

ECLI:NL:RBAMS:2018:10124

Instantie	Rechtbank Amsterdam
Datum uitspraak	14-11-2018
Datum publicatie	07-06-2020
Zaaknummer	C/13/640668 / HA ZA 17-1380
Rechtsgebieden	Civiel recht
Bijzondere kenmerken	Eerste aanleg - enkelvoudig
Inhoudsindicatie	Geschil over aansprakelijkheid IT-bedrijf voor schade door ransomware bij klant
Vindplaatsen	Rechtspraak.nl

Uitspraak

—

vonnis

RECHTBANK AMSTERDAM

Afdeling privaatrecht

zaaknummer / rolnummer: C/13/640668 / HA ZA 17-1380

Vonnis van 14 november 2018

in de zaak van

de besloten vennootschap met beperkte aansprakelijkheid

O'CLIANCE B.V.,

gevestigd te Hilversum,

eiseres in conventie,

verweerster in reconventie,

advocaat mr. A.W. Duthler te 's-Gravenhage,

tegen

[gedaagde] ,

handelend onder de naam [bedrijf]

wonende te [woonplaats] ,

gedaagde in conventie,

eiser in reconventie,

advocaat mr. L.F.P. Coehorst te Utrecht.

Partijen zullen hierna O'Clance en [gedaagde] genoemd worden.

1 De procedure

1.1. Het verloop van de procedure blijkt uit:

- de dagvaarding van 12 december 2017, met producties,
- de conclusie van antwoord in conventie, tevens conclusie van eis in reconventie, met producties,
- de conclusie van antwoord in reconventie, waarvan de rechtbank - in tegenstelling tot [gedaagde] - een conform artikel 83 van het Wetboek van Burgerlijke Rechtsvordering ondertekende versie heeft ontvangen,
- het tussenvonnissen van 18 juli 2018, waarin een comparitie van partijen is bepaald,
- het proces-verbaal van comparitie van 5 oktober 2018.

1.1. Ten slotte is vonnis bepaald.

1 De feiten

1.1. O'Clance is een administratiekantoor. [gedaagde] verricht onder de naam [bedrijf] diensten op het gebied van IT en automatisering.

1.1. In 2009 heeft O'Clance [gedaagde] gevraagd een plan op te stellen voor de (her)inrichting van de IT-infrastructuur van O'Clance. Vervolgens heeft [gedaagde] in opdracht van O'Clance dit plan uitgevoerd en een nieuw netwerk geïnstalleerd. Na de aanleg heeft [gedaagde] herhaaldelijk beheer- en onderhoudswerkzaamheden aan het netwerk van O'Clance verricht.

1.1. Partijen hebben geen afspraken op schrift gesteld. [gedaagde] bracht voor zijn werkzaamheden maandelijks een vast bedrag van € 380,00 in rekening bij O'Clance. Als sprake was van nieuw aan te schaffen producten en/of installatiewerkzaamheden, werden deze separaat in rekening gebracht.

1.1. In een e-mail van 29 april 2010 schrijft [gedaagde] aan O'Clance:

“(..)

Als opmerking kan misschien nog vermeld worden dat we er misschien goed aan doen om die zwarte backup drive dubbelt uit te voeren, zodat eens in de week je die mee naar huis kan nemen zodat als er een keer brand uitbreekt je de data “thuis” hebt. Deze “need” is minder echter mijn inziens als de server achterstaat want dan hebben we een backup in de schuur (de zwarte doos naast het keyboard gaat dan mee naar achteren). Maar indien dit gebeurd is, hebben we

ook de snapshot drive boven in de meterkast (Acronisdrive).

Hoop dat je nu weer goed kan slapen. (..)"

1.1. Op 12 februari 2017 is O'Clance het slachtoffer geworden van een aanval met 'ransomware'. Daarbij zijn hackers doorgedrongen tot het netwerk van O'Clance en hebben zij alle bestanden op de server versleuteld, waaronder ook de back-upbestanden. Na betaling van drie bitcoins á € 963,61 per stuk heeft O'Clance weer toegang gekregen tot haar bestanden.

