van waarschijnlijkheid – en niet met absolute zekerheid" voor de klanten bestemd zijn.[17] Daarmee lijkt de door A-G Szpunar gehanteerde waarschijnlijkheidstoets toch nog relevant.[18] In tegenstelling tot de A-G, gaat het Hof echter nauwelijks in op de vraag hoe waarschijnlijk dit in het concrete geval moet zijn. Om te voorkomen dat het door de wetgever geïntroduceerde onderscheid tussen "reguliere" en bijzondere persoonsgegevens (en de daarbij behorende beschermingsniveaus) verder vervaagt door een steeds ruimere interpretatie van die laatste categorie, was het voor de praktijk in het kader van de rechtszekerheid wenselijk geweest als het Hof een duidelijker criterium had gesteld ten aanzien van de vereiste mate van waarschijnlijkheid van de conclusies over de gezondheidstoestand van betrokkenen. Of een steeds bredere interpretatie van bijzondere persoonsgegevens voor betrokkenen daadwerkelijk tot een hoger beschermingsniveau leidt, is daarbij nog maar de vraag.[19]

S.P. Kloosterboer

Nederland

Computerrecht 2025/50

RECHTBANK NOORD-NEDERLAND
21 september 2022, C/19/131097 / HA ZA 20-82
(Mrs. L. Groefsema, C.J.R. de Locht en S. van Gessel)
m.nt. J. van Helden

(art. 7:401 BW, art. 6:74 BW, art. 6:75 BW, art. 6:99 BW)

ECLI:NL:RBNNE:2024:3519
ECLI:NL:RBNNE:2022:5577
ECLI:NL:RBNNE:2024:3520

Netwerkbeheerder is aansprakelijk voor schade als gevolg van een ransomware-aanval. De netwerkbeheerder heeft nagelaten in duidelijke bewoordingen te wijzen op het ontbreken van netwerksegmentatie, de kwetsbaarheid van de back-upvoorziening en het gebrekkige wachtwoordbeleid, en de daarmee gepaard gaande beveiligingsrisico's.

Tussenuitspraak in de zaak van:
1. **ENVIEM HOLDING B.V.,**
te Harderwijk,
2. **ENVIEM B.V.**,
te Harderwijk,
3. **TRANSNATIONAL BLENDERS B.V.**,
te Dordrecht,
4. **ENVIEM RETAIL HOLDING B.V.**,
te Harderwijk,
5. **ENVIEM RETAIL NEDERLAND B.V.**,
te Harderwijk,
6. **ENVIEM RETAIL B.V.**,
te Harderwijk,
7. **FASE FACILITY SERVICES B.V**,
te Harderwijk,
8. **OLIEHANDEL NEDERLAND B.V.**,
te Harderwijk,
9. **MAIN B.V.**,
te Amsterdam,
10. **ENVIEM WHOLESALE HOLDING B.V.**,
te Den Helder,
eisers in conventie,
verweerders in reconventie,
hierna samen te noemen: Enviem c.s.,
advocaat mr. A.W. Duthler te 's-Gravenhage,
tegen
1. **I-BEHEER ICT B.V.,**
te Coevorden, hierna ook te noemen: I-Beheer,
2. **I-BEHEER GROEP B.V.**,
te Coevorden,
gedaagden in conventie,
eisers in reconventie,
hierna samen te noemen: I-Beheer c.s.,
advocaat mr. G.A.C. van den Hout te Groningen.

1 **De procedure**

[…]

2 **De verdere beoordeling**

[…]
2.3. Per 1 januari 2010 is een overeenkomst gesloten met betrekking tot netwerkbeheer tussen I-Beheer ICT B.V. enerzijds en Gulf Harderwijk, die later is opgegaan in Enviem Retail B.V., anderzijds. Deze overeenkomst werd tot 2016 steeds stilzwijgend verlengd.
2.4. Op 13 januari 2016 is een nieuwe overeenkomst voor netwerkbeheer gesloten. Partijen bij deze nieuwe

17 Zie r.o. 90 van het arrest.

18 Het Hof wijdt in dit verband een paragraaf aan de mogelijkheid om de daadwerkelijke gebruiker (niet zijnde de klant) te identificeren. Zij noemt de situatie waarin de geneesmiddelen bij een ander persoon dan de klant worden afgeleverd of waarin een klant in het kader van de bestelling verwijst naar een andere identificeerbare persoon.

