Mr. N.M. Brouwer[1]

'Vlijt en naarstigheid' in een digitale wereld: eigen schuld en beredding in de context van de cyberverzekering

AV&S 2019/23

De voortschrijdende digitalisering van onze samenleving en de daarmee samenhangende nieuwe wetgeving stimuleren de ontwikkeling van nieuwe verzekeringsproducten, zoals de specifieke cyberverzekering. Net als bij traditionele verzekeringen heeft de verzekerde ook in het kader van de cyberverzekering een eigen verantwoordelijkheid om schade te voorkomen en te beperken: de verzekerde dient zich als zorgvuldig en behoorlijk handelend verzekerde te gedragen. Bij gebrek aan duidelijke standaarden op het gebied van cybersecurity is deze open norm in een digitale context echter moeilijk te duiden. In deze bijdrage wordt onderzocht hoe in de context van de cyberverzekering invulling kan worden gegeven aan de eigen schuld en bereddingsplicht als verzekeringsrechtelijke leerstukken.

1. Inleiding

In mei en juni 2017 werd wereldwijd een groot aantal bedrijven en organisaties slachtoffer van twee ernstige cyberincidenten: Wannacry en NotPetya. De gevolgen waren groot: in verschillende ziekenhuizen in het Verenigd Koninkrijk kwamen gehele afdelingen stil te liggen en werden patiënten noodgedwongen geweigerd.[2] In Spanje werd het virus via telecomprovider Telefónica aan honderden computers doorgegeven.[3] Containergigant Maersk kwam dagenlang tot stilstand en heeft haar complete digitale infrastructuur moeten herzien.[4] Transportbedrijf FedEx kon haar diensten niet meer verrichten.[5] In Nederland werkten meerdere parkeergarages van Q-park niet meer,[6] konden pakketdiensten van TNT niet meer uitrijden[7] en kwam zelfs een deel van de Rotterdamse haven stil te liggen.[8] De totale schade van beide aanvallen wordt ver in de miljarden geschat.[9]

Deze gebeurtenissen maken duidelijk welke enorme gevolgen cyberincidenten kunnen hebben. De complexiteit en connectiviteit in het ICT-landschap nemen toe en er is te weinig aandacht voor digitale veiligheid.[10] De digitale weerbaarheid van Nederland staat daarmee onder druk.

Voor een belangrijk deel heeft deze problematiek te maken met de verdeling van verantwoordelijkheden. Uit het Cybersecuritybeeld Nederland 2018 blijkt dat er voor producenten weinig economische drijfveren bestaan om veilige hard- en software te produceren.[11] De zorg voor een veilig gebruik van de producten rust hierdoor grotendeels op de gebruiker zelf, bijvoorbeeld door het treffen van voorzorgsmaatregelen. Deze status quo beheerst eveneens de verwachtingen tussen gebruikers onderling, bijvoorbeeld in zakelijke verhoudingen en overeenkomsten.

Ook in de verzekeringswereld leiden ontwikkelingen in technologie en wetenschap tot veranderende verplichtingen over en weer, of zoals Vloemans reeds in 2009 opmerkte:

> "In een wereld waar steeds meer risico's ontdekt worden en waar steeds meer onzekerheid zal bestaan, dient eenieder zijn verantwoordelijkheid te nemen, om te beginnen de verzekerde zelf."[12]

Tien jaar later maken de voortschrijdende digitalisering en daarmee samenhangende nieuwe wetgeving (zoals de AVG en de NIB-richtlijn),[13] alsmede de ontwikkeling van nieuwe

1 Mr. N.M. Brouwer is advocaat bij Dirkzwager advocaten & notarissen en als buitenpromovenda verbonden aan het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. Citeerwijze: N.M. Brouwer, ''Vlijt en naarstigheid' in een digitale wereld: eigen schuld en beredding in de context van de cyberverzekering', *AV&S* 2019/23, afl. 4.

2 W. Smart, *Lessons learned review of the WannaCry Ransomware Cyber Attack*, Independent report NHS, London 1 februari 2018, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

3 F. Palazuelos, 'How the WannaCry ransomware attack affected businesses in Spain', *El Pais* 19 mei 2017, https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html.

4 R. Chirgwin, 'IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz', *The Register* 25 januari 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

5 J. Leyden, 'FedEx: TNT NotPetya infection blew a $300m hole in our numbers', *The Register* 20 september 2017, https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/.

6 Redactie, 'Nederlandse parkeergarages getroffen door cyberaanval', *Volkskrant* 14 mei 2017, https://www.volkskrant.nl/cultuur-media/nederlandse-parkeergarages-geraakt-door-cyberaanval~be1e1a80/.

7 NOS, 'Nieuwe aanvallen met gijzelvirus, ook pakketbezorger TNT getroffen', 27 juni 2017, https://nos.nl/artikel/2180251-nieuwe-aanvallen-met-gijzelvirus-ook-pakketbezorger-tnt-getroffen.html.

8 Zie o.a. E. van den Heuvel (red.), *CSR Magazine 2018*, p. 13 en 44-46.

9 Zie bijvoorbeeld de bevindingen van onderzoeksbureau Cybersecurity Ventures in TrendMicro, *2017 Annual Security Roundup: The paradox of Cyber Threats*, Trend Micro: 2018, p. 5.

10 Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2018*, Den Haag 2018, p. 5.

11 CSBN 2018, p. 9. Inmiddels wordt gezocht naar mogelijkheden om het aansprakelijkheidsregime jegens hard- en softwareproducten aan te scherpen, zie Regeerakkoord 2017-2021,*'Vertrouwen in de toekomst'*, 10 oktober 2017, p. 3 en Rijksoverheid, '*Roadmap Digitaal Veilige Hard- en Software*', Den Haag 2018, p. 24.

12 N. Vloemans, 'Onzekerheid en verzekerbaarheid', in: M.L. Hendrikse en J.G.J. Rinkes, *Knelpunten in het verzekeringsrecht deel 2*, Paris: Zutphen 2009, p. 143.

13 Algemene Verordening Gegevensbescherming, (EU) 2016/679 en de Netwerk en Informatieveiligheid Richtlijn, (EU) 2016/1148. De NIB-richtlijn is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni), die op 9 november 2018 in werking is getreden.

verzekeringsproducten zoals de specifieke cyberverzekering, de verdeling van verantwoordelijkheden en daarbij behorende verwachtingen nog altijd tot een actueel en relevant vraagstuk.

De eigen verantwoordelijkheid van de verzekerde is in het verzekeringsrecht op verschillende plekken terug te zien, bijvoorbeeld in de leerstukken eigen schuld (artikel 7:952 BW) en de bereddingsplicht en -kosten (artikel 7:957 en 7:959 BW). In het oude verzekeringsrecht (283 WvK) diende de verzekerde voldoende 'vlijt en naarstigheid' te betrachten. In titel 7.17 BW komen deze woorden thans niet meer voor, maar wordt hetzelfde beoogd. De omvang van de eigen verantwoordelijkheid wordt mede bepaald door een maatman-criterium: de zorgvuldige en behoorlijk handelende verzekerde.[14] Dit vormt tevens het kader voor hetgeen de verzekeraar op dit punt van haar verzekerde mag verwachten.

In dit tijdperk van digitale transformatie en voortschrijdende technologie is deze open norm echter moeilijk te duiden. In deze bijdrage onderzoek ik hoe in de context van de cyberverzekering invulling kan worden gegeven aan de leerstukken eigen schuld en bereddingsplicht. Hierbij ga ik ook in op de rol die verzekeraars kunnen spelen.

Daartoe zal ik eerst een korte schets geven van beide leerstukken (paragraaf 2). Vervolgens ga ik aan de hand van een polisonderzoek nader in op algemene voorzorgsmaatregelen in een digitale context (paragraaf 3) en op het criterium 'onmiddellijk dreigend gevaar' (paragraaf 4). Ik sluit af met een aantal concluderende beschouwingen (paragraaf 5).