1.1. O'Clance heeft True-xs, een bedrijf gespecialiseerd in Cyber Security, nadien opdracht gegeven onderzoek te verrichten naar de vraag hoe de ransomware-aanval heeft kunnen plaatsvinden. True-xs concludeert, blijktens haar Bevindingenrapport onderzoek ransomware van 26 april 2017, onder meer het volgende:

"(..)

Met aan zekerheid grenzende waarschijnlijkheid kan True-xs zeggen dat op 12 februari 2017 om 16:55:09 er ingelogd is op de SBS-server met de account backoffice om vervolgens om 16:59:06 het uitvoerbare bestand "1.exe" op locatie "C:/Temp" te starten. Dit uitvoerbare bestand is later door [gedaagde] , met behulp van Malwarebytes Anti Malware, als ransomware aangeduid en verwijderd.

True-xs adviseert O'Clance om kritisch te kijken naar de inrichting van het netwerk. Uit gesprekken met [gedaagde] heeft True-xs geconstateerd dat het mogelijk was om via poort 443 een RDP-sessie op te kunnen zetten met het SBS-systeem (het zogenaamde Remote Web Workplace). In combinatie met het zwakke wachtwoord van het account backoffice was het een kwestie van tijd tot cybercriminelen toegang tot de SBS-server zouden krijgen.

(..)

Daarnaast adviseert True-xs om kritisch te kijken naar de inrichting van het netwerk. Deze digitale aanval had met eenvoudige maatregelen voorkomen kunnen worden. Door een combinatie toe te passen van eenvoudige maatregelen (wijzigen wachtwoorden gebruikers) en technische maatregelen (VPN-toegang) en het verbeteren van de back-upvoorziening kan O'Clance een nieuwe digitale aanval afslaan. Doordat de back-upvoorzieningen niet op de juiste manier ingeregeld waren heeft O'Clance losgeld betaald om bestanden weer terug te krijgen. Dit had voorkomen kunnen worden met een op de juiste manier ingeregelde backup."

True-xs heeft voor dit onderzoek een totaalbedrag van € 4.437,08 in rekening gebracht bij O'Clance.

1.1. Na de ransomware-aanval heeft [gedaagde] herstelwerkzaamheden verricht voor O'Clance. Voor deze werkzaamheden heeft hij op 23 februari 2018 € 6.854,12 aan O'Clance gefactureerd. O'Clance heeft de factuur onbetaald gelaten.

1 Het geschil

in conventie

1.1. O'Clance vordert - samengevat - dat de rechtbank bij vonnis, voor zover mogelijk uitvoerbaar bij voorraad,

I. verklaart voor recht dat [gedaagde] :

- toerekenbaar is tekortgeschoten in de nakoming van de verplichtingen uit de tussen partijen gesloten overeenkomst van opdracht;
- heeft gehandeld in strijd met haar zorgplicht op grond van artikel 7:401 van het Burgerlijk

Wetboek (hierna: BW);

- jegens O'Clance een onrechtmatige daad heeft gepleegd door een beroepsfout te maken in die zin dat hij zich niet heeft gedragen als een behoorlijk handelend vakbekwaam IT-deskundige;

II. [gedaagde] veroordeelt tot betaling van € 42.227,65 aan schadevergoeding, vermeerderd met de wettelijke rente daarover vanaf de dag der dagvaarding tot aan de dag der algehele voldoening;

III. [gedaagde] veroordeelt tot betaling van € 7.199,540 aan de buitengerechtelijke kosten, vermeerderd met de wettelijke rente daarover vanaf de dag der dagvaarding tot aan de dag der algehele voldoening.

1.1. O'Clance stelt ter onderbouwing van haar vorderingen onder meer dat zij [gedaagde] opdracht heeft gegeven een nieuwe en volledige IT-infrastructuur aan te leggen, te beheren en te onderhouden. Daaronder viel ook de beveiliging van het netwerk en op dat onderdeel van de opdracht is [gedaagde] toerekenbaar tekortgeschoten. Omdat de beveiliging niet in orde was, heeft de ransomware-aanval plaats kunnen vinden en heeft O'Clance schade geleden. Deze schade moet voor rekening van [gedaagde] komen.