19 A-G Szpunar brengt deze vraag in par. 55 ook kort onder de aandacht, omdat de kwalificatie als bijzonder persoonsgegeven volgens hem paradoxaal genoeg juist tot de onthulling van meer gevoelige informatie kan leiden. A-G Bobek heeft in het verleden enigszins vergelijkbare zorgen geuit met betrekking tot de materiële reikwijdte van de AVG en zelfs betoogd dat het Hof of de Uniewetgever de werkingssfeer van de AVG op termijn opnieuw onder de loep zal moeten nemen, omdat een "overmatig ruime toepassing" (kort gezegd) tot rechtsonzekerheid en veronachtzaming van de wet kan leiden. Zie Concl. A-G Bobek, ECLI:EU:C:2021:822, bij HvJ EU 24 maart 2022, C-245/20, ECLI:EU:C:2022:216, par. 63-65.
Zie in dat verband ook Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176.

overeenkomst waren enerzijds I-Beheer ICT B.V. en anderzijds Enviem B.V. Deze overeenkomst is per 1 januari 2018 schriftelijk met twee jaar verlengd tot 31 december 2019, waarbij de omschrijving van de werkzaamheden en het aantal uren is uitgebreid. De overeenkomst behelsde preventief onderhoud, remote health check en 24x7 monitoring, voor een vast aantal uren per jaar. De tekst van deze verlengde overeenkomst luidt, voor zover hier van belang als volgt:
[…]

Omschrijving werkzaamheden binnen overeengekomen uren:

Preventief onderhoud: 1000 uur per jaar, 19 uur per week, waarvan om de week op locatie en om de week op afstand en waarvan 4 uur per week PO op afstand voor TNB en 7 uur per week op locatie TNB, Dordrecht voor algemene werkzaamheden. Tevens ook 1 uur per maand locatie Nigtevecht in combinatie met PO Main.

Dit houdt het volgende in:
- Back-up controle servers
- Harddisk controle servers
- Virusdefinities servers/werkstations
- Service pack / beveiligingsupdates
- Schoonmaak servers
- Inventarisatie gegevens bijwerken ASP

24*7 monitoring: 52 servers
- Monitoring van de capaciteit van het geheugen en beschikbaarheid
- Indien er een capaciteit probleem is, zal op Uitvoerder de Opdrachtgever schriftelijk adviseren over welke mogelijk (preventieve) oplossingen er zijn.

Remote health check op 38 servers: 228 uur per jaar, 19 uur per maand
- Controle op de serverlogs
- Controle op de server capaciteit
- Beveiliging van de ICT omgeving
- Back up
- Betrouwbaarheid/capaciteit

Remote Health Checks worden uitgevoerd op de volgende 38 servers:
[…]

2 Uitvoering van de overeenkomst

A) Uitvoerder moet bij zijn werkzaamheden de zorgen van een goed opdrachtnemer in acht nemen.
[…]

7 Security
A) Aangaande security dienen minimaal door Opdrachtgever de volgende maatregelen te zijn getroffen:
   - Deugdelijke antivirusbeveiliging;
   - Firewall.

B) Uitvoerder zal de deugdelijkheid van de security beoordelen en haar bevindingen aan Opdrachtgever mededelen.
C) Indien de security door Uitvoerder als niet deugdelijk wordt beschouwd, dan is Uitvoerder niet aansprakelijk voor enige schade die als gevolg van de niet deugdelijke security is ontstaan of in de toekomst kan ontstaan.
D) Uitvoerder kan op verzoek/aanvraag van Opdrachtgever zorgdragen voor een deugdelijke security. Deze aanvraag/opdracht zal worden behandeld als zijnde meerwerk als in art. 8 van deze overeenkomst.