2. Eigen schuld en bereddingsplicht: een korte schets

2.1 *Eigen schuld*

Verzekeraars vergoeden geen schade die is veroorzaakt door opzet of roekeloosheid van de verzekerde (artikel 7:952 BW).[15] Gezien deze hoge schuldgradatie is schade door eigen schuld dan ook tot op zekere hoogte verzekerd.[16] Artikel 7:952 BW bevat regelend recht. Er mag in de polisvoorwaarden zowel ten nadele als ten voordele van de verzekerde worden afgeweken, met dien verstande dat de grens is gelegen in de goede zeden en de openbare orde (artikel 3:40 BW). De zwaarste vormen van opzet zijn niet verzekerbaar.[17]

In de polisvoorwaarden kan door middel van een lagere schuldgradatie dus een strenger eigen schuld-beding worden opgenomen dan artikel 7:952 BW. Een voorbeeld is de bepaling dat geen dekking wordt verleend indien de verzekerde niet de normale voorzichtigheid in acht heeft genomen om schade te voorkomen.[18] Vergelijkbare bepalingen komen ook voor in de cyberverzekering, bijvoorbeeld de clausule dat de schade niet is verzekerd als de verzekerde "*te weinig*" heeft gedaan om schade te voorkomen, terwijl "*algemeen bekend is dat de kans op schade groot is*", of indien verzekerde "*niet alle redelijke voorzorgsmaatregelen heeft getroffen*." Dit soort bepalingen zijn weinig concreet. Aan de rechter komt daardoor een ruime vrijheid toe bij de beoordeling of er wel of geen dekking moet worden verleend.[19]

2.2 *Bereddingsplicht*

Ook in het kader van de bereddingsplicht (artikel 7:957 BW) wordt de uitkeringsplicht van de verzekeraar (mede) bepaald door het handelen van de verzekerde zelf.[20] Door middel van deze verplichting wordt voorkomen dat de verzekerde bij dreigende schade achterover gaat leunen 'omdat hij toch verzekerd is'. De bereddingsplicht geldt in beginsel voor alle schadeverzekeringen. De verzekerde moet, wil hij recht hebben op (volledige) uitkering voor zijn schade, *bijzondere* maatregelen treffen om onmiddellijk dreigend gevaar zoveel mogelijk af te wenden of de ontstane schade zoveel mogelijk te beperken.

Maakt de verzekerde daarbij kosten of lijdt hij schade, dan dient de verzekeraar die te vergoeden, mits sprake is van een verzekerd risico (artikel 7:959 BW). De verzekerde beperkt immers de schade waarvoor de verzekeraar het financiële risico draagt. Indien de verzekerde zijn bereddingsplicht verzuimt, dan kan dat een verminderde uitkering of (indien dit op polisniveau is overeengekomen) een geheel verval van uitkering tot gevolg hebben.

2.3 *Samenloop eigen schuld en bereddingsplicht?*

Het temporele toepassingsgebied van de bereddingsplicht is vrij ruim.[21] In de literatuur is daarom de vraag gesteld of er een samenloop mogelijk is tussen eigen schuld en de bereddingsplicht.

Deze samenloop is niet mogelijk indien het schadevoorval reeds heeft plaatsgevonden. Als de schade is ingetreden wordt aan artikel 7:952 BW niet meer toegekomen. In de fase net voorafgaand aan het intreden van de schade is dat anders: dan is samenloop wel mogelijk.[22] In het *Amercentrale*-arrest oordeelde de Hoge Raad dat het enkele feit dat een verzekerde hoe dan ook maatregelen had moeten

14 M.L. Hendrikse e.a., *Parl. Gesch.* Boek 7.17 BW, Deventer: Kluwer 2007, p. 181.

15 Opgemerkt zij dat het bij eigen schuld in het verzekeringsrecht niet gaat om schuld als maatstaf van verwijtbaarheid zoals in het onrechtmatigedaadsrecht, "*maar om de vraag of de verzekerde gelet op zijn handelen in zijn verhouding tot assuradeuren wel recht heeft op uitkering*". Zie Huizink 'Eigen schuld', in Hendrikse red., Verzekeringsrecht, Kluwer, Deventer: Wolters Kluwer 2019, p. 531.

16 Onder het oude verzekeringsrecht was dit anders: artikel 276 en 294 WvK spraken van 'eigen schuld' en 'merkelijke schuld' van de verzekerde.

17 *Asser/Wansink, Van Tiggele & Salomons, Verzekering 7-IX* 2019/465.

18 Dergelijke bepalingen komen regelmatig voor bij diefstal- en kostenbaarhedenverzekeringen.

19 F.H.J. Mijnssen, *Verzekering* (Mon. BW B88), Deventer: Kluwer 2012, p. 68.

20 De bereddingsplicht geldt voor zowel verzekeringnemer als verzekerde. Voor de leesbaarheid wordt in dit artikel verder enkel gesproken van 'verzekerde'. Tenzij uitdrukkelijk anders vermeld, wordt daarmee dus ook de verzekeringnemer bedoeld.

21 M.L. Hendrikse e.a., *Verzekeringsrecht*, Kluwer: Deventer Wolters 2015, p. 558

22 M.L. Hendrikse e.a., *Verzekeringsrecht*, Kluwer: Deventer Wolters 2015, p. 558-560. Anders: HR 23 oktober 1992, *NJ* 1992/814 (*De Gans/Nationale Nederlanden*), bestreden door Blom, *Vrb.* 1993/3, p. 21-22.

treffen, bijvoorbeeld uit hoofde van een overeenkomst (bewaarneming, aanneming van werk of huur),[23] of uit hoofde van zijn algemene zorgvuldigheidsverplichting om schade te voorkomen, de betekenis van de bereddingsplicht onverlet laat.[24] In de periode vlak vóór het plaatsvinden van het schadevoorval kunnen schuld (algemene voorzorgsmaatregelen) en beredding (bijzondere noodmaatregelen) elkaar dus overlappen.

De samenloop tussen eigen schuld en bereddingsplicht kan leiden tot botsende rechtsregels. Zo wordt bijvoorbeeld bij een beroep op schending van de bereddingsplicht de nalatigheid van ondergeschikten en hulppersonen wel aan de verzekerde toegerekend, terwijl eigen schuld uitsluitend ziet op gedrag van de verzekerde zelf.[25] Daarnaast wordt bij de beoordeling van eigen schuld wegens schending van de zorgvuldigheidsnorm uitgegaan van een andere maatstaf dan bij de beoordeling van het al dan niet nakomen van de bereddingsplicht.[26] In het eerste geval wordt dan bijvoorbeeld getoetst aan opzet in de zin van artikel 7:952 BW, terwijl in het laatste geval de normale toerekeningsregels worden toegepast. Ik meen dat deze botsing zich in mindere mate voordoet indien in de polisvoorwaarden een lagere schuldgradatie is opgenomen dan opzet of roekeloosheid. De meeste cyberverzekeringen bevatten bijvoorbeeld de verplichting om 'redelijke voorzorgsmaatregelen' te treffen. De toetsingsmaatstaven lopen dan weinig uiteen.

3. Voorzorgsmaatregelen in een digitale samenleving

Algemene voorzorgsmaatregelen, zoals een slot op de deur, dient iedere verzekerde op eigen kosten te treffen.[27] In een digitale context is dit niet anders. Op iedere organisatie rust de verplichting om te zorgen voor een gedegen cybersecurity.[28] De beschikbaarheid, integriteit en vertrouwelijkheid van systemen en gegevens dienen te worden gewaarborgd. Daarmee wordt niet alleen de beveiliging en stabiliteit van de eigen systemen versterkt. Gezien de grote mate van verwevenheid en onderlinge afhankelijkheid van systemen is ook de beveiliging van anderen daarmee gebaat.[29]

Welke maatregelen precies genomen moeten worden, is echter niet duidelijk. Er bestaan weliswaar beveiligingsstandaarden die zijn gebaseerd op *best practice*, zoals de ISO27000 serie.[30] Deze zijn echter technologieneutraal geformuleerd en bevatten daarom geen concrete voorschriften.[31] De invulling daarvan kan dus per organisatie sterk verschillen. Bovendien is het hebben van een ISO-certificaat geen (standaard)vereiste voor dekking onder een cyberverzekering.

