverancier nooit absolute cyberveiligheid zal garanderen. De reden is simpel: de kosten voor een absolute cyberveiligheid zouden veel te hoog zijn. In de praktijk zal op een leverancier uitsluitend een inspanningsverbintenis rusten. Zulke inspanningsverplichtingen kunnen te vaag geformuleerd kunnen worden. In sommige gevallen is sprake van te lage verwachtingen inzake de cybersecurity van het geleverde product of dienst, bijvoorbeeld wanneer een aanzienlijke "downtime" wordt afgesproken.[21] Een leverancier zal, vanuit zijn perspectief, 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. Vanuit het perspectief van de afnemer zal veeleer worden aangedrongen op het naleven van specifieke cybersecuritynormen zoals een ISO-norm omdat het dan eenvoudiger kan zijn aan te tonen dat de leverancier zich daar niet aan gehouden heeft.

In de praktijk geldt dat de norm lastig is vast te stellen omdat er weinig tot geen vergelijkbare Nederlandse jurisprudentie is met betrekking tot het verhaal van schade als gevolg van digitale

16. 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.
17. Tjong Tjin Tai & Koops (2015).
18. Enerzijds rust op de afnemer een informatieplicht (zo dient hij de leverancier correct te informeren over de aard van zijn werkzaamheden, bedrijvigheden en noden op het terrein van cyberveiligheid), maar anderzijds heeft de leverancier ook 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.
19. Deze normen kunnen bijvoorbeeld vastgesteld worden in een service level agreement.
20. Vergelijk ook de garantiebepalingen in de Share Purchase Agreement in de zaak Ratonigid/Vasco (NL:RBAMS:2014:4888).
21. De tijd dat een product of dienst niet naar behoren hoeft te werken, vaak uitgedrukt als percentage van de totale gewenste duur van het operationeel zijn van het product of de dienst.

onveiligheid in b2b-relaties.[22] Voor consumenten ontwikkelt de discussie over de zorgplicht van partijen zich naar het zich laat aannemen sneller in rechtspraak en Europese wetgeving zoals de recente Europese Richtlijnen 2019/770 en 2019/771.[23] Deze Richtlijnen kleuren de verwachtingen die een consument van een leverancier mag hebben op het gebied van de levering van digitale goederen en diensten in en verduidelijken dus de zorgplicht die de leverancier heeft ten opzichte van de consument. Artikel 7 lid 3 van Richtlijn 2019/771 spreekt bijvoorbeeld over verplichte beveiligingsupdates voor een bepaalde periode. Deze Richtlijnen pogen consumenten te beschermen en maken duidelijk inbreuk op de contractvrijheid. Daarom zijn dergelijke richtlijnen niet geschikt voor b2b-relaties.

Ten tweede is er de norm voor bestuurdersaansprakelijkheid. Deze barrière is flink hoger.[24] In het geval van bestuurdersaansprakelijkheid moet een bestuurder van een vennootschap een persoonlijk ernstig verwijt kunnen worden gemaakt. Dit zijn zeer specifieke gevallen. Ook deze normen zijn in het geval van cybersecurity niet duidelijk. In de exceptionele gevallen waarin een wel ernstig persoonlijk verwijt kan worden aangetoond, zou dus sprake kunnen zijn van bestuurdersaansprakelijkheid.

Speciaal geval: 'Zorgplicht' bij uitsluiting van aansprakelijkheid in het contract

De kern van het contractuele aansprakelijkheidsrecht is dat partijen in Nederland in een b2b-relatie veel mogen afspreken en dus ook veel risico mogen uitsluiten.[25] Dit komt overeen met het rechtseconomische basisprincipe van contractvrijheid, zoals besproken in paragraaf 2, dat partijen in staat stelt hun voorkeuren te maximaliseren. In de b2b-context zullen naar onze verwachting leveranciers (doorgaans via hun algemene voorwaarden) elke vorm van aansprakelijkheid trachten uit te sluiten of te beperken (in juridisch jargon 'exonereren' genoemd).[26]

22. 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 Verbruggen en Wolters (2017). (EU) 2019/770 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten en (EU) 2019/771 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen, tot wijziging van Verordening (EU) 2017/2394 en Richtlijn 2009/22/EG, en tot intrekking van Richtlijn 1999/44/EG.
23. Kleine bedrijven, zoals ZZP'ers, zouden in sommige gevallen ook onder delen van de consumentenbescherming kunnen vallen volgens de zogenaamde reflexwerking, zoals onredelijk bezwarende bedingen in algemene voorwaarden. Dit onderzoek richt zich verder niet op deze aan de consumentenbescherming grenzende b2b-relaties.
24. De Hoge Raad maakt in het arrest Spaanse Villa (HR 23 november 2012, NJ 2013/302 , m.nt. P. van Schilfgaarde en JOR 2013/40 , m.nt. W.J.M. van Andel en K. Rutten (Spaanse Villa) een onderscheid 'tussen de regels van de 'gewone onrechtmatige daad' en de regels van externe bestuurdersaansprakelijkheid'. Zie ook Westenbroek (2016). 'In Hezemans Air en RCI/Kastrop overwoog de Hoge Raad vervolgens dat voor de 'ongewone' onrechtmatige daad van externe bestuurdersaansprakelijkheid een hoge drempel voor aansprakelijkheid in de vorm van de ernstigverwijtmaatstaf geldt die onder meer wordt gerechtvaardigd "door de omstandigheid dat ten opzichte van de wederpartij primair sprake is van handelingen van de rechtspersoon".' HR 5 september 2014, NJ 2015/21 , m.nt. P. van Schilfgaarde en JOR 2014/296 , m.nt. M.J. Kroeze (Hezemans Air) en HR 5 september 2014, NJ 2015/22 , m.nt. P. van Schilfgaarde en JOR 2014/325 , m.nt. Kortmann (RCI/Kastrop).
25. 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. Een beroep op een exoneratiebeding dat op zichzelf beschouwd geldig is, kan in zeer uitzonderlijke gevallen vanwege de omstandigheden van het geval naar maatstaven van redelijkheid en billijkheid onredelijk bewarend zijn. Relevante factoren hierbij zijn o.a. de zwaarte van de schuld maar ook de 'maatschappelijke positie en onderlinge verhouding van partijen'. In b2b-relaties gaat het om bedrijven onderling, zodat er veel minder ruimte zal zijn voor deze uitzonderingsgrond dan in b2c-relaties, zoals ook de zo-even genoemde uitspraak aantoont. Naar mate een onderneming meer het karakter van een consument heeft, bijvoorbeeld een ZZP'er, heeft deze een grotere kans om via de reflexwerking een beroep te doen op de bescherming die geldt voor consumenten.
26. Deze indicatie doen wij op basis van de gesproken experts en de logische 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 natuurlijk prikkel van de leverancier om de onderhandelingen tot sluiten van het contract te beginnen met een voorstel tot beperking en uitsluiting van de aansprakelijkheid. Zie ook Tjong Tjin Tai & Koops (2015); Blok (2010) en Graaf & Stuurman (2014); Tjong Tjin Tai (2013).