1.1. De schade is door O'Clance als volgt begroot:

- omzetderving	€	8.080,00
- personeelskosten	€	14.417,73
- onderzoek door True-xs	€	4.437,07
- netwerkverbeteringen	€	12.366,50
- losgeld (bitcoins)	€	2.926,92

1.1. [gedaagde] voert verweer.

1.1. Op de stellingen van partijen wordt hierna, voor zover van belang, (nader) ingegaan.

in reconventie

1.1. [gedaagde] vordert samengevat – dat de dat de rechtbank bij vonnis, voor zover mogelijk uitvoerbaar bij voorraad, O'Clance veroordeelt tot betaling van € 6.854,12, vermeerderd met rente en kosten.

1.1. [gedaagde] legt aan zijn vordering ten grondslag dat hij na de ransomware-aanval in opdracht van O'Clance herstelwerkzaamheden heeft verricht en materiaal heeft geleverd en dat O'Clance op haar beurt niet aan de daaruit voortvloeiende betalingsverplichting heeft voldaan.

1.1. O'Clance voert verweer.

1.1. Op de stellingen van partijen wordt hierna, voor zover van belang, (nader) ingegaan.

1 De beoordeling

in conventie

de opdracht en de uitvoering daarvan

1.1. [gedaagde] heeft op de zitting erkend dat hij in opdracht van O'Clance een volledige IT-infrastructuur heeft aangelegd en, op afroep, het beheer en onderhoud daarvan verzorgde. Dat tussen partijen een afspraak bestond die inhield dat [gedaagde] een 'totaalpakket' zou leveren, is

dus niet in geschil. De vraag die partijen wel verdeeld houdt, is of ook de beveiliging van het netwerk deel uitmaakte van dat totaalpakket. Nu partijen hun afspraken niet op papier hebben gesteld, moet het antwoord op die vraag uit andere feiten en omstandigheden worden afgeleid. Daarbij is van belang wat partijen redelijkerwijs over de omvang van de opdracht hebben kunnen begrijpen en wat zij over en weer van elkaar mochten verwachten. De stelplicht (en eventuele bewijslast) dat de opdracht ook zag op het aanleggen van een adequate beveiliging rust op O'Clance, omdat zij zich beroept op de rechtgevolgen hiervan.