Deze onduidelijkheid doet zich ook voor bij de in het kader van de bereddingsplicht te nemen *bijzondere* maatregelen. Wil de verzekerde de bereddingskosten vergoed krijgen, dan dienen de bijzondere maatregelen redelijk en doelmatig te zijn: zij moeten voldoen aan de eisen van proportionaliteit (staan de kosten van de maatregelen wel in verhouding tot de te verwachten verzekerde schade?) en subsidiariteit (kon er geen andere, goedkopere maatregel worden getroffen die hetzelfde effect zou hebben?).[32]

Of dit het geval is, dient de verzekerde naar eigen kennis en wetenschap in te schatten. Deze kennis wordt tot op zekere hoogte geobjectiveerd. Daarbij wordt als maatstaf gehanteerd de behoorlijke en zorgvuldige verzekerde, waarbij met alle omstandigheden van het geval rekening moet worden gehouden.[33] Het gaat er dus niet enkel om waarvan een verzekerde op de hoogte *is*, maar ook waarvan hij op de hoogte *behoort te zijn*. Door het gebrek aan standaarden en certificeringen op het gebied van cybersecurity heeft de verzekerde daarbij een zekere eigen beoordelingsruimte voor de te treffen maatregelen.[34]

Met het oog op de leerstukken schuld en bereddingsplicht is het voor een verzekerde belangrijk om zowel vóór als direct na een incident juiste keuzes te maken over de te treffen maatregelen. Het eigen handelen van de verzekerde kan er immers toe leiden dat hij geen of een verminderde uitkering krijgt. Anders dan bij veel traditionele verzekeringen (denk aan voorgeschreven sprinklers bij brand of gecertificeerde sloten bij scooters) zijn cyberverzekeraars niet duidelijk in wat zij van hun verzekerden op dit punt verwachten. De vraag is ook of dat wel mogelijk is, nu cyberrisico's in hoge mate afhankelijk zijn van de specifieke kenmerken van organisaties, zoals omvang, type, sector en mate van digitalisering.[35]

23 Vgl. Hof Amsterdam 18 januari 2011, ECLI:NL:GHAMS:2011:BP6224 (*DL/SRA*) resp. HR 15 april 2011, *NJ* 2011/179 (*besmette cacao*), resp. HR 30 november 2007, *NJ* 2007/641 (*Staedion*).

24 HR 13 juni 1975, *NJ* 1975/509 (*Amercentrale*).

25 Zie *Asser/Wansink, Van Tiggele & Salomons 7-IX* 2019/574 en Hendrikse, *Verzekeringsrecht*, Deventer: Wolters Kluwer 2019, p. 641-642.

26 K.W. Brevet, 'Beredding en eigen schuld', in: N. van Tiggele-Van der Velde e.a. (reds.), *De Wansink-bundel Van draden en daden*, Deventer: Kluwer 2006, p. 130-132. In navolging van Dutilh (I.J. Dutilh in: *2000 Weken rechtspraak, Arresten van de Hoge Raad der Nederlanden gewezen in zaken, bepleit door mr. C.R.C. Wijckerheld Bisdom, advocaat*, Zwolle: W.E.J. Tjeenk Willink 1978, p. 131) pleit Brevet voor gelijktrekking van de schuldgradaties in de leerstukken eigen schuld en bereddingsplicht. Zie tevens *Asser/Wansink* 2019/574 en Hendrikse 2019, p. 642

27 M.L. Hendrikse e.a., *Parl. Gesch*. Boek 7.17 BW, Deventer: Kluwer 2007, p. 177.

28 P.T.J. Wolters & C.J.H. Jansen, *Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity*, Cyber Security Raad, Nijmegen 2017.

29 Vgl. ook CSBN 2018, p. 9.

30 Zie bijvoorbeeld ISO/IEC 27000:2018(E), 2018-2.

31 Het Verbond van Verzekeraars speelt hier inmiddels op in door samen met publieke en private partijen te werken aan een keurmerk voor cybersecurity, zie Verbond Van Verzekeraars, 'Verzekeraars maken werk van cybersecurity', 7 juni 2018, https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-maken-werk-van-cybersecurity (laatst bezocht op 18 januari 2019). Dit geldt ook voor de Rijksoverheid in de '*Roadmap Digitaal Veilige Hard- en Software*', Den Haag 2018.

32 HR 15 april 2011, *NJ* 2011/179 (*Besmette cacao*). Zie ook H. Kramer, 'De kwalificatie van kosten als bereddingskosten bij AVB-polis', *Bb* 2011/37.

33 M.L. Hendrikse e.a., *Parl. Gesch*. Boek 7.17 BW, Deventer: Kluwer 2007, p. 181.

34 Vgl. HR 30 november 2007, *NJ* 2007/641 (*Staedion*).

35 Zie ook het rapport van de Federation of European Risk Management Associations (FERMA), *Preparing for cyber insurance*, oktober 2018, p. 5.

3.1 *Methode*

Het maatman-criterium en de daarbij aansluitende objectieve kennis van de verzekerde vormen de norm waaraan het gedrag van de verzekerde moet worden getoetst.[36] In het navolgende poog ik aan deze normstelling gestalte te geven door te kijken naar de verwachtingen die de cyberverzekeraar op dit punt van haar verzekerden heeft. Aan de hand van de vragen en acceptatie-eisen in de aanvraagformulieren en zorgvuldigheidsnormen in de polisvoorwaarden kan de contractuele verplichting van de verzekerde tot op zekere hoogte concreet worden ingevuld. Daarnaast kan hieruit in meer algemene zin worden afgeleid welk kennisniveau bij een verzekerde aanwezig wordt geacht en in welke mate zij zich volgens de verzekeraar moet inspannen om schade te voorkomen en te beperken.[37] De concrete informatie uit de acceptatieformulieren en polisvoorwaarden bieden daarmee algemene inzichten over de (invulling van de) zorgplicht van de verzekerde.

Voor dit artikel zijn de (gestandaardiseerde)[38] aanvraagformulieren en polisvoorwaarden onderzocht van de verzekeraars die op dit moment in Nederland een cyberverzekering aanbieden. De bevindingen heb ik afgezet tegen de empirische inzichten die het Centraal Bureau voor Statistiek geeft in haar Cybersecuritymonitor 2018 ('CSM 2018').[39] Als parameters heb ik derhalve de door het CBS samengestelde indicatoren gebruikt.[40]

3.2 *Indicaties in de aanvraagfase*

Tussen de verschillende verzekeraars blijken grote verschillen te bestaan in de wijze waarop de vragen zijn geformuleerd en gecategoriseerd. Bovendien stellen lang niet alle verzekeraars dezelfde vragen. Toch is hierin wat betreft veiligheidsmaatregelen een zekere rode draad te ontdekken.[41]

Alle cyberverzekeraars vragen bij aanvang van de verzekering naar het gebruik van firewalls, de aanwezigheid van herstelprocedures en een beleid voor *back-ups*. Al deze vereisten komen op de lijst van het CBS niet voor. Wel op de lijst én door alle cyberverzekeraars gevraagd zijn antivirussoftware en een authenticatiebeleid. Verder vraagt het merendeel van de verzekeraars om een wachtwoordenbeleid, automatische updates van beveiligingssoftware (*patches*) en encryptie van data. Zaken die niet of weinig worden gevraagd, maar wel op de lijst van het CBS voorkomen, zijn de aanwezigheid van logbestanden om incidenten te kunnen analyseren, VPN bij internetgebruik buiten het eigen bedrijf en *network access control*.

Nu een aantal van deze maatregelen in de meeste aanvraagformulieren terugkomt, is dat een indicatie dat onder verzekeraars een redelijke consensus bestaat dat deze maatregelen algemene voorzorgsmaatregelen zijn die iedere verzekerde dient te treffen.[42]

Een enkele uitzondering daargelaten, worden deze maatregelen echter weinig geconcretiseerd. Binnen hoeveel dagen een *patch* of update moet worden geïmplementeerd, is dus aan de inschatting van de verzekerde zelf.[43] Ik vraag mij af of dit niet een gemiste kans is voor zowel verzekeraars zelf als de maatschappij in bredere zin. Grote incidenten zoals Wannacry en NotPetya tonen aan dat het belang van zo snel mogelijk *patchen* zeker niet moet worden onderschat.[44] Ter verhindering van de kwetsbaarheid die Wannacry mogelijk maakte had Microsoft al twee maanden eerder een *patch* uitgegeven, maar nog niet alle bedrijven en organisaties hadden deze geïnstalleerd. Dit lijkt vrij eenvoudig te ondervangen door in de polisvoorwaarden of – zou dit meer maatwerk betreffen – op het polisblad een termijn voor het installeren van *patches* op te nemen. Hetzelfde geldt voor de algemeen gestelde vraag naar *back-ups*. De aanvraagformulieren geven niet aan hoe vaak deze back-ups moeten worden gemaakt en waar dat wel het geval is, zijn de verschillen groot: dagelijks, wekelijks, maandelijks.