Maar ook exoneratie heeft een grens. In de kern komt het erop neer dat onaanvaardbaar geachte risico's niet via exoneratie uitgesloten kunnen worden. Binnen b2b-relaties is, naar de omstandigheden van het geval, schade die is ontstaan door *opzet en bewuste roekeloosheid* niet uit te sluiten, omdat zo'n beding strijdig is met de goede zeden.[27] Dit zou uitgelegd kunnen worden als de minimale zorgplicht van partijen.

Er is in zowel de wetenschap als in de rechtspraak grote onduidelijkheid over wat opzet of bewuste roekeloosheid inhoudt in het geval van aansprakelijkheid voor cybersecurityschade in b2b-relaties. Het volgende artificieel geconstrueerde voorbeeld wordt aangehaald in een CSR-advies over zorgplichten[28]:

> *"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."*

Dit voorbeeld handelt dus om een casus waar de leverancier zich jegens de afnemer op een exoneratieclausule zou willen beroepen ter vrijwaring van zijn contractuele aansprakelijkheid uit wanprestatie. Ervan uitgaande dat de houding van die leverancier als bewuste roekeloosheid kan worden gekwalificeerd, zou dit een casus kunnen zijn waarin de leverancier zich niet op de exoneratieclausule kan beroepen. Dit voorbeeld biedt ook nog ruimte voor verdere verduidelijking, bijvoorbeeld wanneer er aan de voorwaarde 'kennis is van onveiligheid' is voldaan. Uiteindelijk zal een rechter moeten toetsen of, gegeven de omstandigheden van het specifieke geval, er sprake is van opzet of roekeloosheid.

Het CSR advies biedt nog een tweede voorbeeld[29]:

> *"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."*[30]

Ook dit voorbeeld doet vragen rijzen. Zo rijst de vraag op welk moment een organisatie bewust gebruik maakt van sterk tekortschietende ICT. Er wordt door de CSR een aanzet tot meer duidelijkheid omtrent de grens van opzet/bewuste roekeloosheid, maar duidelijk wordt dat hier meer kennisontwikkeling voor nodig is. Beide voorbeelden maken wel duidelijk dat in de meeste gevallen de exoneratie inderdaad tot limitering of uitsluiting van de aansprakelijkheid van de leverancier zal leiden omdat er in de veel gevallen geen sprake is van opzet of bewuste roekeloosheid. In gevallen van extreme onvoorzichtigheid van de leverancier zou sprake kunnen zijn van bewuste roekeloosheid. Waar die precieze grens van de exoneratie ligt zal in de praktijk moeilijk te bepalen zijn. De rechter zal van geval tot geval moeten bepalen wat opzet of bewuste roekeloosheid inhoudt. Helaas blijft het onduidelijk waar de grens van de contractvrijheid ligt, aangezien op dit terrein niet veel jurisprudentie bestaat. Het uitgangspunt in het Nederlandse recht blijft echter dat bedrijven

27. Zie Asser/Sieburgh (2016), nr. 365.
28. Wolters en Jansen (2017), p.22
29. Wolters en Jansen (2017), p.13.
30. In dit geval zou de schade niet alleen door afnemers, maar ook door derden kunnen worden geleden. Daarbij rijst in de eerste plaats al de vraag of de exoneratie aan de derde kan worden tegengeworpen. De exoneratie is immers in het contract te vinden dat aan de derde onbekend is. Daarnaast zou wederom van bewuste roekeloosheid sprake kunnen zijn.

in een b2b-relatie zelf dienen te onderhandelen over de mate van aansprakelijkheid die zij willen aanvaarden. Contractuele exoneratieclausules zullen derhalve in beginsel door de rechter worden gerespecteerd. Dat komt uiteraard ook met de rechtseconomische beginselen overeen. Rechterlijk ingrijpen zou tot nadelige consequenties en welvaartsverlies kunnen leiden.

3.3 Juridische barrière 2: schade

Uiteraard moet er schade zijn om een mogelijkheid te hebben om deze te verhalen bij zowel wanprestatie als bestuurdersaansprakelijkheid. In de eerste plaats rijst de vraag waaruit de schade ten gevolge van een cyberonveiligheid precies bestaat. Er kan reële en kwantificeerbare schade zijn. Het bedrijf van de afnemer zou ten gevolge van de veiligheidsbreuk zijn activiteiten niet meer kunnen uitoefenen en dus inkomstenderving kunnen lijden.[31] Een voorbeeld: een afnemer kan gedurende een dag zijn e-mailsysteem niet gebruiken. Deze schade is reëel, maar wel vaak moeilijk kwantificeerbaar. De afnemer moet bijvoorbeeld de schade vaststellen van het niet kunnen gebruiken van het e-mailsysteem. Wellicht kan er die dag niet snel gereageerd worden op een inkomende aanvraag voor een product dat het bedrijf levert en ketst de deal af. Het is echter lastig vast te stellen of de deal wel gesloten zou zijn als men wel binnen een dag had kunnen reageren. In het geval van het niet kunnen gebruiken van een e-mailsysteem is er sprake van 'zuivere vermogensschade', die veelal moeilijker vast te stellen is dan zaakschade of letselschade. In het geval van zaakschade is er schade aan een zaak en bepalen de herstel- of vervangingskosten vaak de omvang van de schade. Dit zijn bijvoorbeeld de kosten van het opnieuw lakken van een auto als er krassen op een die auto zijn veroorzaakt. De kosten en mogelijkheden van het aantonen van de schade kunnen dus een barrière zijn.

Daarnaast kan een securitybreuk bij een afnemer ook reputatieschade veroorzaken. In het geval van reputatieschade is er vaak een groot verschil tussen werkelijke en gepercipieerde reputatieschade. Vaak is de reputatieschade niet of nauwelijks te kwantificeren.[32] 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 de daadwerkelijke schade laag of non-existent is. Materiële schade aan systemen en processen is in die zin het meest eenvoudig te kwantificeren doordat hier in algemene zin directe kosten gemaakt worden zoals bijvoorbeeld herstel van systemen en de inhuur van forensische IT diensten zoals bijvoorbeeld bij de ransomware-aanval op Maersk in juni 2017.

3.4 Juridische barrière 3: causaliteit

Er dient een causaal verband te zijn tussen de geschonden norm, in casu de cyberonveiligheid van de leverende partij, en de geleden schade van de afnemende partij in het geval van wanprestatie en bestuurdersaansprakelijkheid. Het aantonen van het bestaan van dit verband tussen cyberonveiligheid bij de leverancier en de geleden schade is wellicht een van de grootste barrières voor aansprakelijkheid. Zo achten Tjong Tjin Tai en Koops een "claim … niet kansrijk [is] aangezien hij zou moeten bewijzen dat er causaal verband is tussen

31. Vergelijk ook de zaak Ratonigid/Vasco (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."
32. Bisogni, Asghari en van Eeten (2017) & Nieuwesteeg en Faure (2018) geven een analyse en overzicht van het onderzoek dat is gedaan naar reputatieschade aan de hand van cybersecurityaanvallen zoals datalekken.