- 1.1. O'Clance voert in dit kader aan dat zij haar IT-infrastructuur volledig in handen van [gedaagde] heeft gelegd en dat de beveiliging daarvan vanzelfsprekend deel uitmaakte. Omdat O'Clance met gevoelige gegevens werkt, is een adequate beveiliging voor haar van groot belang en [gedaagde] was hiervan op de hoogte. O'Clance is afgegaan op de deskundigheid van [gedaagde], die altijd benadrukte dat het netwerk goed beveiligd was en in geval van calamiteiten binnen afzienbare tijd weer in gebruik zou kunnen worden genomen.
- 1.1. [gedaagde] voert ter betwisting aan dat hij wel beveiligingsmaatregelen heeft voorgesteld, maar dat al zijn voorstellen door O'Clance van de hand werden gewezen. In zijn aanvankelijke voorstel stond onder meer de aanleg van de firewall, maar dit is niet overgenomen in het uiteindelijke ontwerp omdat de [functie] en [functie] van O'Clance, [betrokkene] (hierna: [betrokkene]), tijdens de voorbereidende gesprekken aangaf dat hij dit te duur vond. Het voorstel van [gedaagde] om bij wijze van back-up met roulerende externe schijven te werken, gaf volgens [betrokkene] te veel gedoe. Bij gebrek aan toestemming heeft [gedaagde] noodgedwongen bepaalde beveiligingsmaatregelen achterwege gelaten en gemakkelijke wachtwoorden ingesteld. [betrokkene] was geen leek op computergebied en wist dus welke risico's aan zijn keuzes kleefden.
- 1.1. Naar het oordeel van de rechtbank heeft [gedaagde] hiermee onvoldoende gemotiveerd betwist dat O'Clance er vanuit is gegaan en mocht gaan dat [gedaagde] bij het vervullen van de opdracht een volledige IT-infrastructuur aan te leggen, tevens zorg zou dragen voor een adequate beveiliging. Daarbij overweegt de rechtbank dat het gelet op het gestelde en niet betwiste belang hiervan, moeilijk voorstelbaar is hoe onder de opdracht een totaalpakket te leveren niet tevens de aanleg van de daarbij behorende beveiliging kan zijn begrepen. Met hetgeen [gedaagde] heeft aangevoerd, wat daar feitelijk ook van zij, wordt bovendien niet zozeer betwist dat de opdracht tevens de aanleg van de beveiliging inhield, maar enkel dat [gedaagde] hier door toedoen van O'Clance niet in is geslaagd. De stelling van O'Clance dat de opdracht tevens het aanleggen van adequate beveiliging inhield, slaagt dus.
- 1.1. Door het netwerk aan te leggen zonder firewall en zonder externe back-ups, heeft [gedaagde] deze opdracht niet naar behoren uitgevoerd. Dat, zoals [gedaagde] stelt, O'Clance de voorgestelde beveiligingsmaatregelen van de hand zou hebben gewezen, maakt dit niet zonder meer anders. Het had dan op de weg van [gedaagde] gelegen de opdracht te weigeren wegens onuitvoerbaarheid, alternatieven aan te dragen of op zijn minst indringend en herhaaldelijk te waarschuwen voor de risico's die het achterwege laten van een firewall en externe back-upstructuur met zich meebrachten. Dat [betrokkene] wellicht zelf kennis van zaken op het gebied van IT had, ontsloeg [gedaagde] niet van deze verantwoordelijkheid. Gelet op de afspraak dat hij een totaalpakket inclusief beveiliging zou leveren, in combinatie met zijn professionele deskundigheid, kon hij niet volstaan met een enkele waarschuwing en berusten in de keuzes van O'Clance. Dat [gedaagde] meer heeft gedaan dan het geven van een enkele waarschuwing, is door hem niet, althans onvoldoende, gesteld. Uit de e-mail van 29 april 2010 blijkt juist het tegendeel. Dat [gedaagde] niet uitdrukkelijk heeft gewaarschuwd wordt nog eens onderstreept doordat [gedaagde] op de zitting heeft verklaard dat hij op de vraag of het systeem veilig genoeg was slechts zou hebben geantwoord: "*Er moeten nog een aantal dingen bij.*" [gedaagde] is hiermee toerekenbaar tekort geschoten in de uitvoering van zijn opdracht.

het causaal verband, verzuim en de eigen schuld

1.1. Zoals volgt uit 2.7 heeft True-xs op basis van haar onderzoek geconcludeerd dat de ransomware-aanval voorkomen had kunnen worden door een combinatie van technische maatregelen (firewall) en sterkere wachtwoorden. O'Clance beroept zich op dit rapport. [gedaagde] heeft op de zitting weliswaar verklaard dat een aanval als deze nooit kan worden uitgesloten, maar heeft daarbij erkend dat het met een goede beveiliging (waaronder sterke wachtwoorden) in ieder geval langer had geduurd voordat de hackers het netwerk hadden kunnen binnendringen en dat dit had kunnen maken dat de hackers de aanval hadden afgebroken. [gedaagde] heeft tevens erkend dat als er externe back-ups waren gebruikt, deze buiten het bereik van de ransomware waren gebleven en O'Clance haar activiteiten dan aanzienlijk sneller had kunnen oppakken, zonder betaling van bitcoins. [gedaagde] heeft als verweer gevoerd dat sprake is van eigen schuld van O'Clance, omdat zij de adviezen van [gedaagde] niet op wilde opvolgen. Voor zover [gedaagde] al iets te verwijten valt, geldt bovendien dat O'Clance hem nooit heeft aangespoord alsnog aan zijn verplichtingen te voldoen. Hij kan dus niet worden aangesproken voor de schade van O'Clance, aldus [gedaagde] .