[…]
2.9. Enviem B.V. is op 12 oktober 2019 getroffen door een ransomware aanval waarbij haar gegevensbestanden en ook haar back-up bestanden werden versleuteld. Hierdoor kon Enviem enige tijd niet meer bij haar bedrijfsgegevens en werd de bedrijfsvoering belemmerd. Enviem c.s. heeft de versleuteld geraakte bedrijfsinformatie deels kunnen laten reconstrueren uit snapshots die anderhalve week tevoren door I-Beheer waren gemaakt. Enviem c.s. heeft de aanvaller geen losgeld betaald.
2.10. Enviem c.s. heeft forensisch onderzoeksbureau NFIR ingeschakeld om onderzoek te verrichten naar de oorzaak en omvang van de ransomware aanval.
2.11. Per brief van 21 februari 2020 heeft Enviem c.s. I-Beheer in gebreke gesteld en de ontbinding ingeroepen van de overeenkomst voor netwerkbeheer.
[…]

3 **Het geschil**

[…]
3.2. Enviem c.s. legt aan haar vorderingen ten grondslag dat de ransomware aanval heeft kunnen plaatsvinden doordat I-Beheer toerekenbaar tekort is geschoten in haar contractuele verplichtingen jegens Enviem B.V. en in de op haar als opdrachtnemer rustende zorgplicht. I-Beheer is aansprakelijk voor de hierdoor ontstane schade.
I-Beheer heeft daarnaast jegens Enviem c.s. onrechtmatig gehandeld door haar bloot te stellen aan onaanvaardbaar grote ICT beveiligingsrisico's. I-Beheer heeft nagelaten de noodzakelijke maatregelen te nemen en Enviem c.s. te waarschuwen voor deze risico's. I-Beheer is aansprakelijk voor de schade die Enviem c.s. heeft geleden ten gevolge van de verwezenlijking van de risico's waaraan I-Beheer haar heeft blootgesteld. De schade bestaat uit de kosten van doorbetaling van niet-productieve werknemers, overuren van personeel voor herstelwerkzaamheden, kosten forensisch onderzoek en mitigatie door NFIR en kosten voor het inschakelen van derden.
Daarnaast stelt Enviem c.s. dat I-Beheer onjuiste en onterechte facturen aan Enviem heeft verstuurd, welke facturen Enviem onverschuldigd heeft voldaan, en dat I-Beheer

ten onrechte heeft nagelaten toegezegde creditfacturen te versturen en toegezegde kortingen te verrekenen.

3.3. I-Beheer c.s. voert verweer. Zij stelt haar verplichtingen jegens Enviem c.s. te hebben nageleefd zodat van toerekenbaar tekortschieten of onrechtmatig handelen geenszins sprake is geweest. Niet I-Beheer maar een ander bedrijf, Guardian 360, was verantwoordelijk voor de beveiliging van het netwerk van Enviem c.s. Causaal verband met de beweerde schade ontbreekt aangezien de oorzaak van de schade niet vast staat. Voorts geldt een beperking van aansprakelijkheid op grond van de toepasselijke algemene voorwaarden.

De betalingen die I-Beheer van Enviem c.s. heeft ontvangen, waren wel degelijk verschuldigd, behoudens een tweetal facturen die Enviem per abuis dubbel heeft voldaan. Er is sprake van rechtsverwerking.

I-Beheer c.s. concluderen tot niet-ontvankelijkheid van Enviem c.s., dan wel tot afwijzing van de vorderingen van Enviem c.s., met uitvoerbaar bij voorraad te verklaren veroordeling van Enviem c.s. in de kosten van deze procedure.

[…]

4. **De beoordeling**

[…]

Is I-Beheer tekortgeschoten in de nakoming van haar contractuele verplichtingen?

4.2. Enviem B.V. vordert van I-Beheer ICT B.V. vergoeding van schade als gevolg van toerekenbare tekortkoming in de nakoming van de netwerkbeheerovereenkomst. Enviem stelt dat de ransomware aanval heeft kunnen plaatsvinden door een zestal risicofactoren, te weten: er stonden RDP-poorten open; er werd geen zogenoemde whitelisting toegepast (waarbij alleen vooraf goedgekeurde IP-adressen toegang kunnen krijgen); de wachtwoorden die I-Beheer gebruikte voor het uitvoeren van het beheer voor de servers waren één en dezelfde en bovendien gemakkelijk te achterhalen; er was geen netwerksegmentatie doorgevoerd; updates van servers waren niet doorgevoerd; en een server die al jaren buiten service was en niet meer werd gebruikt, was niet uitgezet, maar hing nog steeds onbeveiligd aan het internet.