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."[33] Daarbij komt dat een claimende partij in het geval van cybersecurity tevens moet aantonen dat deze de beveiliging van de computersystemen geheel op orde heeft omdat hij anders zelf ook een aandeel kan hebben in de door hem geleden schade.[34] 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 hoge expertkosten gemoeid, maar dit is essentieel om te bepalen welk deel van de schade verhaald kan worden op de initieel leverende partij.[35]

3.5 Juridische barrière 4: bewijslast

De bewijslast ligt in beginsel bij de partij die de schade wil verhalen, in het geval van dit onderzoek hetzij via wanprestatie of via bestuurdersaansprakelijkheid, tenzij anders overeengekomen. Dit beginsel bemoeilijkt de mogelijkheid om schade te verhalen enorm omdat de afnemende partij niet in de IT-systemen van de leverende partij kan kijken en dus ook niet kan identificeren of de zorgplicht is geschonden en er een causaal verband is tussen de geschonden zorgplicht en de geleden schade. Probleem is bovendien dat, zoals werd aangegeven, op een leverancier vaak geen resultaatsverplichting rust tot het leveren van absolute cyberveiligheid. De afnemer zal dus dienen te bewijzen dat de leverancier de in het contract overeengekomen inspanningsverplichting niet correct is nagekomen. Bovendien is het gemakkelijk voor de leverende partij om dit bewijs te laten verdwijnen, door bijvoorbeeld logbestanden te verwijderen.[36] Hier kan wel het een en ander contractueel over afgesproken worden, bijvoorbeeld het vereiste om logbestanden voor een bepaalde periode te bewaren.

3.6 Economische barrière 1: onderhandelingsmacht

Naast juridische barrières zijn er ook economische barrières die een afnemende partij ervan weerhouden om verhaal te halen. We bespreken drie economische barrières.

Grote partijen zoals Google, Microsoft en Amazon sluiten in het algemeen aansprakelijkheid volledig uit en beperken ook hun zorgplicht. Hier valt, in ieder geval in de perceptie van MKB partijen, niet of nauwelijks over te onderhandelen.[37] Het is ook vaak niet mogelijk om naar een andere partij over te stappen omdat alle grote partijen dezelfde volledige exoneratiebedingen hanteren en er op het gebied van veel internetdiensten een *de facto* mono- of oligopolie is. Zo heeft Microsoft een *de facto* monopolie op tekstverwerkingsdiensten

33. Tjong Tjin Tai & Koops (2015). Vergelijk ook de zaak Ratonigid/Vasco (NL:RBAMS:2014:4888) waarin door het uitvoerige onderzoek van Fox-IT en de onderzoeksraad voor de veiligheid de verhaal houdende partij veel munitie had om causaliteit aan te tonen. Door deze (extern gefinancierde) bewijsvoering kon de rechtbank stellen dat elk van de drie vastgestelde beveiligingsgebreken een garantieschending (i.e. schending van de norm) opleverde.
34. Het leerstuk 'contributory negligence' wordt in het kader van cybersecurity onder andere besproken door Rustad & Koenig (2005).
35. EU (2019).
36. Het EU rapport 'Liability for Artificial Intelligence and other emerging digital technologies stelt een beleidsoptie voor om de bewijslast in een aantal gevallen te verschuiven (gebaseerd op verschillende Europese uitspraken en uit verschillende jurisdicties), onder andere op basis van 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. EU (2019), p 26.
37. Interview met Erik Rutkens; Interview met Maarten Wegdam.

met Microsoft Office voor veel organisaties.[38] Er kan zich ook een omgekeerde asymmetrie in onderhandelingsmacht voordoen, bijvoorbeeld als de overheid als afnemende partij met standaardvoorwaarden werkt. Een asymmetrie in onderhandelingsmacht zonder keuzevrijheid beperkt de contractvrijheid en geeft wellicht ook verkeerde prikkels ten aanzien van cybersecurity aan die partijen. Dit kan tot het bekende probleem van antiselectie (of averechtse selectie) leiden: door de marktmacht van bepaalde partijen kunnen zij inefficiënte contractuele clausules opleggen die daardoor in de markt overleven, hoewel zij inefficiënt zijn. Een voorbeeld: deze grote partijen kunnen de aansprakelijkheid voor de cybersecurity van hun producten uitsluiten, terwijl deze partijen wellicht ook tegen de laagste kosten cyberaanvallen kunnen voorkomen als zij deze aansprakelijkheid niet hadden uitgesloten. Het gevolg zou een grotere exoneratie kunnen zijn dan efficiënt is in een vrijemarkteconomie.

3.7 Economische barrière 2: toegang tot de rechter

Nadat er een initiële verdeling van de risico's is gemaakt via de onderhandeling tussen partijen is het natuurlijk van belang om te bezien in hoeverre het aansprakelijkheidsrecht het faciliteert om daadwerkelijk een claim in te dienen. Als de juridische kosten heel hoog zijn en de succesverwachting laag, dan kan er een situatie ontstaan waarbij *de jure* de aansprakelijkheid bij een leverende partij ligt, maar *de facto* bij de afnemende partij omdat deze te veel kosten moet maken om de schade te verhalen.[39] Als bijvoorbeeld een afnemer in Nederland een Amerikaanse leverancier mag aanklagen in Nederland in plaats van in bijvoorbeeld Amerika, dan kan die afnemer makkelijker verhaal halen. Verder onderzoek is nodig naar de toegankelijkheid van de rechter met betrekking tot relaties met grote internationale (veelal Amerikaanse) cloudleveranciers. Dit internationaal privaatrechtelijke onderzoek kan bijvoorbeeld analyseren of er een mogelijkheid is om aansprakelijkheidszaken voortvloeiend uit een contractuele relatie tussen een Nederlandse partij en grote Amerikaanse cloudleveranciers ook in Nederland te beslechten.

3.8 Economische barrière 3: faillissement

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 maximumclaim opgerekt door het maximale bedrag dat een verzekering kan uitkeren. Partijen richten soms strategisch aparte B.V.'s op voor risicovolle cybersecurityprojecten, die vervolgens kunnen 'klappen' als er teveel schade geclaimd dreigt te worden.

38. 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.
39. Dit heet 'rationele apathie' en kan vooral relevant zijn bij gespreide schade, waar de totale schade dan heel groot kan zijn, maar de schade voor individuele partijen te klein kan zijn om individuele zaken te starten.

4. Omschrijving en schematische analyse van de vier scenario's

In deze sectie omschrijven we kort vier scenario's als gevolg van digitale onveiligheid met voorbeelden van eventuele schade. We gaan uit van claims met betrekking tot 1.) reputatieschade, 2.) 'materiële' schade aan systemen en processen door digitale onveiligheid en 3.) schade ten gevolge van bedrijfsonderbreking. Deze vormen van schade relateren we vervolgens aan de door ons geobserveerde barrières om schade te verhalen.

4.1 Omschrijving van de vier scenario's

Scenario 1

Het eerste voorval betreft een b2b-relatie tussen 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.