1.1. [gedaagde] heeft de stelling van O'Clance dat het (het gevolg van) de ransomware-aanval voorkomen had kunnen worden als de juiste maatregelen waren getroffen hiermee onvoldoende gemotiveerd betwist. Zelfs als moet worden aangenomen dat het niet mogelijk is een dergelijke aanval met technische maatregelen volledig uit te sluiten, geldt dat met een externe back-upstructuur de gevolgen beperkt waren gebleven. Met betrekking tot het ontbreken van de firewall en externe back-upstructuur, heeft de rechtbank in 4.5 al overwogen dat [gedaagde] op dit punt te weinig inspanning heeft geleverd en dat het ontbreken van deze veiligheidsmaatregelen dus (geheel) voor zijn rekening moet komen. Nadat de ransomware-aanval eenmaal had plaatsgevonden, was nakoming bovendien blijvend onmogelijk geworden zodat [gedaagde] direct in verzuim was. De schade die O'Clance ten gevolge van deze tekortkoming in de nakoming door [gedaagde] heeft geleden, komt daarom op grond van artikel 6:74 BW in beginsel voor rekening van [gedaagde] .

1.1. Tussen partijen is echter niet in geschil dat naast het ontbreken van een firewall en externe back-upstructuur ook het gebruik van te gemakkelijke wachtwoorden heeft bijgedragen aan de gelegenheid voor geslaagde een ransomware-aanval. Met betrekking tot deze wachtwoorden staat bovendien vast dat [gedaagde] aanvankelijk complexe wachtwoorden had ingesteld, maar dat hij deze op uitdrukkelijk verzoek van O'Clance heeft vereenvoudigd. Op de zitting heeft [betrokkene] hierover verklaard dat hij herhaaldelijk met [gedaagde] over de wachtwoorden heeft gesproken en dat hij zich ervan bewust was dat het gebruik van simpele wachtwoorden risico's met zich bracht.

1.1. De stelling van [gedaagde] dat hij op dit onderdeel van de beveiliging wel voldoende inspanning heeft verricht, en dat de keuze van O'Clance voor gemakkelijke wachtwoorden mede debet is geweest aan de kwetsbaarheid voor een ransomware-aanval, is hiermee door O'Clance onvoldoende betwist. Dat de hackers zich mede door de gemakkelijke wachtwoorden toegang tot het netwerk van O'Clance konden verschaffen, is daarom een omstandigheid die voor rekening van O'Clance moet blijven.

1.1. Daarmee komt de rechtbank tot de conclusie dat [gedaagde] jegens O'Clance aansprakelijk is voor de schade die kon ontstaan doordat [gedaagde] niet heeft voldaan aan de opdracht een adequate beveiliging aan te leggen, maar dat O'Clance medeschuldig is aan het ontstaan van het lek in de beveiliging. De rechtbank zal de schade dan ook over beide partijen verdelen. Gelet op de mate waarin elk van de partijen aan de schade heeft bijgedragen, stelt de rechtbank de schadevergoedingsplicht van [gedaagde] vast op 2/3 van het geheel. Het overige deel van de schade blijft voor rekening van O'Clance.