Dergelijke afwegingen laat de cyberverzekeraar kennelijk aan de verzekerde zelf over. Zouden de bepalingen echter concreter zijn, dan schept dat meer duidelijkheid over de verwachtingen die de verzekeraar van haar verzekerde heeft. Bovendien zou de cyberverzekering dan ook in een grotere mate kunnen bijdragen aan een betere cybersecurity. Bedrijven worden dan immers gestimuleerd tot het nemen van concrete maatregelen.[45]

Verder besteden niet alle cyberverzekeraars in de aanvraagfase aandacht aan de menselijke factor bij cybersecurity, terwijl dit een cruciaal element is bij cyberrisicomanagement.[46] De mens is immers niet zelden de zwakste schakel,

36 Ik zie dit criterium dus niet als de feitelijke veronderstelling over het daadwerkelijke gedrag van verzekerden, maar als een normstelling. Vgl. M. Th. Beumers e.a., *Aansprakelijkheidsrecht en maatmens*, Deventer: Wolters Kluwer 2016, p. 7.

37 A. Drougkas, *Commonality of Risk Assessment Language in Cyber Insurance – Study Findings*, ENISA 2017, p. 22.

38 Cyberverzekeringen voor het hogere segment zijn in de regel maatwerk; zo ook op het gebied van acceptatie. Waar wordt gewerkt met een gestandaardiseerde aanvraag, is de doelgroep van de verzekering doorgaans het MKB(+).

39 CBS, *Cybersecuritymonitor 2018: een verkenning van dreigingen, incidenten en maatregelen*, Den Haag: CBS 2018.

40 Zie voor de verantwoording van de keuze van deze indicatoren CSM 2018, p. 16 en 17.

41 Zie ook A. Drougkas (ENISA) 2017, p. 8.

42 Zie FERMA 2018, p. 7 en A. Drougkas (ENISA) 2017, p. 22.

43 In de minderheid van de gevallen wordt wel een termijn genoemd, die varieert van 30 dagen tot zes maanden.

44 W. Smart, *Lessons learned review of the WannaCry Ransomware Cyber Attack*, Independent report NHS, London 1 februari 2018: "[…] *all NHS organisations infected by WannaCry had unpatched, or unsupported, Windows operating systems*" (p. 8).

45 Vergelijk in dit kader ook B.F. Nieuwesteeg, L. Visscher en B. de Waard, 'De rechtseconomie van cyberverzekeringen', *Het Verzekeringsarchief* 2017-3, p. 159. De auteurs concluderen dat de cyberverzekeraar rechtseconomisch gezien op dit punt in grotere mate zou kunnen bijdragen aan een hogere maatschappelijke welvaart.

46 B.F. Nieuwesteeg, *The Law and Economics of Cyber Security* (diss. Erasmus University Rotterdam), 2018, p. 25. Zie ook FERMA 2018, p. 10.

denk bijvoorbeeld aan *social engineering*.[47] Het opleiden en trainen van personeel is als een van de basisvoorschriften van informatiebeveiliging opgenomen in de ISO27000 standaard.[48] Door dit aspect niet in de aanvraagfase te benoemen, geeft de verzekeraar er blijk van dit niet relevant te achten.[49] De menselijke factor lijkt in de aanvraagfase ondergeschikt te zijn aan de technische aspecten. Ook dit acht ik een gemiste kans en bovendien leidt dit tot onnodige onduidelijkheid ten aanzien van het antwoord op de vraag wat een verzekeraar van haar verzekerde verwacht.

3.3 *Zorgvuldigheidsnormen in polisvoorwaarden*

In de polisvoorwaarden van verschillende cyberverzekeringen zijn de verplichtingen van de verzekerde op algemene(re) wijze opgenomen.[50] Zo biedt een van de verzekeraars geen dekking indien de schade is veroorzaakt doordat de verzekerde (n)iets doet, terwijl hij behoort te weten dat de kans op schade groot is, dan wel doordat de verzekerde "*te weinig*" heeft gedaan om schade te voorkomen, terwijl het "*algemeen bekend is dat dat te weinig is*" en hij had moeten weten dat de kans op schade groot is.[51] Naast deze algemene bepaling maakt deze verzekeraar het iets concreter door uitdrukkelijk op te nemen dat geen dekking wordt verleend als de voorgeschreven preventieve maatregelen (wachtwoordenbeleid, firewall, antivirus en wekelijkse back-ups) niet zijn genomen.

Een andere polis noemt niet méér dan de verplichting om zich "*als verantwoord ondernemer*" te gedragen, en schrijft een bepaald softwarepakket voor,[52] terwijl een andere verzekeraar van haar verzekerde verlangt dat zij zich "*naar redelijkheid*" zal inspannen om de IT-beveiligingsmaatregelen, passend bij de aard en omvang van de activiteiten, up to date te houden. Ook komt voor de verplichting van verzekerde om "*redelijke voorzorgsmaatregelen te treffen om aansprakelijkheid op grond van de polis te voorkomen, verminderen of beëindigen*". Een enkeling hanteert een vergelijkbare maatstaf van "*redelijke voorzorgsmaatregelen*", maar koppelt dit aan de omvang en complexiteit van de verzekerde en de middelen die haar ter beschikking staan. Daarnaast is soms een verwijzing naar de AVG terug te zien:[53] onder redelijke voorzorgsmaatregelen "[…] *vallen in ieder geval het nemen van passende technische en organisatorische maatregelen* […]". Ook deze verzekeraar verwijst overigens naar de door haar gestelde, maar niet nader omschreven preventie-eisen. Zij doet dat echter niet expliciet in de polisvoorwaarden, maar in de Verzekeringskaart.

Waar de cyberverzekeraars in de aanvraagfase relatief concrete eisen en vragen stellen, gebruiken zij in de polisvoorwaarden zelf open normen[54] die qua schuldgradatie lager liggen dan het wettelijk criterium van opzet of roekeloosheid.[55] Naast de in de acceptatie gevraagde maatregelen verwachten verzekeraars blijkens de polisvoorwaarden ook gedurende de looptijd van de verzekering nog het nodige van hun verzekerden. Gelet op het feit dat cybersecurity een continu proces is en niet enkel een momentopname, past dat bij de aard van het verzekerde risico.

Gezien de snelheid waarmee de techniek zich ontwikkelt, is het gebruik van open normen begrijpelijk. Een technische eis van vandaag is morgen alweer achterhaald. Een open, technologie-neutrale norm is wat dat betreft toekomstbestendig. Wat een 'redelijke voorzorgmaatregel' is of wanneer een verzekerde zich 'naar redelijkheid' heeft ingespannen, zal – ook als dit niet expliciet in de polisvoorwaarden is benoemd – afhangen van de specifieke omstandigheden van het geval, zoals de omvang en expertise van de verzekerde organisatie, de mate waarin het bedrijf risico loopt, de kosten en bezwaarlijkheid om maatregelen te treffen.[56] Van een gespecialiseerd bedrijf mag eerder worden verwacht dat hij op het kennisniveau van een *'expert of the field*' zit dan van een klein schildersbedrijf of een horecaondernemer.[57] Daarnaast mag van een bedrijf dat enorme hoeveelheden gevoelige data verwerkt of een kritieke digitale infrastructuur in stand moet houden, ook meer worden verwacht dan van een onderneming met enkel een digitaal klantenbestand.

3.4 *Contouren van de algemene zorgplicht van de verzekerde; taak voor de verzekeraar*

Hoewel de invulling van redelijke voorzorgsmaatregelen van geval tot geval kan verschillen, is mede gezien de ac-

47 B.F. Nieuwesteeg, *The Law and Economics of Cyber Security* (diss. Erasmus University Rotterdam), 2018, p. 25. Zie ook FERMA 2018, p. 10. Zie ook CBS 2018. *Social engineering* is een techniek waarbij via menselijke kwetsbaarheden (nieuwsgierigheid, medelijden, angst) informatie wordt verkregen waarmee vervolgens toegang tot het systeem kan worden verkregen.

48 Bewustwording, trainen en opleiden van personeel worden zelfs aangeduid als een van de "*critical succes factors*" voor een goed *information security management system*. ISO/IEC 27000:2018(E), 2018-2, art. 4.6(e).

49 Een van de verzekeraars biedt als onderdeel van de dekking (dus ná afsluiten van de verzekering) een doorlopende leergang aan om specifieke kennislacunes van de verzekerden te beperken (zie SCHADE Magazine 2018/5, p. 50). Dit illustreert dat het nodig wordt geacht om het kennisniveau van de verzekerde omhoog te brengen.

50 Discussies over de kwalificaties van dergelijke bepalingen (preventieve garantieclausules of primaire dekkingsomschrijvingen) en de gevolgen daarvan vallen buiten het bestek van dit artikel.

51 Deze gedragsnorm is ook terug te vinden in een aantal traditionele verzekeringen van deze verzekeraar, zoals de Bedrijfsmiddelenverzekering Brand en Bedrijfsschade.