Scenario 2

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 gedurende een week de Nederlandse MKB-er 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.[40]

Scenario 3

In dit voorbeeld volgen we een cybersecurityleverancier die zaken doet 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 al haar andere klanten.[41]

Scenario 4

Dit scenario betreft een situatie waarin twee kleine bedrijven een lange zakelijke relatie hebben waarin cybersecurityproducten worden geleverd. Er is

40. 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).
41. Dit scenario is geïnspireerd op de DigiNotaraffaire, waarbij een hacker inbrak bij het bedrijf DigiNotar, dat beveiligingscertificaten verzorgde, zie bijvoorbeeld van der Meulen (2013).

een duidelijke norm vastgesteld en deze norm is duidelijk geschonden. De leverancier heeft in de overeenkomst aansprakelijkheid niet uitgesloten of beperkt en de afnemer lijdt duidelijk kwantificeerbare schade. Ook heeft de leverancier voldoende middelen om de schade te vergoeden.

4.2 Koppeling scenario's aan rechtseconomische barrières voor verhaal

In onderstaande tabel worden de juridische en economische barrières gekoppeld aan de scenario's. Opgemerkt moet worden dat de schattingen van de effecten zijn gemaakt voor het indicatieve doel van het overzicht, en gericht zijn op het weerspiegelen van de opgestelde scenario's en de rechtseconomische analyse. Het is echter geen strikte kwantificering van deze effecten. De verwachtingswaarde die aangeeft of het aansprakelijk stellen een afnemende partij iets oplevert, wordt ook meegenomen. Deze formuleren we als volgt:

*Verwachtingswaarde = kans op succes * schadevergoeding – niet verhaalbare proceskosten*

Tabel 1 koppelt de zoëven geschetste scenario's aan de in Sectie 3 geïdentificeerde rechtseconomische barrières. Belangrijk voor de interpretatie van de tabel is dat als één factor een barrière vormt, het hele schadeverhaal niet kan slagen. Als bijvoorbeeld een leverende partij failliet is, kan er uiteraard geen schade verhaald worden, maar als de schade niet kan worden aangetoond, dan kan er natuurlijk ook geen schade verhaald worden. We zien dat in de drie verschillende scenario's een aanzienlijke tot zeer grote kans is dat één of meerdere barrières niet geslecht kunnen worden. Per scenario verschillen de barrières die naar verwachting de grootste obstakels vormen.

In het geval van Scenario 1 is het aantonen van daadwerkelijke reputatieschade en het vervolgens aantonen van de causaliteit tussen het ontstaan van de schade en de geschonden norm de grootste barrière. Verschillende zeer grondige en tijdrovende academische studies kunnen vaak

Tabel 1: koppeling scenario's en rechtseconomische barrières voor verhaal

	Hoogte van barrière (meer • is hoger):			
Barrières	**Scenario 1 Reputatieschade**	**Scenario 2 Bedrijfs-onderbreking**	**Scenario 3 Materiële schade aan systemen en processen**	**Scenario 4 Kleine b2b-partijen met duidelijke norm en schade**
Juridisch				
Geschonden zorgplicht	• •	• • • (zeer hoog door exoneratie)	•	•
Schade	• • •	• •	•	•
Causaliteit	• • •	•	•	•
Bewijslast	• • •	• • •	• •	•
Economisch				
Asymmetrie in onderhandelingsmacht	•	• • •	• • (omgekeerd, overheid heeft vaak meer macht)	•
Toegang tot de rechter	•	• • •	•	•
Faillissement	• •	•	• • •	•
Verwachtings-waarde juridische procedure	Lage verwachtings-waarde succes door vaststelling schade en causaliteit	Zeer lage verwachtings-waarde door exoneratie, toegang tot de rechter en bewijslast	Lage verwachtings-waarde door grote kans faillissement.	Lage kans op proces, juist door hoge verwachtingswaarde

geen langdurige reputatieschade aantonen bij grote bedrijven die slachtoffer zijn geworden van zeer omvangrijke cyberaanvallen.[42]

In het geval van Scenario 2 gooit primair de uitsluiting van de aansprakelijkheid roet in het eten. Door de grote verschillen in onderhandelingsmacht tussen partijen als de internationale leverancier van clouddiensten en een Nederlandse MKB-er ontstaat er vaak geen ruimte om enige vorm van aansprakelijkheid te behouden bij de leverende partij.[43] Zoals we hebben geconstateerd in sectie 3.1 moet volgens Nederlands recht de leverende partij opzettelijk of door bewuste roekeloosheid een norm hebben overschreden, wil een beroep op exoneratie niet slagen. De Nederlandse MKB-er moet dan bewijzen dat dat de leverancier in zijn servers in de Amerikaanse westkust opzettelijk of door middel van bewuste roekeloosheid de veiligheid van zijn systemen niet op orde had. De MKB-er heeft geen toegang tot de interne systemen van de cloudleverancier. Opzet of bewuste roekeloosheid trachten te bewijzen kost dus veel tijd en geld. De kans bestaat dat de Nederlandse partij dit moet doen bij de Amerikaanse rechter, waardoor de kosten voor verhaal verder stijgen. Al met al heeft Scenario 2 een zeer kleine kans van slagen en zijn de kosten van een procedure zeer hoog.

In het geval van Scenario 3 weerhoudt een mogelijk faillissement van de leverende partij ons van een positief oordeel omtrent kansrijkheid van de verhaalbaarheid van de schade. Het scenario is zo geconstrueerd dat er overduidelijk schade is ten gevolge van een normoverschrijding. Er is immers sprake van opzettelijk handelen. Desalniettemin is er een relatief lage verwachtingswaarde omdat in een dergelijk geval de kans op faillissement van de leverancier groot is, enerzijds omdat andere klanten van de leverancier ook schade hebben en zullen claimen waardoor de kosten hoger worden en anderzijds omdat het vertrouwen in de leverancier een dusdanige deuk heeft opgelopen waardoor toekomstige inkomsten die de kosten kunnen dragen onwaarschijnlijk zijn. In het geval van Scenario 3 kan een claim op basis van bestuurdersaansprakelijkheid tevens zinvol zijn, en de maximale waarde van die claim is dan gebaseerd op het vermogen van de bestuurder en eventueel het verzekerde bedrag van zijn of haar bestuurdersaansprakelijkheidsverzekering, voor zover die verzekering cybersecurity niet uitsluit.[44]

In het geval van Scenario 4 is er een 'ideaal' scenario geschetst waarin partijen onderling heldere afspraken hebben gemaakt. Er is een duidelijke geschonden norm, kwantificeerbare schade en een verband tussen de geschonden norm en de schade. Ook heeft de leverancier voldoende middelen in kas om de schade te vergoeden. Juist omdat er in dit geval lage barrières tot verhaal zijn ligt het in de lijn van verwachting dat niet geprocedeerd zal worden. De leverancier heeft hier namelijk geen enkel belang bij een rechtszaak en zal de schade gelijk willen vergoeden. Ten eerste houdt een directe vergoeding van de schade door de leverancier de (lange) relatie met de afnemer goed. Bovendien zou de leverancier bijzonder zwak staan als de afnemer een zaak zou starten en zou deze uiteindelijk toch gedwongen worden om de schade te vergoeden. Dit scenario illustreert de voordelen van duidelijke afspraken in contracten met betrekking tot onder andere de zorgplicht. Als het duidelijk is dat een afnemer verhaal kan halen bij een leverancier verkleint dit de kans dat tijdrovende en maatschappelijk kostbare juridische procedures gevolgd dienen te worden.