de schade: omzetsderving en personeelskosten

- 1.1. O'Clance stelt dat zij na de ransomware-aanval gedurende de eerste week niet en gedurende de tweede week nauwelijks haar gebruikelijke werkzaamheden heeft kunnen verrichten en daardoor een omzetsderving van € 8.080,00 heeft geleden. Zij vordert tevens vergoeding van (een deel van) haar personeelskosten. O'Clance heeft deze posten onderbouwd met een overzicht waarin per medewerker het aantal gewerkte uren, het uurloon en - naar de rechtbank begrijpt - de misgelopen omzet per medewerker per uur is weergegeven.
- 1.1. [gedaagde] heeft aanvankelijk betwist dat O'Clance anderhalve week niet heeft kunnen werken, maar heeft op de zitting erkend dat het bij grote hoeveelheden data, zoals de drie terrabites waarmee O'Clance werkte, lang duurt voordat alle gegevens weer zijn teruggezet en het systeem weer 'up and running' is. [gedaagde] voert verder aan dat O'Clance uitsluitend gederfde winst en niet gederfde omzet zou kunnen vorderen, omdat O'Clance zich ook kosten heeft kunnen besparen en dat in ieder geval de compensatie voor de post personeelskosten al is inbegrepen in de omzetsderving.
- 1.1. [gedaagde] heeft hiermee de stelling van O'Clance dat zij als gevolg van de ransomware-aanval enige tijd buiten bedrijf is geweest en daarmee een bedrag van € 8.080,00 aan omzet is misgelopen, onvoldoende gemotiveerd betwist. In artikel 6:96 BW is bepaald dat vermogensschade zowel geleden verlies als gederfde winst omvat. Daarmee omvat de schade die voor vergoeding in aanmerking komt niet enkel de gederfde winst, maar ook de gemaakte kosten waartegenover, als gevolg van de schadeveroorzakende gebeurtenis, geen opbrengsten staan. O'Clance heeft niet gesteld waaruit deze kosten bestaan, anders dan uit personeelskosten. [gedaagde] heeft echter evenmin uiteengezet welke kosten O'Clance zich als gevolg van de ransomware-aanval zou (kunnen) hebben bespaard. Gelet op de aard van de bedrijfsactiviteiten van O'Clance en de relatief korte duur van de stillegging van de bedrijfsactiviteiten, gaat de rechtbank er vanuit dat de kostenbesparing voor O'Clance zeer gering tot nihil is geweest. De gederfde omzet is daarmee gelijk te stellen aan de optelsom van gederfde winst en gemaakte, niet terugverdiende, kosten (waaronder de personeelskosten), zodat het bedrag van € 8.080,00 in zijn volledigheid als schade kan worden aangemerkt. Voor een afzonderlijke vergoeding van de personeelskosten bestaat dan uiteraard geen grond meer.

schade: onderzoek door True-xs

- 1.1. O'Clance heeft ook vergoeding van de kosten voor het inschakelen van True-xs gevorderd. Volgens [gedaagde] zijn deze kosten onnodig gemaakt, aangezien hijzelf de oorzaak van de ransomware-aanval al had achterhaald.
- 1.1. Op grond van artikel 6:96, tweede lid, sub b, BW komen redelijke kosten ter vaststelling van schade en aansprakelijkheid voor vergoeding in aanmerking. Gelet op het (aanvankelijk vermoedelijke) aandeel van [gedaagde] in het ontstaan van de schade, bestond er voor O'Clance voldoende aanleiding om een deskundige derde onderzoek te laten doen naar de oorzaak van de ransomware-aanval. O'Clance heeft dit onderzoek dan ook in redelijkheid kunnen laten uitvoeren. Gesteld nog gebleken is dat de kosten die True-xs voor haar werkzaamheden in rekening heeft gebracht, niet redelijk zijn. De kosten van dat onderzoek ad € 4.437,07 zullen daarom worden aangemerkt als schade die voor vergoeding in aanmerking komt.

schade: verbeteringen aan het netwerk

- 1.1. O'Clance heeft na de ransomware-aanval DeLorentz & Partners B.V, verbeteringen aan het netwerk laten aanbrengen. Zo heeft zij onder meer een firewall laten plaatsen. [gedaagde] betwist dat deze kosten als schade kunnen worden aangemerkt.
- 1.1. Vast staat dat de beveiliging van het netwerk voorafgaand aan de ransomware-aanval onvoldoende was. Verder staat vast dat [gedaagde] kosten van nieuw aan te schaffen producten en/of installatiewerkzaamheden altijd los van de maandelijkse vaste vergoeding in rekening bracht bij O'Clance (zie 2.3). Als O'Clance de aanval had willen voorkomen, had zij daarom hoe dan ook

extra kosten moeten maken, onder meer voor het plaatsen van een firewall. O'Clance heeft niet gesteld dat de kosten van het aanleggen van de noodzakelijke beveiliging als gevolg van de ransomware-aanval hoger zijn uitgevallen dan zij aanvankelijk zouden zijn geweest. De kosten voor verbetering van het netwerk kunnen daarom niet worden aangemerkt als schade die een gevolg is van de tekortkomingen van [gedaagde] en komen om die reden niet voor vergoeding in aanmerking.