52 Een duidelijke correlatie tussen het handelen als verantwoord ondernemer en het gebruik van het softwarepakket volgt overigens niet zonder meer uit deze voorwaarden.

53 Algemene verordening gegevensbescherming (Verordening (EU) 2016/679).

54 Met uitzondering van een verzekeraar, die een lijst van relatief concrete preventieafspraken in de polisvoorwaarden heeft opgenomen.

55 Ik realiseer mij dat over de term 'redelijke voorzorgsmaatregelen' en de daarbij te hanteren schuldgradatie discussie mogelijk is, net als bij de term 'normale voorzichtigheid' (vgl. bijv. in het kader van consumentenverzekeringen M.L. Hendrikse, *Eigen schuld, bereddingsplicht en medewerkingsplicht in het schadeverzekeringsrecht*, Deventer: Kluwer 2002, § 3.4.2). Zie anders: Van Tiggele-Van der Velde 2008 (diss.), p. 301. Een uitgebreide discussie op dit punt valt echter buiten het bestek van dit artikel. Duidelijk is wel dat cyberverzekeraars de eigen zorgvuldigheidsverplichting van de verzekerde expliciet hebben opgenomen en derhalve niet lijken te willen terugvallen op het wettelijk schuldcriterium van artikel 7:952 BW.

56 Deze factoren zijn ook terug te zien in de jurisprudentie over 'normale voorzichtigheid' die van verzekerden wordt verlangd, zie bijvoorbeeld ECLI:NL:RBROT:2018:7923, ECLI:NL:RBARN:2012:BV3840, ECLI:NL:GHSHE:2012:BY6963, ECLI:NL:RBROT:2013:BY8745, ECLI:NL:RBALK:2004:AP7366.

57 Vgl. E. de Jong, 'Voorzorgverplichtingen', *AV&S* 2016/47.

ceptatieformulieren toch een aantal maatregelen te duiden die – zij het voorzichtig en de bovenstaande nuances in acht nemend – als algemeen bekend en haalbaar (en dus als redelijk) kunnen worden aangewezen.

De wijze waarop verzekeraars op dit moment blijkens hun acceptatie- en aanvraagformulieren richting geven aan hun verwachting van de behoorlijke en zorgvuldige verzekerde, correspondeert in grote lijnen met de feitelijke situatie zoals die volgt uit de cijfers van het CBS. Uit de CSM 2018 blijkt bijvoorbeeld dat 87% van de bedrijven in 2017 antivirussoftware gebruikte. Meer dan de helft van de bedrijven heeft een beleid voor sterke wachtwoorden en bewaart gegevens op een andere fysieke locatie.[58] Ook gebruikt de meerderheid van de middelgrote en grote bedrijven een automatisch of handmatig security update-beleid voor beveiligingssoftware en operationele software.[59]

Daar staat tegenover dat bijvoorbeeld het gebruik van data-encryptie (waar de meerderheid van de verzekeraars naar vraagt), logging en risicoanalyses slechts door een minderheid van de bedrijven wordt toegepast. Opvallend is verder dat het hebben van herstelprocedures in het geheel niet voorkomt op de lijst van de CSM 2018, terwijl wel alle verzekeraars daarnaar vragen. Belangrijk punt is de grote rol van de externe ICT-leverancier bij de organisatie van digitale beveiliging van organisaties, zeker bij middelgrote bedrijven. Bijna 70% van de bedrijven die werk maken van beveiliging, besteedt dit uit aan een ICT-leverancier.[60]

Bovengenoemde indicaties schetsen de contouren van de eigen verantwoordelijkheid van de verzekerde. Door de algemeen geformuleerde zorgvuldigheidsnormen en de onbepaaldheid en ogenschijnlijke willekeur van de concreet gestelde eisen blijft echter de nodige onduidelijkheid bestaan. Cyberverzekeraars zouden daarin verandering kunnen aanbrengen door open normen meer te concretiseren en door processen meer te harmoniseren.

Hoewel het gebruik van open normen vanuit het perspectief van de verzekeraar verklaarbaar is, leidt dit tot een gebrek aan transparantie over de dekking. Dit terwijl de verzekeraar, zeker ten opzichte van het MKB, een kennisvoorsprong heeft op haar verzekerden. De sociale functie van verzekeringen vraagt om een actief handelen van de verzekeraar om de verzekerde te beschermen.[61] Waar open normen onduidelijkheid creëren, dient de verzekeraar zich er dan ook voor in te spannen om de verzekerde bij de hand te nemen en aan die normen meer gestalte te geven.

Een manier waarop cyberverzekeraars dat zouden kunnen doen, is door actief kennis te delen, bijvoorbeeld door het aanbieden van preventieve diensten en het verzorgen van voorlichtingsbijeenkomsten over de omgang met cyberrisico's. Daarnaast zouden de open voorzorgverplichtingen nader kunnen worden uitgewerkt. Indien de techniek te snel verandert om deze maatregelen in polisvoorwaarden te verankeren, zou gewerkt kunnen worden met bijvoorbeeld een bijlage bij de polis waarin technische en organisatorische maatregelen worden gespecificeerd.[62] De in de acceptatiefase gestelde vragen en/of eisen kunnen daaraan dan bovendien explicieter worden gekoppeld als minimum beveiligingsvereisten. Een dergelijke lijst kan jaarlijks worden geëvalueerd en waar nodig worden herzien. Daarmee schept de cyberverzekeraar een duidelijker kader over de dekking. Gezien de professionaliteit van de verzekeraar en de daaraan verbonden 'gidsfunctie',[63] mag dat gelet op de zorgplicht van een prudent verzekeraar ook worden verwacht.[64]

Bovendien zouden verzekeraars op een grondiger manier kunnen bijdragen aan een meer gestructureerd en overzichtelijk landschap door hun *risk assessment* en *underwriting*-processen meer te harmoniseren. Een geharmoniseerd *underwriting*-proces kan een gemeenschappelijke basis voor cyberverzekeringen creëren.[65] De ISO27000-normen kunnen hiervoor een uitgangspositie bieden. Hoewel deze normen geen concrete beveiligingsmaatregelen voorschrijven, vormen zij wel een allesomvattend kader waarbinnen concrete voorschriften kunnen worden geformuleerd (ICT-technisch, ICT-organisatorisch en bewustwording). Een geharmoniseerde methode past bovendien bij de aard van cyberrisico's, die veelomvattend is en samenwerking vereist tussen verschillende partijen en disciplines. Een dergelijke aanpak schept helderheid over de wijze waarop een behoorlijke en zorgvuldige verzekerde zich dient te gedragen.

4. De bereddingsplicht in een digitale samenleving

In vrijwel alle cyberpolisvoorwaarden zijn zelfstandige bereddingskostenclausules opgenomen.[66] Deze bepalingen vormen in feite een weergave van de wettelijke bepaling van artikelen 7:957 en 7:959 BW.[67] Hoewel dit op zichzelf ook in polisvoorwaarden van traditionele verzekeringen ge-

58 CBS 2018, p. 20-21.
59 CBS 2018, p. 22.
60 CBS 2018, p. 22.
61 J.H. Wansink, 'Bespiegelingen op de rode draden in het verzekeringsrecht na tien jaar titel 7.17 BW', in: N. van Tiggele-van der Velde, *Bespiegelingen op 10 jaar 'nieuw' verzekeringsrecht*, Deventer: Wolters Kluwer 2015, p. 2-3. Zie ook J.H. Wansink, 'Assurance oblige: de maatschappelijk verantwoord handelende verzekeraar in de 21e eeuw', *AV&S* 2003/2 en T. Hartlief, *Anno 2010. Beschouwingen over aansprakelijkheid en verzekering*, Amsterdam: Uitgeverij deLex, 2009, p. 79-80.
62 Het uitwerken van variabele elementen zoals technische maatregelen in een bijlage bij een overeenkomst is niet ongebruikelijk, zo ook bijvoorbeeld bij verwerkersovereenkomsten in de zin van artikel 28 lid 3 Algemene verordening gegevensbescherming.
63 Vgl. Wansink 2003.
64 Vgl. Wansink 2015, p. 4.
65 A. Drougkas (ENISA), 2017.
66 Enkel in een tweetal sets voorwaarden trof ik geen algemene bereddingskostenclausule aan. Het ontbreken van een expliciete clausule neemt overigens de werking van artikel 7:957 en 7:959 BW niet weg.
67 Een voorbeeld van dergelijke bepalingen in de cyberpolis is: "*Verzekerde dient alle maatregelen te nemen ter voorkoming of vermindering van schade of dreigende schade als bedoeld in artikel 7:957 BW (bereddingsplicht)*" en "*Verzekeraar zal de bereddingskosten vergoeden die verzekerde maakt in het kader van een gedekte aanspraak*".

bruikelijk is, roept de invulling daarvan bij de cyberverzekering vragen op.