Uit zoëven beschreven analyse van de vier scenario's kan worden afgeleid dat er weinig gevallen met een simpele aansprakelijkheidsroute zullen zijn die een hoge verwachtingswaarde zullen hebben. Zelfs als de verwachtingswaarde

42. Bisogni, Asghari en van Eeten (2017) en Nieuwesteeg en Faure (2018) geven een analyse en overzicht van het onderzoek dat is gedaan naar reputatieschade aan de hand van cybersecurityaanvallen zoals datalekken. Vaak kunnen er uiteraard wel directe kosten aangetoond worden zoals de kosten van forensisch onderzoek en het herstel van data.
43. Interview met Erik Rutkens; Interview met Maarten Wegdam.
44. Er moet dan sprake zijn van een persoonlijk ernstig verwijt. Zie onder andere Olden (2015); Westenbroek (2016) en het arrest Ontvanger/Roelofsen (HR 8 december 2006, NJ 2006/659 (Ontvanger/Roelofsen).

hoog is omdat er allereerst directe schade is geleden die makkelijk te bewijzen is en vervolgens aansprakelijkheid niet geëxonereerd is, dan is de schade nog immer gemaximeerd tot de waarde en de eventuele cybersecurityverzekering van het bedrijf, of eventueel het vermogen en de eventuele bestuurdersaansprakelijkheidsverzekering.

5. Conclusie en aanbevelingen voor verder onderzoek naar beleidsopties

Deze studie onderzocht of het Nederlandse aansprakelijkheidsregime voldoende mogelijkheden biedt om in een b2b-relatie cybersecurityschade te verhalen.

Onze conclusie is dat het mes van het aansprakelijkheidsregime bot is. Dit heeft een simpele reden. De juridische en economische barrières voor verhaal zijn dermate groot dat in verreweg de meeste gevallen verhaal niet loont.[45] Dat zou de reden kunnen zijn dat er voor zover wij weten geen rechtszaken hebben plaatsgevonden in een b2b-relatie waarbij gebrekkige cybersecurity bij de leverancier van producten of diensten op het gebied van cybersecurity schade veroorzaakte bij de afnemer.

Het stimuleren van verhaal zal een uitdagende opgave zijn als men de contractvrijheid zoveel mogelijk in stand wil houden, wat vanuit rechtseconomisch oogpunt verstandig is.[46] Desalniettemin zijn er wel beleidsopties mogelijk om die barrières te verlagen en derhalve doen wij een aantal aanbevelingen. De contouren voor deze beleidsopties die wij schetsen zijn geen 'panacea'. Mogelijke (neven)effecten dienen in de specifieke context geanalyseerd te worden voordat men tot implementatie overgaat.

1. **Vergroot duidelijkheid over de contractuele zorgplicht.** Wat kan hiermee bereikt worden? Meer duidelijkheid over de grens van de zorgplicht verlaagt de barrière tot verhaal, omdat onzekerheid weggenomen wordt of een partij nu wel of niet zijn verplichtingen heeft geschonden. *Toelichting:* De overheid kan partijen assisteren om de contractuele zorgplicht verduidelijken. Zij zou hierin dus een informerende rol kunnen innemen (bijvoorbeeld advies over normen in contracten). Wat is een contractuele zorgplicht? In elk contract heeft de leverancier (impliciet of expliciet) een zorgplicht. Dit is een bepaald niveau van cybersecurity die de leverancier moet leveren. Soms is deze uitgebreid, bijvoorbeeld wanneer expliciet

45. De mogelijkheden die een organisatie heeft in een b2b-relatie om het huidige civiele aansprakelijkheidsrecht te kunnen inzetten wanneer zij schade lijdt door digitale onveiligheid worden uiteraard sterk bepaald door hetgeen een organisatie in een contract met een afnemende partij heeft afgesproken.
46. Er geldt in Nederland een hoge mate van contractvrijheid. Dat is vanuit rechtseconomisch oogpunt wenselijk, maar dat betekent wel dat als partijen aansprakelijkheid beperken of uitsluiten, de mogelijkheden tot verhaal zeer sterk worden beperkt.

wordt gesproken van het patchen en updaten van het geleverde IT-systeem. Soms is deze beperkt, bijvoorbeeld in het geval van uitsluiten van aansprakelijkheid, dan is deze beperkt tot opzet en bewuste roekeloosheid, maar de meningen verschillen over wat opzet of bewuste roekeloosheid precies is omdat een rechter zich daar nog niet over heeft uitgesproken. De zorgplicht kan verduidelijkt worden door bijvoorbeeld te stimuleren dat cybersecuritystandaarden opgenomen worden in contracten. Men zou zelfs onderling kunnen afspreken in contracten wat men onder opzet of bewuste roekeloosheid verstaat. Standaarden, bijvoorbeeld in de vorm van keurmerken, hebben ook zelf weer nadelen, die voor deze specifieke context verder onderzocht dienen te worden. Zo moet men standaarden, zeker als deze specifiek zijn, continu onderhouden en aanpassen aan de veranderlijke natuur van cybersecurity en moet de partij die de standaarden vaststelt snel toegang hebben tot de informatie op basis waarvan bepaald kan worden of standaarden aangepast moeten worden.

2. **Stimuleer vergemakkelijken van bewijsvoering (en onderzoek verzwaren verweerplicht of omkeren bewijslast).** Wat kan hiermee bereikt worden? Een verzwaarde motiveringsplicht[47], zoals de verplichting tot het bewaren van de logs van een cybersecurityincident of omkering van de bewijslast voor de leverende partij zouden de barrières tot verhaal kunnen verlagen, omdat het makkelijker wordt te bewijzen dat een leverancier schade veroorzaakt. Dit zal wel verder onderzocht moeten worden, omdat dit ingrijpt in het contractenrecht. 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. *Toelichting:* 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 afnemende partij niet de IT-systemen van de leverende partij kan analyseren en dus ook niet kan identificeren of de zorgplicht geschonden is en of er een causaal verband is tussen de geschonden zorgplicht en de geleden schade. Vanuit rechtseconomisch perspectief zou er maatschappelijke meerwaarde kunnen ontstaan als degene die tegen de laagste kosten de informatie kan leveren, de bewijslast krijgt opgelegd. De leverende partij kan bijvoorbeeld door logs waarschijnlijk beter aantonen dat bepaalde stappen wél gezet zijn, dan dat de afnemende partij kan aantonen dat die stappen niet zijn gezet.