4.3 I-Beheer betwist dat zij dezelfde of zwakke wachtwoorden hanteerde en stelt dat updates van de servers wel waren doorgevoerd. I-Beheer erkent dat er RDP poorten open stonden, dat geen whitelisting werd toegepast en dat netwerksegmentatie ontbrak hoewel dit volgens I-Beheer wel nodig is. I-Beheer heeft tijdens de mondelinge behandeling aangegeven dat zij voor het backupsysteem hetzelfde wachtwoord gebruikte als voor het administrator account van de servers.

I-Beheer stelt dat zij Enviem heeft geadviseerd over deze risico's en dat Enviem haar adviezen en belangrijke offertes heeft genegeerd. I-Beheer betwist voorts dat de genoemde zes risicofactoren de oorzaak zijn geweest van de ransomware aanval. Volgens I-Beheer moet de oorzaak eerder worden gezocht in het binnenhalen van een virus door het openklikken van een besmette e-mail.

4.4. Enviem heeft ter onderbouwing van haar vorderingen slechts een managementsamenvatting overgelegd van het onderzoeksrapport van NFIR, hoewel zij beschikt over het volledige onderzoeksrapport. NFIR vermeldt in de managementsamenvatting dat het door de hoeveelheid mogelijke manieren van toetreding niet meer mogelijk is om precies vast te stellen via welke servers de hackers zijn binnengekomen. NFIR noemt als 'veelgebruikte methodes' het verspreiden van de malware middels een brute forceaanval op het Remote Desktop Protocol (RDP) of het uitbuiten van kwetsbaarheden in verouderde programmatuur, en schetst vervolgens welke factoren de netwerkomgeving van Enviem kwetsbaar maakten voor ongeautoriseerde toegang. Uit de NFIR managementsamenvatting volgt echter niet dat een van de genoemde zes risicofactoren of een combinatie daarvan daadwerkelijk de oorzaak is geweest van de ransomware aanval.

4.5. Hoe de hackers het netwerk van Enviem zijn binnengedrongen, kan naar het oordeel van de rechtbank echter in het midden blijven. Van belang is dat schade is ontstaan doordat bij de aanval niet alleen de werkbestanden maar ook de back-up bestanden van Enviem versleuteld zijn geraakt. Niet in geschil is dat de bedrijfsvoering van Enviem enige tijd belemmerd is geweest doordat Enviem niet meer bij haar systemen en bestanden kon, en dat hierdoor schade is ontstaan. Netwerksegmentatie, een beter wachtwoordbeleid en een deugdelijk afgescheiden back-upvoorziening hadden dat kunnen voorkomen.

4.6. Op grond van de netwerkbeheerovereenkomst was I-Beheer ICT B.V. verplicht om maandelijks de beveiliging van de ICT omgeving van Enviem B.V. en haar dochter-vennootschappen in Harderwijk, Dordrecht, Amsterdam en Den Helder te controleren en was zij ook verplicht om de deugdelijkheid van de security te beoordelen en haar bevindingen aan Enviem B.V. mee te delen. Gezien deze contractuele verplichtingen mocht van I-Beheer worden verwacht dat zij het ontbreken van netwerksegmentatie, de kwetsbaarheid van de back-up voorziening en het gebrekkige wachtwoordbeleid, en de daarmee gepaard gaande risico's, tijdig zou signaleren en haar bevindingen aan Enviem zou meedelen.

4.7. I-Beheer stelt weliswaar dat zij netwerksegmentatie en een beter wachtwoordbeleid heeft geadviseerd, maar gezien de betwisting door Enviem heeft I-Beheer dit verweer onvoldoende onderbouwd. I-Beheer heeft niet gesteld wie van Enviem zij heeft geadviseerd over een beter wachtwoordbeleid, hoe zij dat heeft gedaan en wat het advies concreet behelsde. I-Beheer verwijst naar een e-mail van 3 oktober 2019 waarin staat vermeld: "Wachtwoordbeleid nakijken Done, geen eenduidig beleid"