4.1 *Risico heeft zich verwezenlijkt: incident response*

Bij bereddingskosten in een digitale context kan in ieder geval worden gedacht aan *incident response*. Dat houdt in dat direct na bijvoorbeeld een privacy-inbreuk of beveiligingsincident (al dan niet door een externe partij) wordt gewerkt aan het achterhalen van de oorzaak, het beoordelen van de ernst van de gebeurtenis in het licht van de privacyregelgeving en het zoveel mogelijk beperken van verdere (reputatie)schade door op de juiste wijze met de juiste partijen te communiceren.[68]

In elke cyberverzekering vormen deze diensten een van de hoofdelementen van de dekking. De verzekeraar heeft dus lijn aangebracht in de uitvoering en kosten van wat in feite bereddingsmaatregelen zijn, door deze diensten zelf in de primaire dekking te integreren en op voorhand zelf de uitvoerende partijen aan te wijzen. Daarmee is het op dit punt niet meer de verzekerde die naar eigen kennis en kunde beslist welke bereddingsmaatregelen getroffen moeten worden, maar de verzekeraar.[69]

Nu in de polisvoorwaarden echter ook aparte, algemene bereddingskostenclausules zijn opgenomen, moet kennelijk ook nog aan andere maatregelen worden gedacht dan *incident response*. Cyberverzekeraars signaleren bovendien een verschuiving in de vraag naar verzekeringsdekking voor privacyaansprakelijkheid (waarop *incident response* veelal betrekking heeft) naar dekking voor bedrijfsstilstand, reputatieschade en boetes, waarvoor de cyberverzekering ook dekking biedt.[70] De bereddingsplicht kan derhalve ook buiten *incident response* van belang zijn. Door het algemene karakter van de clausule speelt de eigen inschatting van de verzekerde dan een grote rol.

4.2 *Onmiddellijk dreigend gevaar*

Waar bij de verwezenlijking van het gevaar door middel van *incident response* de verzekeraar een groot aandeel heeft in de wijze waarop de schade zo goed mogelijk wordt beheerst, is dit in de fase daarvóór, bij een onmiddellijke dreiging van gevaar, aan de verzekerde zelf.

Of sprake is van een onmiddellijk dreigend gevaar, dient de verzekerde naar eigen kennis en inschatting te bepalen. Het gaat erom of de verzekerde in redelijkheid heeft mogen aannemen dat sprake was van een onmiddellijk dreigend gevaar, dat slechts door het treffen van bijzondere maatregelen kan worden weggenomen.[71] Er valt niet altijd een scherpe lijn te trekken tussen alledaagse, doorlopende risico's en een situatie waarin sprake is van een onmiddellijk dreigend gevaar. Gezien de overlap tussen eigen schuld en bereddingsplicht kan dit problematisch zijn; algemene voorzorgsmaatregelen en bijzondere (bereddings)maatregelen lopen dan in elkaar over.

4.2.1 *Herkennen van onmiddellijk dreigende digitale gevaren*

Als geen sprake is van onmiddellijk dreigend gevaar, is evenmin sprake van een bereddingsplicht van de verzekerde, noch van een vergoedingsplicht van de verzekeraar. De bekendheid van de verzekerde met het onmiddellijk dreigende gevaar wordt tot op zekere hoogte geobjectiveerd. Het gaat er dus om wat de verzekerde behoorde te weten.

In traditionele situaties kan een onmiddellijk dreigend gevaar evident aanwezig zijn: als een plafond al krakend en piepend op instorten staat, mag een behoorlijke en zorgvuldige verzekerde in redelijkheid aannemen dat sprake is van een situatie waarin hij dient te beredden en waarin de daaraan verbonden kosten op de verzekeraar kunnen worden verhaald.[72] Bij digitale risico's is een dergelijk onmiddellijk dreigend gevaar minder eenvoudig vast te stellen. Hierdoor is het onduidelijk wanneer een verzekerde van een dergelijk risico op de hoogte behoort te zijn.

Het belang van (digitale) gevaarherkenning moet niet worden onderschat. Het merendeel van de bedrijfsprocessen wordt tegenwoordig automatisch (digitaal) uitgevoerd. Dat ICT nooit 100% beveiligd is, wordt als een vaststaand gegeven aangenomen[73] en blijkt ook uit een lange reeks van structurele kwetsbaarheden. Spectre/Meltdown in de processors van Intel en Stagefright in het Android besturingssysteem van Google zijn daarvan sprekende voorbeelden.[74] Kwetsbare systemen komen des te meer voor bij bedrijven en organisaties die gebruikmaken van zogeheten *legacy systems*.[75] Dit zijn oude systemen die lastig te vervangen zijn, bijvoorbeeld doordat de verrichte diensten permanent beschikbaar moeten blijven (denk aan de systemen van ziekenhuizen of overheden). De systemen zijn vaak in de loop der jaren gefaseerd opgebouwd en aan elkaar geknoopt, waardoor er een grote onderlinge verwe-

68 Uit HR 10 oktober 2003, ECLI:NL:HR:2003:AI0828 ('*t Witte Paerdje*) volgt dat kosten van hulppersonen – zelfs als die hun taak niet goed uitvoeren – onder de door de verzekeraar te vergoeden bereddingskosten kunnen worden gebracht.

69 Vergelijk in dit kader de bepalingen ten aanzien van de schaderegeling bij klassieke AVB-polissen, zie Wansink 2006, p. 381.

70 European Insurance and Occupational Pensions Authority (EIOPA), *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies*, Luxemburg: Publications Office of the European Union, 2018, p. 10.

71 HR 30 november 2007, *NJ* 2007/641 (*Staedion*). Vergelijk ook *Asser/Wansink 7-IX* 2019/578.

72 Mits uiteraard sprake is van een gedekt risico.

73 Het Rathenau Instituut noemt dit zelfs "de inherente onveiligheid van ICT". G. Munnichs e.a., *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid*, Den Haag: Rathenau Instituut 2017, p. 29.

74 J. Schellevis, 'Chips in computers en smartphones vatbaar voor ernstige lekken', *NOS* 4 januari 2018, https://nos.nl/artikel/2210445-chips-in-computers-en-smartphones-vatbaar-voor-ernstige-lekken.html en de waarschuwingen van het NCSC van 4 januari 2018, te vinden op https://www.ncsc.nl/actueel/nieuwsberichten/meltdown-en-spectre.html. Deze chips zitten in miljoenen apparaten ingebouwd. De kwetsbaarheid bevond zich in het intrinsieke ontwerp van de chip en kon dus niet met een simpele *patch* opgelost worden. De gevolgen van deze kwetsbaarheid, althans van de oplossing daarvan, zijn dus groot.

75 H. Donkers & J. Koedijk, *Maak legacy klaar voor de toekomst: Inventarisatie en aanzet tot praktische acties*, rapportage KPMG, december 2015

venheid bestaat en vervanging wordt bemoeilijkt. *Legacy systems* veroorzaken evenwel problemen, omdat nieuwe beveiligingssoftware en *patches* daarmee niet altijd compatibel zijn. Deze oude systemen worden dus steeds kwetsbaarder.

Daarvan uitgaande werken alle organisaties – zeker bij gebruik van *legacy systems* – figuurlijk gezien met een krakend en piepend plafond, waarvan het niet de vraag is *of* dat een keer zal instorten, maar *wanneer*. Indien een deel daarvan daadwerkelijk dreigt te gaan afbrokkelen of lekken, is sprake van een situatie van onmiddellijk dreigend gevaar en zal de verzekerde in actie moeten komen. Deze gevaren zijn echter virtueel en derhalve niet zomaar zichtbaar. Een gemiddelde verzekerde zal deze gevaren dan ook lang niet altijd zelf herkennen en zal daarbij afgaan op het oordeel van een deskundige.