Verder onderzochten wij of het Nederlandse aansprakelijkheidsregime voldoende prikkels voor cybersecurity voor partijen bevat. Binnen een b2b-relatie is de contractvrijheid niet problematisch, tenzij er sprake is van bijvoorbeeld een zodanig verschil in onderhandelingsmacht dat de sterke partij hiervan misbruik kan maken. Daartoe strekken ook een aantal aanbevelingen tot verder onderzoek, zoals:

3. **Stimuleer of dwing meerdere aansprakelijkheidsopties af bij grote partijen.** Wat kan hiermee bereikt worden? Dit kan de keuzeopties 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. *Toelichting:* Grote partijen zoals Google, Microsoft en Amazon sluiten in het algemeen aansprakelijkheid volledig uit. Dit zou kunnen worden opgevat als een beperking van de effectieve contractvrijheid van kleine partijen om met deze grote partijen zaken te doen. We 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. Dit om te voorkomen

47. Artsen hebben bijvoorbeeld een verzwaarde motiveringsplicht voor medische fouten, zie o.a. HR 15.6.2007 NJ 2007 nr. 335, VR 2007 nr. 134 met noot Van Wassenaer onder nr. 133, JA 2007 nr. 144 met noot Van der Meer, RAV 2007 nr. 45.

dat er een grotere exoneratie zou kunnen zijn dan efficiënt is in een vrije markteconomie (zie sectie 3.5). Hieraan gerelateerd is verder onderzoek naar consumentenbescherming die ook zou kunnen doorwerken naar kleine ondernemers (reflexwerking). In Nederland is er immers al veel dwingend recht voor consumenten. Met zou dus ook kunnen onderzoeken in hoeverre deze reflexwerking kan gelden of al geldt voor b2b-situaties waarin er grote verschillen in macht, informatie en andere facetten van de onderhandeling bestaan.

4. **Onderzoek de toegang tot de rechter van? en vergroot deze waar mogelijk.** Wat kan hiermee bereikt worden? Als een afnemer in Nederland een internationale leverancier mag aanklagen in plaats van in bijvoorbeeld Amerika kan een partij gemakkelijker verhaal halen. *Toelichting:* Verder onderzoek is nodig naar de toegankelijkheid van de rechter met betrekking tot relaties met grote internationale (veelal Amerikaanse) cloudleveranciers. Dit internationaal privaatrechtelijke onderzoek kan bijvoorbeeld analyseren of er een mogelijkheid is om aansprakelijkheidszaken voortvloeiend uit een contractuele relatie tussen een Nederlandse partij en grote Amerikaanse cloudleveranciers ook in Nederland te beslechten. Een alternatieve beleidsroute is het stimuleren van alternative dispute resolution (ADR). Dat is vaak goedkoper, eenvoudiger en sneller en kan ook gebeuren zonder noodzakelijke tussenkomst van een advocaat. Bijkomend voordeel is dat reputatieschade uitblijft en dat zelfs claims met een relatief lage verwachte opbrengst misschien toch gebracht kunnen worden als ze via mediation tot een redelijke oplossing zouden kunnen leiden.

Zelfs als men de beleidsopties doorvoert zal het stimuleren van verhaal een uitdagende opgave zijn als men de contractvrijheid zoveel mogelijk in stand wil houden. De vraag is of het aansprakelijkheidsregime in een b2b-relatie het meest effectieve middel is om schade te verhalen en prikkels goed te leggen. Men zou ook alternatieven kunnen onderzoeken en/of stimuleren, zoals het risico afdekken. Voor een afnemende partij kan een cyberverzekering of een risicospreidingsovereenkomst een laagdrempelig alternatief zijn voor het niet beperken of uitsluiten van de aansprakelijkheid bij de leverancier.

5. **Alternatief: stimuleer het afdekken van het risico door afnemende partijen.** Wat kan hiermee bereikt worden? Voor een afnemende partij kan een cyberverzekering of een risicospreidingsovereenkomst een laagdrempelig alternatief zijn voor aansprakelijkheid van de leverancier die bemoeilijkt wordt door de grote juridische en economische barrières voor verhaal. *Toelichting:* Dit geldt met name als de premie van de cyberverzekering een accurate weerspiegeling is van het schaderisico dat wordt overdragen aan de verzekeraar. Hiervoor is noodzakelijk dat de cyberverzekeringsmarkt verder ontwikkelt en daarvoor is verder onderzoek nodig.[48] Voor een leverende partij kan een cyberverzekering meerwaarde hebben doordat een van de belangrijkste dekkingselementen 'incident response' is.[49] Dat kan de kans dat het bedrijf wordt geconfronteerd met aansprakelijkheidsclaim verkleinen (incident response heeft namelijk een mitigerend effect op de schade richting afnemende partijen).

48. In een volwassen cyberverzekeringsmarkt zullen verzekeraars ook preventie bij partijen gaan stimuleren voor zover de besparing op toekomstige claims vanuit het oogpunt van de verzekeraar lager is dan de kosten van preventie. Dit is nu nog onvoldoende het geval.
49. Incidentrespons is een georganiseerde aanpak voor het aanpakken en beheren 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.

6. Gesproken experts

De volgende experts zijn gesproken ter kleuring van het onderzoek. De analyse en ingenomen standpunten van het onderzoek berusten echter exclusief bij de auteurs en behoren niet toe aan de gesproken experts tenzij deze experts letterlijk geciteerd zijn in het onderzoek.

Dhr. Maarten van Wieren
Managing Director bij Aon (12 december 2019)

Mw. Nynke Brouwer
Advocaat bij Dirkzwager en promovenda aan de Radboud Universiteit Nijmegen (18 december 2019)

Dhr. Maarten Wegdam
CEO bij InnoValor Software (18 december 2019)

Dhr. Erik Rutkens
Founder van Qbit Cyber Security (19 december 2019)

Dhr. Pieter Wolters
Onderzoeker bij de Radboud Universiteit Nijmegen (24 december 2019)

Bijlage 1 – Aansprakelijkheid en maatschappelijke schade

Risico op maatschappelijke schade

In de contractuele relatie tussen afnemer en leverancier kunnen specifieke afspraken worden gemaakt over het door de leverancier te bieden niveau van cybersecurity en de risicoverdeling tussen partijen wanneer onverhoopt ook schade zou optreden. Die afspraken tussen partijen aangaande de door de leverancier uit te voeren investeringen in cybersecurity en de risicoallocatie zullen uiteraard ook hun weerslag hebben op de door de afnemer te betalen prijs. Echter, aangezien het hier om een b2b-relatie gaat kan er doorgaans van worden uitgegaan dat partijen conform hun specifieke preferenties in staat zijn optimale afspraken te maken via het contract. Juist omdat die mogelijkheid van ex ante contracteren niet voor derden bestaat, is de zaak complexer wanneer de schade (door gebrekkige cybersecurity) niet alleen de afnemer raakt, maar ook derden. Juist omdat die derden zich niet op het contract kunnen beroepen (dat door de relativiteit van contracten alleen de partijen bindt) dienen zij in beginsel de weg van de aansprakelijkheid uit onrechtmatige daad te bewandelen, een weg waarop zich vele voetangels en klemmen kunnen bevinden.