schade: betaling bitcoins

- 1.1. Tussen partijen is niet in geschil dat O'Clance drie bitcoins ter waarde van € 963,61 en daarmee een totaalbedrag van € 2.890,83 heeft moeten betalen om haar bestanden te ontsleutelen. Dit bedrag zal daarom worden aangemerkt als schade die voor vergoeding in aanmerking komt.

totale schade

- 1.1. De totale schade die voor vergoeding in aanmerking komt, bedraagt daarmee (€ 8.080,00 + € 4.437,07 + € 2.890,83=) € 15.407,90. [gedaagde] zal worden veroordeeld tot het vergoeden van 2/3 deel (€ 10.271,93) van deze schade.

verklaringen voor recht

- 1.1. O'Clance heeft niet toegelicht waarom zij naast de uit te spreken veroordeling tot vergoeding van haar schade, waarin reeds een oordeel omtrent het handelen van [gedaagde] ligt besloten, ook belang heeft bij de onder I gevorderde verklaringen voor recht. Dit deel van de vordering zal daarom worden afgewezen.

buitengerechtelijke kosten en wettelijke rente

- 1.1. O'Clance vordert vergoeding van buitengerechtelijke incassokosten, maar heeft niet gesteld dat zij buitengerechtelijke werkzaamheden heeft verricht of heeft laten verrichten. De vordering tot vergoeding van buitengerechtig incassokosten zal daarom worden afgewezen.
- 1.1. O'Clance vordert wettelijke rente over de schadevergoeding vanaf de dag van de dagvaarding. [gedaagde] heeft de verschuldigdheid van wettelijke rente niet betwist. De gevorderde rente is op grond van artikel 6:119 BW toewijsbaar als gevorderd, met dien verstande dat deze rente slechts berekend zal worden over het toegewezen deel van de hoofdsom.

proceskosten

- 1.1. [gedaagde] zal als de in conventie grotendeels in het ongelijk gestelde partij in de proceskosten worden veroordeeld. Omdat een aanzienlijk deel van het gevorderde bedrag wordt afgewezen, begroot de rechtbank de proceskosten aan de zijde van O'Clance op basis van het toegewezen bedrag op:
 - dagvaarding € 102,10
 - griffierecht € 1.924,00
 - salaris advocaat € 1.086,00 (2 punten × tarief € 543,00)totaal € 3.112,10
- 1.1. Verder zal [gedaagde] worden veroordeeld in de nakosten voor zover deze kosten op dit moment reeds kunnen worden begroot. De nakosten zullen worden begroot op de wijze zoals in de beslissing vermeld.
- 1.1. Anders dan O'Clance heeft gevorderd zal de wettelijke rente over de proceskosten en nakosten, zoals gebruikelijk en redelijk, eerst zijn verschuldigd vanaf veertien dagen na het vonnis en niet na acht dagen.