Veel bedrijven hebben hun ICT-beheer uitbesteed aan een derde die, gezien het verschil in kennisniveau, als deskundige kan worden aangemerkt.[76] De verzekerde mag zich bij het inschatten van de potentieel gevaarlijke situatie laten leiden door het advies van een deskundige.[77] Als de IT-deskundige aangeeft dat zich een ernstige, kritieke kwetsbaarheid voordoet in de systemen van verzekerde, die enkel met grootschalige 'sanering' van de digitale systemen is op te lossen,[78] mag een zorgvuldige en behoorlijk handelende verzekerde dan in redelijkheid aannemen dat sprake is van een onmiddellijk dreigend gevaar en maatregelen treffen die als bereddingskosten onder de verzekering kunnen worden gebracht?[79] Een aantal cyberverzekeraars heeft de kosten die voortvloeien uit het verwijderen van fouten en kwetsbaarheden in software expliciet uitgesloten. Het merendeel benoemt dit evenwel niet.

In het *Staedion*-arrest uit 2007 deed zich een vergelijkbare discussie voor ten aanzien van preventieve asbestsaneringskosten en de vraag of deze als bereddingskosten onder de AVB-verzekering konden worden gebracht.[80] Het gerechtshof beantwoordde die vraag bevestigend en wees daarbij onder andere op het advies dat Staedion had gekregen van de door haar ingeschakelde deskundige. De Hoge Raad liet dit oordeel in stand.

Dit arrest verruimt de reikwijdte van de bereddingskosten. In een digitale context zijn de gevolgen voor verzekeraars echter niet te overzien indien verzekerden veelvuldig 'saneringskosten' als gevolg van kwetsbaarheden als bereddingskosten onder de verzekering zouden weten te brengen. De voorbeelden Spectre en Meltdown, die de veiligheid van miljoenen apparaten aantasten, sluiten aan bij een lange reeks van kwetsbaarheden en zullen ook zeker niet de laatste zijn.[81] Er zal dus ergens een grens moeten worden getrokken.

Cyberverzekeraars kunnen op dit punt steun vinden in de uitspraak van de Rechtbank Den Haag in de zaak *Samsung/Consumentenbond*.[82] De Consumentenbond vorderde daarin een verklaring voor recht dat Samsung in strijd met de wet/zorgvuldigheid handelde door smartphones niet snel en lang genoeg van updates te voorzien, zelfs niet als Google kwetsbaarheden in Android als 'kritiek' heeft aangemerkt (zoals Stagefright). De rechtbank wees de vorderingen van de Consumentenbond evenwel af, mede omdat de Consumentenbond onvoldoende had aangetoond dat een door Google als kritiek aangemerkte kwetsbaarheid zonder meer leidde tot een daadwerkelijk gevaar voor consumenten. Daarbij nam de rechtbank ook in aanmerking dat het niet gemakkelijk was om misbruik te maken van de kwetsbaarheid. Dit vergde volgens Samsung een grote investering in tijd, inspanning en knowhow. Bovendien was er – voor zover bekend – nog geen feitelijk misbruik van het lek gemaakt.

Deze laatste omstandigheden doen zich vaker voor bij kwetsbaarheden, bijvoorbeeld ook bij Spectre en (met name) Meltdown.[83] De benadering van de rechtbank in de *Samsung*-zaak geeft er blijk van dat er juridisch gezien anders naar digitale risico's wordt gekeken dan technisch gezien. Waar in technische zin sprake kan zijn van een 'kritieke kwetsbaarheid', bijvoorbeeld omdat apparaten van afstand zijn over te nemen of de kern van het besturingssysteem kan worden geraakt, hoeft er in juridische zin nog geen sprake te zijn van een reëel gevaar. Er zou juridisch gezien dan ook betoogd kunnen worden dat er bij kritieke kwetsbaarheden niet direct sprake is van een 'onmiddellijk dreigend gevaar'. Maatregelen die de verzekerde in zo'n geval treft, zijn niet ten bate van de verzekeraars genomen, maar ten bate van de verzekerden zelf. Van een vergoedingsplicht zijdens verzekeraars is dan geen sprake.[84]

76 CBS 2018, p. 20-21. Vergelijk bijvoorbeeld de asbestsaneringsadviseur die woningcorporatie Staedion had ingeschakeld; HR 30 november 2007, *NJ* 2007/641 (*Staedion*).

77 HR 30 november 2007, *NJ* 2007/641 (*Staedion*) en HR 2 mei 1997, *NJ* 1998/281 (*Forbo 'Novilon'*).

78 Dit voorbeeld is te vergelijken met de zaak die is beoordeeld door de Rechtbank Amsterdam, 28 augustus 2013, ECLI:NL:RBAMS:2013:6781. Daarin deed zich een dergelijke situatie voor in 'analoge' zin: de integrale vervanging van de installatie was de enige oplossing om de installatie weer goed te laten functioneren. Van bereddingskosten was echter geen sprake wegens een herstelclausule in de polisvoorwaarden. Zie bijvoorbeeld ook de uitspraak van de Raad van Toezicht RvT II-81/19, genoemd in M.L. Hendrikse, *Eigen schuld, bereddingskosten en medewerkingsplicht in het schadeverzekeringsrecht* (diss.), Deventer: Kluwer 2002, p. 178.

79 Dit voorbeeld is niet onrealistisch, zoals de kwetsbaarheden in de chips van Intel (Spectre en Meltdown) aantonen.

80 HR 30 november 2007, *NJ* 2007/641 (*Staedion*).

81 Bijvoorbeeld Heartbleed en Shellshock 2014, Stagefright en Ghost in 2015, Drown in 2016.

82 Rb. Den Haag 30 mei 2018, ECLI:NL:RBDHA:2018:6310.

83 Zie bijvoorbeeld S. van Voorst, '*Meltdown en Spectre – Q&A*', Tweakers 4 januari 2018, https://tweakers.net/reviews/5939/meltdown-en-spectre-vraag-en-antwoord.html.

84 Vergelijk in dit kader Rb. Amsterdam 28 augustus 2013, ECLI:NL:RBAMS:2013:6781 ten aanzien van de kosten van vervanging van een installatie: "*Voor deze herstelkosten geldt immers* […] *dat zij zijn gemaakt in het belang van de bedrijfsvoering van Wupperman en niet strekten ter afweer van een onmiddellijk dreigend gevaar of bestrijding van een acute schadeoorzaak*". (r.o. 2.5.3).

Een dergelijke risicobenadering staat echter haaks op de inspanningen van zowel private als publieke partijen om het (cyber)risicobewustzijn te verhogen.[85] Daarnaast strookt dit niet met de ernst van de mogelijke gevolgen van cyberrisico's, die – zoals in de inleiding van dit artikel geschetst – verstrekkend kunnen zijn. Gezien het bijzondere karakter van deze risico's kan men zich dan ook afvragen of dit huidige juridische toetsingskader wel in alle gevallen tot een gewenste uitkomst leidt.

4.2.2 *Verhouding tot algemene voorzorgsmaatregelen*

Er is ook een andere reden dat het onwenselijk kan zijn als de bereddingsplicht te ruim wordt toegepast. In een digitale context valt een complexe samenloopdiscussie te voorzien tussen het ontstaan van een onmiddellijk dreigend gevaar en de verplichting om algemene voorzorgsmaatregelen te treffen.

Een onmiddellijk dreigend gevaar kan min of meer spontaan ontstaan, maar kan ook te maken hebben met onvoldoende onderhoud of voorzorgsmaatregelen. Hiervoor noemde ik reeds het *Staedion*-arrest, waarin preventieve asbestsaneringskosten als bereddingskosten onder de AVB-verzekering werden gebracht. De Hoge Raad passeerde daarbij het verweer van de verzekeraars dat Staedion al jarenlang wist dat asbest gevaarlijk kon zijn en dat in de woningen die zij als woningcorporatie verhuurde asbest was verwerkt. Staedion had het op een acuut gevaar laten aankomen, aldus verzekeraars. Een specifiek beroep op eigen schuld komt echter niet helder naar voren.[86] A-G Wuisman verwerpt dit verweer onder verwijzing naar het advies dat de deskundige aan Staedion had uitgebracht. De Hoge Raad laat zich hier verder niet over uit.

De kosten van normaal onderhoud lijken in dit arrest iets te gemakkelijk te zijn afgewenteld op de aansprakelijkheidsverzekeraar.[87] Indien een verzekerde immers lang genoeg geen algemene voorzorgsmaatregelen treft, krijgt zij vanzelf te maken met een onmiddellijk dreigend gevaar op schade.[88] Het is onwenselijk en ook onjuist als een verzekerde die zijn algemene onderhoudsplicht verzaakt, de kosten voor de noodmaatregelen kan claimen bij haar verzekeraar.[89] Dit kan strijdig zijn met het indemniteitsbeginsel en/of het vereiste van onzekerheid (artikel 7:925 BW), of zelfs misbruik van verzekering (artikel 6:248 lid 2 BW) opleveren.[90]

Specifiek bij de cyberverzekering zou de verzekeraar zich in dat geval wellicht kunnen beroepen op de eigen schuld van de verzekerde wegens de schending van de verplichting om redelijke voorzorgsmaatregelen te treffen. De verzekerde organisaties weten immers dat digitale processen risico's meebrengen en dat slecht onderhoud tot verwezenlijking van die risico's kan leiden. Vrijwel alle cyberverzekeraars leggen de verzekerden daarbij bovendien expliciet een 'voorzorgverplichting' op.