Deze andersoortige situatie ontstaat wanneer er naast schade bij een afnemende partij ook maatschappelijke schade ontstaat ten gevolge van onvoldoende niveau van cybersecurity bij de leverende partij én die maatschappelijke schade niet gemakkelijk kan worden verhaald op de leverende partij. Dit kan het geval zijn wanneer er situatie is waarbij (ook) derden, dat wil zeggen niet (alleen) de afnemers schade lijden. Dit zou uit zeer concrete schade voor bepaalde individuele derden kunnen bestaan die nadeel ondervinden van de veiligheidsbreuk bij de afnemer. Maar de maatschappelijke schade kan ook veel breder (en potentieel groter) zijn. Daarbij kan bijvoorbeeld worden gedacht aan:

- Het verlies van vertrouwen in IT-producten & diensten door derden. Als een bank bijvoorbeeld voor zijn internetbankierdiensten zakendoet met een cybersecurityleverancier en deze de beveiliging niet goed op orde heeft met schade bij diezelfde bank als gevolg, kan ook bij klanten van andere banken het vertrouwen in betaaldiensten verminderen. Voor de leverancier is dit reputatieschade, in het geval van schade van de derde (de andere bank waar bijvoorbeeld ook klanten weglopen) gaat dit om een algemeen verlies van vertrouwen waardoor niet meer gebruik gemaakt wordt van de product of dienst.
- Systeemrisico. Cybersecurityrisico's lijken te correleren en daardoor kan een suboptimaal cybersecurityniveau bij de ene partij leiden tot schade bij vele andere partijen. Zo zorgde malware in een boekhoudprogramma van het Oekraïense bedrijf Intellect Service er in juni 2017 voor dat een grootschalige ransomware-aanval zich kon verspreiden onder honderden

bedrijven.[50] Hier kan ook sprake zijn van schade bij derden als er geen contract is tussen de schadelijder en de organisatie die suboptimale cyberveiligheid had waardoor er schade bij de schadelijder kon ontstaan.

In een situatie waarin ook derden schade lijden geeft een verdeling van de risico's tussen een afnemende en een leverende partij onvoldoende prikkels aan de leverende partij om een redelijk niveau van cybersecurity te hanteren. Immers, de schade die de leverende partij veroorzaakt aan derden doet de leverende partij zelf geen pijn (het is een zogenaamde 'negatief extern effect') en rechtvaardigt voor deze partij dus geen extra investeringen in cybersecurity om die schade in toekomstige gevallen te beperken.[51] Vanuit maatschappelijk oogpunt is het echter wèl wenselijk dat deze partij rekening houdt met de schade (het externe effect 'internaliseert'), om zo geprikkeld te worden die voorzorgsmaatregelen te nemen die minder kosten dan ze opleveren in de vorm van een daling van de verwachte schade.

Barrières voor derden om schade te verhalen

We zullen in deze bijlage kort ingaan op de barrières voor derden om schade te verhalen. Een uitvoerige beschouwing van deze materiële en praktische voorwaarden voor aansprakelijkheid valt buiten de reikwijdte van dit onderzoek, daar dit onderzoek zich primair richt op het verhalen van schade binnen een b2b-relatie en niet op schadeverhaal door derden. De kern van ons betoog luidt dat in veel gevallen de zo-even beschreven barrières voor derden hoger zijn dan voor afnemende partijen. We lichten een aantal voorbeelden van die verhoogde barrières nader toe. Voor de goede orde: wij gaan er nu van uit dat deze vordering uit onrechtmatige daad wordt ingesteld door een derde die niet in een contractuele relatie staat met de leverancier.

Zorgplicht

In sectie 3.1 werd toegelicht dat het complex kan zijn om te bepalen wat de exacte zorgstandaard is bij cybersecurity en dat het ook lastig kan zijn aan te tonen dat deze door de leverancier werd geschonden. Hoewel, zoals aangegeven, er wel bepaalde cybersecurity standaarden bestaan, zoals ISO-normeringen, gaven de respondenten tijdens de interviews toch aan dat niet gesproken kan worden van een glasheldere en onbetwiste norm inzake cybersecurity.[52] De reden is dat het niveau van de te leveren cybersecurity afhankelijk is van hetgeen ter zake contractueel tussen leverancier en afnemer is afgesproken. Dit vergroot de barrière om schade te verhalen. Een derde dient immers eerst zelf aan te tonen wat de zorgplicht inhoudt en dient daarnaast ook te bewijzen dat die zorgplicht is geschonden.

Schade en causaliteit

In de tweede plaats rijst voor derden vaak de vraag welke schade zij exact hebben geleden. Zelfs wanneer sprake van vergoedbare schade is, moet de derde ook een oorzakelijk verband aantonen tussen de gedraging van de leverancier en de door de derde geleden schade. Het bewijs van die causaliteit kan ook complex zijn, wellicht complexer dan het bewijzen van causaliteit van gedragingen van de leverancier en schade bij een afnemer. Het is bijvoorbeeld gemakkelijker om het oorzakelijke verband tussen de gedragingen van de leverende partij en de schade bij een afnemende partij vast te stellen dan een oorzakelijk verband tussen de gedragingen van de leverende partij en de schade bij een derde partij, die zich wellicht op een totaal ander continent bevindt.

Verspreiding schade

Er zijn ook praktische redenen zijn waarom het juist voor derden lastig kan zijn een aansprakelijk-

50. Voor informatie, zie bijvoorbeeld: Lawrence en Robertson (2017) <https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry-global-hack-could-have-been-much-much-worse> (geraadpleegd 2 januari 2020); Verschuren (2017) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> (geraadpleegd 2 januari 2020); Sedee (2017) <https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740)> (geraadpleegd 2 januari 2020).
51. Dit kan natuurlijk anders zijn als daardoor de goede naam van de leverende partij wordt geschaad.
52. Alle gesproken experts gaven dit aan.

heidsvordering in te stellen.[53] In sommige gevallen kan de schade zeer wijdverspreid zijn. Een enkele derde lijdt dan een vrij geringe schade (waardoor die te geringe prikkels zal hebben om te vorderen), maar de totale maatschappelijke schade kan zeer groot zijn. Die praktische problemen worden uiteraard nog groter wanneer de schadelijders niet slechts in één land gelokaliseerd zijn, maar verspreid over vele landen. Het recht kan in sommige gevallen slachtoffers te hulp komen, bijvoorbeeld door een groepsvordering (collectieve actie) mogelijk te maken.[54] Maar juist in gevallen waarin de schadelijders zich in verschillende landen bevinden, is dat weer complex.

Faillissement

Daarnaast geldt bij elke aansprakelijkheidsvordering dat de schadeloosstelling altijd gemaximeerd is tot de draagkracht van de partij die de schade dient te vergoeden. Is de schade hoger, dan rijst een solvabiliteitsprobleem. Ten gevolge van insolventie vindt niet alleen ondercompensatie van slachtoffers plaats, maar zal de leverancier ook te geringe prikkels hebben tot investering in optimale cybersecurity. Als er veel derden schade lijden, bijvoorbeeld als gevolg van een wereldwijde ransomware-aanval, dan is de kans groter dat de schade niet verhaald kan worden wegens insolventie van de leverancier.