in reconventie

- 1.1. Tussen partijen staat vast dat [gedaagde] na de ransomware-aanval (herstel)werkzaamheden heeft verricht voor O'Clance, waaronder het plaatsen van een nieuwe server, en dat O'Clance hem hiervoor niet heeft betaald.
- 1.1. [gedaagde] vordert in reconventie betaling voor deze werkzaamheden alsmede de geplaatste server. O'Clance voert als verweer dat de werkzaamheden enkel zagen op herstel en beperking van de door [gedaagde] zelf veroorzaakte schade. De door [gedaagde] geplaatste server was destijds nodig voor het ontsleutelen van bestanden, maar wordt inmiddels niet meer door O'Clance gebruikt.
- 1.1. Uit het in conventie gegeven oordeel van de rechtbank dat [gedaagde] aansprakelijk is voor de schade van O'Clance, volgt tevens dat op hem een verplichting rustte om de schade ten gevolge van zijn handelen zoveel mogelijk te beperken. Partijen zijn het erover eens dat de werkzaamheden die [gedaagde] heeft verricht noodzakelijk waren om de bedrijfsvoering van O'Clance zoveel mogelijk doorgang te laten vinden. Daarmee is de schade van O'Clance, in de vorm van omzetverlies, beperkt. Omdat [gedaagde] verplicht was de schadebeperkende werkzaamheden te verrichten, kan hij geen aanspraak maken op betaling hiervoor door O'Clance. Dat O'Clance een eigen aandeel heeft in het ontstaan van de schade doet hier niet aan af. Weliswaar rustte ook op haar de (zelfstandige) verplichting maatregelen te treffen om de schade zoveel mogelijk te beperken, maar gelet op de hoedanigheid en deskundigheid van beide partijen lag schadebeperking in de vorm van het verrichten van herstelwerkzaamheden bij uitstek op de weg van [gedaagde] .
- 1.1. Ook het beroep van [gedaagde] op onrechtmatige verrijking door O'Clance slaagt niet. [gedaagde] heeft onvoldoende gesteld om aan te kunnen nemen dat O'Clance dankzij de werkzaamheden van [gedaagde] in een betere vermogenspositie is gebracht dan voor de ransomware-aanval. Dit geldt tevens voor de server, nu [gedaagde] niet heeft gesteld dat de server na de herstelwerkzaamheden op andere wijze door O'Clance in gebruik is genomen. O'Clance heeft bovendien op de zitting verklaard dat de server door [gedaagde] kan worden opgehaald.
- 1.1. De vordering in reconventie zal daarom worden afgewezen, met dien verstande dat O'Clance de server terug dient te geven aan [gedaagde] .
- 1.1. [gedaagde] zal als de in reconventie in het ongelijk gestelde partij in de proceskosten worden veroordeeld. De kosten aan de zijde van O'Clance worden begroot op € 461,00 aan salaris advocaat (2 punten × factor 0,5 × tarief € 461,00).

1 De beslissing

De rechtbank

in conventie

- 1.1. veroordeelt [gedaagde] om aan O'Clance te betalen een bedrag van € 10.271,93 vermeerderd met de wettelijke rente als bedoeld in art. 6:119 BW over het toegewezen bedrag met ingang van 12 december 2017 tot de dag van volledige betaling,
- 1.1. veroordeelt [gedaagde] in de proceskosten, aan de zijde van O'Clance tot op heden begroot op € 3.112,10, te vermeerderen met de wettelijke rente als bedoeld in art. 6:119 BW over dit bedrag vanaf veertien dagen na de datum van dit vonnis tot de dag van volledige betaling,
- 1.1. verklaart dit vonnis in conventie wat betreft de onder 5.1 en 5.2 genoemde beslissingen

uitvoerbaar bij voorraad,

in reconventie

1.1. veroordeelt [gedaagde] in de proceskosten, aan de zijde van O'Clance tot op heden begroot op € 461,00,

1.1. wijst het meer of anders gevorderde af,

In conventie en reconventie

1.1. veroordeelt [gedaagde] in de na dit vonnis ontstane kosten, begroot op € 246,00 aan salaris advocaat, te vermeerderen met de wettelijke rente vanaf de vijftiende dag na dit vonnis en te vermeerderen, onder de voorwaarde dat [gedaagde] niet binnen veertien dagen na aanschrijving aan het vonnis heeft voldaan en er vervolgens betekening van de uitspraak heeft plaatsgevonden, met een bedrag van € 82,00 aan salaris advocaat en de exploitkosten van betekening van de uitspraak, te vermeerderen met de wettelijke rente vanaf de vijftiende dag na betekening,

Dit vonnis is gewezen door mr. J.M.R. Vastenburg en in het openbaar uitgesproken op 14 november 2018.