Gezien de huidige lijn in de jurisprudentie zal een succesvol beroep op de schending van de algemene 'voorzorgsverplichting' evenwel niet gemakkelijk zijn. Bij gebrek aan duidelijkheid over de invulling van de 'voorzorgverplichting' van de verzekerde is lastig te onderbouwen dat daaraan niet is voldaan. Zoals ook in Staedion zal het advies van de deskundige daaraan in de weg kunnen staan, zeker nu er geen standaarden bestaan waaraan verzekerden zelf kunnen toetsen en het kennisniveau zodanig is dat verzekerden veelal vertrouwen op extern advies. Dit laat hen een grote beoordelingsvrijheid bij de inschatting van het gevaar. Door de voorzorgsverplichtingen concreter te beschrijven in de polisvoorwaarden en waar mogelijk expliciete uitsluitingen op te nemen, kunnen verzekeraars die beoordelingsvrijheid verkleinen en ongewenste situaties voorkomen.

5. Conclusie en aanbevelingen

In deze bijdrage is onderzocht hoe in een digitale context invulling kan worden gegeven aan de verzekeringsrechtelijke leerstukken eigen schuld en bereddingsplicht.

In beide leerstukken gaat het om een samenspel tussen de eigen verantwoordelijkheid van de verzekerde en de verwachtingen die de verzekeraar op dat punt heeft. Bij gebrek aan standaarden op het gebied van cybersecurity is het moeilijk om aan deze verantwoordelijkheden van de verzekerde invulling te geven. De verzekerde heeft een ruime beoordelingsvrijheid, waarbij hij bovendien mag afgaan op advies van deskundigen.

Hoewel de polisvoorwaarden van cyberverzekeringen onderling van elkaar verschillen, gaan de meeste polissen ervan uit dat de verzekerde in zekere mate 'redelijke voorzorgsmaatregelen' dient te treffen om schade te voorkomen. Welke voorzorgsmaatregelen redelijk zijn, hangt af van de

85 *Supra*, noot 31.

86 Dit kan met de in de polisvoorwaarden opgenomen schuldgradatie te maken hebben. Indien dat het wettelijk opzetcriterium ex artikel 7:952 BW is geweest, dan zou een beroep daarop weinig kans van slagen hebben gehad.

87 Zie Krenning & Vloemans, 'Bereddingskosten in het verzekeringsrecht/Sanering van woning in verband met asbestverontreiniging', *NTBR* 2008/1 (p. 21-25).

88 Als een wankele schoorsteen niet wordt gerepareerd, ontstaat op een gegeven moment vanzelf de situatie dat de schoorsteen naar beneden komt (acute schadeoorzaak) of het onmiddellijk dreigende gevaar dat dit zal gebeuren, vgl. Stadermann, *Enige vraagstukken van verzekeringsrecht*, Zutphen: Paris 2011, p. 86.

89 Zie op dit punt ook Krenning & Vloemans 2008, p. 23. Vergelijk ook HR 12 januari 2007, *NJ* 2007/371 (*Eindhoven/Allianz*).

90 Vgl. Wansink 2006, p. 306. Zie ook N. Vloemans, 'De bereddingsplicht', in: N. van Tiggele-van der Velde e.a. (reds.), *Bespiegelingen op 10 jaar 'nieuw' verzekeringsrecht*, Deventer: Wolters Kluwer 2015, p. 102-104. Zie ten aanzien van misbruik van verzekering HR 12 januari 2007, *NJ* 2007, 371, r.o. 4.1.2: "*Bij een verzekering als hier in het geding is niet uitgesloten dat feiten en omstandigheden die niet toereikend zijn om een beroep op art. 7:952 BW of een opzetclausule als de onderhavige te doen slagen, niettemin van dien aard zijn dat het naar maatstaven van redelijkheid en billijkheid onaanvaardbaar geacht moet worden dat de verzekerde aanspraak maakt op een uitkering onder de polis (art. 6:248 lid 2 BW).*"

concrete omstandigheden van het geval. De eisen en vragen die cyberverzekeraars stellen in de aanvraagfase vormen een indicatie van het cybersecurityniveau dat verzekeraars van hun verzekerden verlangen. Hoewel er over een aantal concrete maatregelen consensus lijkt te bestaan, zijn algemene (security)maatstaven aan de hand waarvan de zorgplicht van de verzekerde moet worden getoetst, of algemene minimumeisen waaraan de verzekerde dient te voldoen, moeilijk uit het geheel van voorschriften af te leiden. Evenmin is uit het geheel van voorschriften van de verzekeraar af te leiden of van de verzekerde organisatie een alomvattend cybersecuritybeleid mag worden verwacht, of dat het voldoende is dat er ad hoc maatregelen zijn getroffen.

Ten aanzien van bijzondere maatregelen direct nadat het verzekerde risico zich heeft verwezenlijkt, hebben de cyberverzekeraars het heft in eigen hand genomen door *incident response* – in de kern te beschouwen als bereddingsmaatregelen – in de primaire dekking te integreren. De inschatting welke acute maatregelen de verzekerde dient te treffen bij een verwezenlijkt risico laat de cyberverzekeraar dus niet aan haar verzekerde over.

Dit geldt niet voor situaties waarin de verwezenlijking van het gevaar ophanden is. Of daarvan sprake is en welke maatregelen dan getroffen moeten worden, hangt af van wat de verzekerde wist of behoorde te weten. Het herkennen van een onmiddellijk dreigend cybergevaar is echter verre van eenvoudig. Het kennisniveau van de meeste organisaties loopt structureel achter ten opzichte van de snelheid waarmee de techniek zich ontwikkelt. Wat in een digitale wereld moet worden gezien als een daadwerkelijk gevaar en welke maatregelen dan geboden zijn, is niet helder. Evenmin is helder hoe dit juridisch dient te worden beoordeeld. Uit de eerste rechtspraak die tegen deze materie aanschurkt, blijkt dat de juridische kijk op risico's niet gelijkloopt met de technische beoordeling daarvan.

Door de onduidelijkheden over de te treffen algemene voorzorgsmaatregelen en het ontstaan en herkennen van onmiddellijk dreigende gevaren door de verzekerde, zijn complexe samenloopdiscussies over schuld en bereddingsplicht denkbaar. De ICT-deskundige zal daarbij een belangrijke rol spelen.

Deze bevindingen leiden tot verschillende aanbevelingen voor de praktijk. Allereerst is samenwerking tussen en krachtenbundeling van verschillende disciplines van groot belang om digitale risico's beter beheersbaar en herkenbaar te maken is. Cyberverzekeraars zouden meer richting kunnen geven aan wat zij van hun verzekerden verlangen door meer invulling te geven aan open normen, eventueel met een bijlage bij de polis. Hierin zouden in het bijzonder technische maatregelen kunnen worden uitgewerkt. Deze lijst kan jaarlijks worden herzien (zie ook onder 3.4).

Daarnaast zouden cyberverzekeraars zich meer kunnen richten op het risicomanagement van hun verzekerde en kennis kunnen delen, bijvoorbeeld door preventieve diensten aan te bieden door technici en advocaten of juridisch experts. Dit helpt de verzekerde om beter te kunnen afbakenen welke maatregelen getroffen moeten worden en om onmiddellijk dreigende digitale gevaren te herkennen. In het kader van transparantie, de professionele hoedanigheid van de verzekeraar en diens veronderstelde kennisvoorsprong, mag dat ook van de verzekeraar worden verwacht.

Tot slot kan een betere harmonie tussen bestaande beveiligingsstandaarden, acceptatie-eisen en polisvoorwaarden leiden tot meer duidelijkheid over de verwachtingen van verzekeraars en verzekerden over en weer. Een standaard of keurmerk voor cybersecurity, bijvoorbeeld te ontwikkelen vanuit een publiek-private samenwerking, kan een vertrekpunt zijn voor het cybersecurityniveau waaraan iedere verzekerde minimaal dient te voldoen. Daarmee kan de 'voorzorgsverplichting' van de verzekerde eenduidiger worden ingevuld.