Daaruit blijkt niet dat I-Beheer Enviem heeft gewezen op de noodzaak om een beter wachtwoordbeleid toe te passen, heeft geadviseerd welke verbeteringen nodig zijn en heeft gewezen op de urgentie voor het nemen van maat-

regelen. Bovendien heeft I-Beheer voor de back-up gelijkluidende wachtwoorden gebruikt als voor het administrator account van de servers, zodat I-Beheer naar het oordeel van de rechtbank zelf heeft bijgedragen aan de kwetsbaarheid van de ICT voorziening.
Uit de stellingen van I-Beheer blijkt ook niet hoe en bij wie I-Beheer de noodzaak tot netwerksegmentatie bij Enviem heeft aangekaart. I-Beheer heeft verwezen naar een offerte van 14 maart 2019 die zij heeft uitgebracht aan Enviem Retail Nederland B.V. Deze offerte behelst de installatie en configuratie van een nieuwe ICT-omgeving met nieuwe hardware en de aansluiting op de bestaande netwerk. Blijkens het bijbehorende werkplan is een vorm van netwerksegmentatie en een veiligere back-upvoorziening weliswaar onderdeel van de geoffreerde nieuwe ICT-omgeving, maar uit de offerte blijkt niet dat I-Beheer de ondeugdelijkheid van de bestaande beveiliging en de noodzaak tot het nemen van maatregelen, laat staan de urgentie daarvan, aan Enviem heeft meegedeeld.
4.8. De rechtbank is van oordeel dat I-Beheer ICT B.V. jegens Enviem B.V. is toerekenbaar tekortgeschoten in haar verplichtingen uit de netwerkbeheerovereenkomst door Enviem niet in duidelijke bewoordingen te wijzen op het ontbreken van netwerksegmentatie, de kwetsbaarheid van de back-up voorziening en het gebrekkige wachtwoordbeleid, en de daarmee gepaard gaande beveiligingsrisico's. I-Beheer ICT B.V. is dan ook aansprakelijk voor de schade die Enviem B.V. ten gevolge van deze tekortkoming heeft geleden.
4.9. De rechtbank begrijpt uit de stelling van I-Beheer dat zij niet in gebreke is gesteld, dat I-Beheer meent dat zij niet in verzuim is komen te verkeren en daarom niet schadeplichtig is. Dat standpunt is onjuist. Het gaat hier om een netwerkbeheer-overeenkomst, die voor beide partijen voortdurende verplichtingen inhoudt. Indien een partij is tekortgeschoten in de nakoming van een dergelijke verplichting, kan deze – wellicht – in de toekomst alsnog worden nagekomen, maar daarmee wordt de tekortkoming in het verleden niet ongedaan gemaakt en wat deze tekortkoming betreft is nakoming dan ook niet meer mogelijk (vgl. HR 11 januari 2002, ECLI:NL:HR:2002:AD4925, *NJ* 2003, 255).
I-Beheer is gezien het bepaalde in artikel 6:74 BW dan ook wel degelijk schadeplichtig zonder dat daartoe – kort gezegd – een ingebrekestelling vereist is.
4.10. Dat ook de firma Guardian360 een rol had bij de ICT-beveiliging van Enviem, en daarin wellicht tekort is geschoten, doet niets af aan de eigen aansprakelijkheid van I-Beheer aangezien de schade in elk geval (ook) een gevolg is van het tekortschieten van I-Beheer (artikel 6:99 BW). Netwerksegmentatie, een beter wachtwoordbeleid en een deugdelijk afgescheiden back-upvoorziening hadden immers kunnen voorkomen dat bij de ransomware aanval ook de back-up bestanden versleuteld zouden raken.
4.11. De geleden schade bestaat volgens Enviem uit de kosten van doorbetaling van niet-productieve werknemers, overuren van personeel voor herstelwerkzaamheden, kosten van forensisch onderzoek en schadebeperking door NFIR en kosten voor het inschakelen van derden. Indien de rechtbank oordeelt dat op grond van de algemene voorwaarden de aansprakelijkheid van I-Beheer is beperkt tot € 50.000,- dan erkent I-Beheer dat de geleden schade in elk geval € 50.000,- bedraagt, zo gaf zij ter gelegenheid van de zitting te kennen. De rechtbank ziet daarin aanleiding om eerst het beroep op de exoneratieclausule te beoordelen alvorens te oordelen over de hoogte van de door I-Beheer verschuldigde schadevergoeding.