Samenvattend zullen de barrières voor het slagen van een aansprakelijkheidsvordering voor derden in veel situaties nog hoger zijn dan in het geval van een contractuele relatie. Wanneer derden schade lijden en er dus sprake is van maatschappelijke schade, zullen leveranciers niet via het aansprakelijkheidsrecht tot optimale investeringen in cybersecurity gedwongen kunnen worden. Daarom lijkt het er op dit ogenblik op dat het aansprakelijkheidsrecht, gegeven de vele barrières, onvoldoende mogelijkheden biedt om, gegeven de specifieke eigenschappen van cybersecurity, het tweede genoemde doel, namelijk het internaliseren van maatschappelijke schade door de schadeveroorzakende partij, te realiseren. Er kan dus een probleem rijzen wanneer derden ook schade lijden en die trachten te verhalen op de leverende partij.[55] De barrières voor derden zijn in veel gevallen hoger dan voor een partijen die een relatie hebben met de leverancier. Precies die door derden geleden schade kan ook maatschappelijke schade vormen, maar deze bevindt zich buiten de reikwijdte van het rapport en daarvoor is verder onderzoek noodzakelijk.[56]

53. De eerdergenoemde voorwaarden zijn zogeheten materieelrechtelijk van aard.
54. Sinds 1 januari 2020 is bijvoorbeeld de Wet afwikkeling massaschade in collectieve actie in werking getreden.
55. Als derden hun schade trachten te verhalen op de afnemende partij van de leverende partij (die weer hun leverende partij) is dan doet er een situatie zich van verhaal in de zin van een b2b-relatie die de hoofdmoot is van dit rapport.
56. Verder onderzoek zou zich bijvoorbeeld kunnen richten op het verkleinen van barrières voor verhaal voor derden. De precieze barrières voor derden bij het verhalen van schade als gevolg van digitale onveiligheid zouden beter in kaart kunnen worden gebracht. Vervolgens kan worden onderzocht hoe de overheid deze belemmeringen kan wegnemen, bijvoorbeeld door het stimuleren van het coördineren van groepsvorderingen bij een wijdverspreide cyberaanval als gevolg van de digitale onveiligheid van één of een beperkt aantal partijen. Een nadeel van het stimuleren van verhaalsmogelijkheden door derden is dat, als de mogelijkheid te ver doorschiet, het innovatie kan beperken bij de leverancier omdat het aansprakelijkheidsrisico hoger wordt. Bovendien wordt ook middels het stimuleren van een rechtszaak de facto ingegrepen in de contractvrijheid, dat, zoals geschetst in de sectie 2, ook grote nadelen heeft. Tevens zou men kunnen onderzoeken in welke mate een sterke rechtszaak waarbij ook derden schade hebben geleden gestimuleerd zou kunnen worden. Als een bedrijf met cyberonveiligheid grote maatschappelijke schade veroorzaakt, maar derden moeite hebben om verhaal te zoeken wegens hoge kosten, dan kan de overheid bedrijven die een b2b-relatie hebben met de schadeveroorzaker stimuleren om deze schadeveroorzaker aansprakelijk te stellen zodat er in ieder geval een deel van de schade geïnternaliseerd wordt. Bovendien kan een succesvolle rechtszaak ook de barrières voor verhaal in andere zaken tegen dezelfde veroorzaker verlagen. Of, hoe en in welke gevallen een stimulering van een inhoudelijk sterke rechtszaak kan werken, kan onderwerp van vervolgonderzoek zijn.

Literatuur

Asser/Hartkamp & Sieburgh (2015), '6-IV De Verbintenis uit de wet', (Kluwer: Alphen aan den Rijn, 14e druk), nr. 10 en 12.

Asser/Sieburgh (2016), '6-I De verbintenis in het algemeen, eerste gedeelte', (Kluwer: Alphen aan den Rijn, 14e druk), nr. 365.

Bisogni, Asghari & Van Eeten (2017), 'Estimating the size of the iceberg from its tip- An investigation into unreported data breach notifications', (presented at the sixteenth Annual Workshop on the Economics of Information Security, La Jolla, 26-27 June 2017).

Blok (red.) (2010), 'Overeenkomsten inzake informatietechnologie', (SDU Uitgevers: Den Haag), pp. 112-113.

Blomquist, (1988), 'Goals. Means, and Problems for Modern Tort Law: A Reply to Professor Priest', Valparaiso University Law Review.

EU (2019), 'Liability for Artificial Intelligence and other emerging digital technologies.' From https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608, geraadpleegd 11 maart 2020.

Graaf & Stuurman (2014), 'ICT-contracten', in: Van der Hof e.a. (2014) 'Recht en Computer', p. 79.

Lindenbergh (2014), 'Monografieen BW B34 - Schadevergoeding Algemeen deel 1' (Kluwer: Alphen aan de Rijn, 4e druk).

Nieuwesteeg (2018), 'The Law and Economics of Cyber Security', (Delex: Amsterdam).

Nieuwesteeg & Faure (2018), 'An Analysis of the Effectiveness of the EU Data Breach Notification Law', Computer Law & Security Review.

Olden (2015), 'Koester de maatstaf "ernstig verwijt": beter hebben we niet', Ondernemingsrecht.

Pfleeger (2003), 'Data security' in: Ralston, Reilly & Hemmendinger (red), 'Encyclopedia of Computer Science', (Wiley: New Jersey, 4e editie).

Priest (1988), 'Satisfying the Multiple Goals of Tort Law', Valparaiso University Law Review.

Rustad & Koenig (2005), 'The Tort of Negligent Enablement of Cybercrime', Berkeley Technology Law Journal.

Tjong Tjin Tai (2013), 'Zorgplichten van banken tegen DDoS-aanvallen', Nederlands Juristenblad.

Tjong Tjin Tai & Koops (2015), 'Zorgplichten tegen cybercrime', Nederlands Juristenblad.

Van der Meulen (2013), 'DigiNotar: Dissecting the First Dutch Digital Disaster', Journal of Strategic Security.

Verbruggen & Wolters. (2017), 'Consument en cybersecurity: Een agenda voor Europese harmonisatie van zorgplichten', Tijdschrift voor consumentenrecht & handelspraktijken.

Westbroek (2016), 'Externe bestuurdersaansprakelijkheid, rechtspersoonlijkheid en toerekening', Ondernemingsrecht.

Wolters en Jansen (2017), 'Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity', Cyber Security Raad.

Erasmus University Rotterdam
Centre for the Law and Economics of Cyber Security

Visiting address: Burgemeester Oudlaan 50

Correspondence address: Postbus 1738
3000 DR Rotterdam
the Netherlands
clecs@eur.nl

www.eur.nl/esl/research/research-areas/institutes/cyber-security