Is aansprakelijkheid van I-Beheer beperkt op grond van haar algemene voorwaarden?

[…]

5 **De beslissing**

[…]
Dit vonnis is gewezen door mrs. L. Groefsema, voorzitter, C.J.R. de Locht en S. van Gessel en uitgesproken op 21 september 2022 door de voorzitter in tegenwoordigheid van de griffier mr. K.M.N. Baurdoux.

Noot

1. Deze uitspraak gaat over de aansprakelijkheid van een netwerkbeheerder voor schade als gevolg van een ransomware-aanval. De uitspraak werd gedaan in 2022, maar werd pas recent gepubliceerd.
2. De rechtspraak over aansprakelijkheid voor schade als gevolg van cyberaanvallen is casuïstisch van aard. Of een IT-leverancier aansprakelijk is voor schade als gevolg van een cyberaanval hangt sterk af van de precieze inhoud van de contractuele afspraken en de omstandigheden van het geval. Het debat tussen partijen spitst zich vaak toe op de uitleg van contractuele afspraken over informatiebeveiliging, de reikwijdte van de zorgplicht van de IT-leverancier en de causaliteitsvraag, met vaak bijzondere aandacht voor verplichtingen aangaande het maken van een back-up.[1] Deze uitspraak is daarop geen uitzondering. De uitspraak is vooral interessant voor de vraag onder welke omstandigheden, en op welke wijze, een IT-leverancier moet waarschuwen voor beveiligingsrisico's.
3. Enviem B.V. (hierna: "Enviem"), een onderneming in de olie- en brandstoffensector die onder meer tankstations exploiteert, wordt op 12 oktober 2019 slachtoffer van een ransomware-aanval. De hackers slagen erin de werkbestanden en back-ups van Enviem te versleutelen waardoor de bedrijfsvoering van Enviem enige tijd ernstig wordt belemmerd. Uiteindelijk weet Enviem de versleutelde data weer te reconstrueren aan de hand van

1 Hof Amsterdam 28 april 2015, ECLI:NL:GHAMS:2015:1635; Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124; Hof Amsterdam 16 februari 2021, ECLI:NL:GHAMS:2021:508; Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731.

aanwezige 'snapshots' van de systemen, maar niet zonder substantiële schade te lijden. In deze procedure vordert Enviem van haar netwerkbeheerder, I-Beheer ICT B.V. (hierna: "I-Beheer"), vergoeding van de schade op grond van wanprestatie en onrechtmatige daad.

4. De rechtbank staat, enigszins ongebruikelijk, eerst stil bij de oorzaak van het incident en de causaliteitsvraag. Bij een cyberaanval kan lang niet altijd worden achterhaald hoe de aanvallers precies toegang hebben gekregen tot het netwerk. Voor beantwoording van die vraag zijn veelal logbestanden nodig. Die logging is niet altijd aanwezig of logbestanden zijn verloren gegaan na het uitschakelen van systemen. Ook in deze casus kon het *point-of-entry* niet met zekerheid worden vastgesteld. De rechtbank overweegt dat dit in het midden kan blijven. Volgens de rechtbank is voldoende dat de schade voorkomen had kunnen worden met behulp van netwerksegmentatie, een beter wachtwoordbeleid en een deugdelijk afgescheiden back-upvoorziening.

5. Deze benadering sluit aan bij andere voorbeelden uit de rechtspraak waaruit volgt dat onduidelijkheid over het *point-of-entry* niet in de weg hoeft te staan aan aansprakelijkheid van de IT-leverancier.[2] Waar de IT-leverancier verantwoordelijk is voor het treffen van mitigerende maatregelen, zoals netwerksegmentatie en back-ups, lijkt die opvatting mij ook juist. Een en ander sluit bovendien aan bij langlopende ontwikkelingen in het vakgebied informatiebeveiliging. Waar beveiliging voorheen vaak bestond uit enkel een harde buitenschil ('het kokosnoot-model'), bestaat informatiebeveiliging tegenwoordig uit meerdere beveiligingslagen waarbij ervan uit wordt gegaan dat aanvallers vroeg of laat ergens 'binnen' zullen komen ('het ui-model').

6. Na te hebben vastgesteld dat sprake is van csqn-verband tussen de schade en het ontbreken van o.a. netwerksegmentatie, gaat de rechtbank in op de inhoud van de verplichtingen van I-Beheer en de reikwijdte van de zorgplicht. In dit geval was in de desbetreffende overeenkomst uitdrukkelijk opgenomen dat I-Beheer de deugdelijkheid van de beveiliging zou beoordelen en haar bevindingen hierover aan Enviem zou mededelen. De rechtbank leidt hieruit af dat I-Beheer gehouden was om Enviem in duidelijke bewoordingen te wijzen op de aanwezigheid van eventuele beveiligingsrisico's. Een waarschuwingsplicht volgde in dit geval dus min of meer expliciet uit het contract.

7. I-Beheer erkende dat netwerksegmentatie ontbrak en dat dit een beveiligingsrisico was. Zonder netwerksegmentatie kunnen hackers, zodra zij eenmaal toegang hebben tot een netwerk, relatief eenvoudig door het netwerk bewegen en systemen binnen het netwerk infecteren. Door het gebrek aan segmentatie konden de aanvallers, zo lijkt het, bovendien relatief eenvoudig bij de back-up komen. Verder had I-Beheer erkend dat zij voor het beheer van het back-upsysteem hetzelfde wachtwoord gebruikte als voor het beheer van de operationele systemen. I-Beheer stelde echter dat zij Enviem wel degelijk over deze aspecten had geadviseerd. Hierbij verwees zij naar een e-mail met een korte opmerking over het nakijken van het wachtwoordbeleid en een door haar uitgebrachte offerte voor een nieuwe, gesegmenteerde ICT-omgeving. De rechtbank oordeelt echter dat uit deze stukken niet kan worden afgeleid dat I-Beheer Enviem in duidelijke bewoordingen heeft gewezen op deze beveiligingsrisico's, zodat sprake is van een tekortkoming.

8. Dit oordeel doet denken aan de uitspraak uit 2018 van de Rechtbank Amsterdam waarin een IT-leverancier ook een voorstel had gedaan voor een veiliger back-upvoorziening, op welk voorstel de klant niet was ingegaan, en waarna het de leverancier werd verweten dat deze niet indringend en herhaaldelijk had gewaarschuwd voor de risico's.[3] Tot een ander oordeel kwam de Rechtbank Overijssel, meer recent in 2023, in de kwestie van de *Gemeente Hof van Twente*. Hier oordeelde de rechtbank dat de kwetsbaarheid van de back-up voor rekening en risico bleef van de gemeente, doordat zij niet was ingegaan op het voorstel dat door de IT-leverancier was gedaan voor back-up hardening.[4] Dat het oordeel in laatstgenoemde uitspraak anders uitviel had er wellicht mee te maken dat de IT-leverancier in die kwestie al bij aanvang van de overeenkomst had gewaarschuwd voor het back-upsysteem en dit vrij nadrukkelijk nogmaals had gedaan in het latere voorstel. In die zin had de IT-leverancier de gemeente mogelijk wel "indringend en herhaaldelijk" gewaarschuwd.[5]

9. Al met al blijft het lastig manoeuvreren voor netwerkbeheerders in een speelveld waarin de dreigingen toenemen en de eisen aan informatiebeveiliging worden aangescherpt, zonder dat klanten ook altijd bereid zijn extra in beveiliging te investeren. Het devies blijft om met de klant duidelijke afspraken te maken over de verdeling van verantwoordelijkheden ten aanzien van informatiebeveiliging en uitdrukkelijk, herhaaldelijk en aantoonbaar (schriftelijk) te waarschuwen voor beveiligingsrisico's.

J. van Helden

2 Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124.

3 Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124.

4 Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731.

5 Een andere verklaring kan zijn gelegen in het feit dat de rechtbank signaleert dat er mogelijk beperkt ruimte bestaat om toepassing te geven aan het leerstuk van de zorgplicht wanneer een leverancier is geselecteerd op basis van een Europese aanbesteding, in verband met het transparantiebeginsel.