30 Aansprakelijkheid voor digitale beveiligingsgebreken

Jeroen van Helden

Gebrekkige beveiliging van software kan leiden tot dataverlies, het stilvallen van hele productieomgevingen of het op afstand overnemen van kritieke infrastructuur. De gevolgen kunnen enorm zijn. In 2017 werd scheepvaartgigant Maersk slachtoffer van een ransomware aanval. Als gevolg daarvan kon wekenlang geen transport of overslag van containers plaatsvinden. Schade: 300 miljoen dollar aan gemiste omzet. Dichter bij huis werd de Universiteit Maastricht in 2019 slachtoffer van een cyberaanval. Studenten en medewerkers konden wekenlang niet meer bij hun bestanden en kregen pas weer toegang tot de systemen nadat de universiteit twee ton aan losgeld had betaald. Nadat het stof is neergedwarreld en het incident is afgehandeld, rijst onherroepelijk steeds dezelfde vraag: wie is aansprakelijk voor de schade? Dit hoofdstuk belicht deze vraag aan de hand van een fictieve casus van ziekenhuis Boerhaave.

Casus: slimme thermostaat

Ziekenhuis Boerhaave wil energiekosten besparen en besluit een slimme thermostaat aan te schaffen. De thermostaat is gefabriceerd door de firma ThermosX en wordt geleverd en geïnstalleerd door IT-leverancier ComputerAssistent, die ook de bedrijfsautomatisering van Boerhaave verzorgt. Bij de aanleg van de thermostaat laat ComputerAssistent na om het netwerk waar de thermostaat gebruik van maakt te scheiden van het bedrijfsnetwerk. De firmware van de slimme thermostaat bevat een kwetsbaarheid waardoor hackercollectief DarkForce toegang weet te krijgen tot de thermostaat. Vanuit de thermostaat dringen de hackers door in het bedrijfsnetwerk en voeren vervolgens een ransomware aanval uit.

Boerhaave heeft geen back-ups waar zij op kan terugvallen, maar weigert in eerste instantie te betalen. Daarop zetten de hackers een deel van het patiëntenbestand online, waaronder de gezondheidsgegevens van patiënt Herman. Als gevolg van de hack kan de geplande operatie van Herman ook niet doorgaan, waardoor hij gezondheidsschade oploopt. Boerhaave ziet zich gedwongen alsnog losgeld te betalen in de

vorm van 5 Bitcoin, omgerekend ruim € 200.000.[411] Een flinke schadepost. Boerhaave wil de schade verhalen op ThermosX en/of ComputerAssistent. Herman wil genoegdoening voor opgelopen letsel en inbreuk op zijn privacy.

Wanprestatie ComputerAssistent?

Boerhaave heeft alleen een overeenkomst met ComputerAssistent gesloten en kan dus alleen ComputerAssistent aanspreken op grond van wanprestatie (artikel 6:74 BW). Boerhaave zal dan moeten aantonen dat ComputerAssistent toerekenbaar tekort is geschoten in de nakoming van de overeenkomst door het netwerk onvoldoende te segmenteren en/of te voorzien van een ontoereikende back-upstructuur.

Het kan zijn dat partijen over dit soort aspecten expliciete afspraken hebben gemaakt, in welk geval deze afspraken bepalend zullen zijn voor de vraag of sprake is van wanprestatie. De kans is echter groot (zo leert de ervaring) dat partijen hierover geen (duidelijke) afspraken hebben gemaakt. Betekent dit dat een actie op basis van wanprestatie kansloos is? Nee, niet per se.

De inhoud van een overeenkomst bestaat uit hetgeen partijen *bedoeld hebben* overeen te komen (de zgn. Haviltex-formule). Redelijke verwachtingen over en weer spelen daarbij een belangrijke rol. Zodoende kunnen prestaties onderdeel uit gaan maken van een overeenkomst zonder dat daarover ooit met zoveel woorden is gesproken. Zo oordeelde de rechtbank Amsterdam in 2018 dat een klant die opdracht geeft tot levering van een 'totaalpakket' – bestaand uit de aanleg en het beheer en onderhoud van een bedrijfsnetwerk – mag verwachten dat een adequate beveiliging in de vorm van een firewall en adequate back-up structuur is inbegrepen.[412]

De overeenkomst op basis waarvan ComputerAssistent diensten verleent kwalificeert bovendien als een overeenkomst van opdracht zodat ComputerAssistent de zorg van een goed opdrachtnemer in acht moet nemen. ComputerAssistent moet zich met andere woorden als een redelijk bekwaam en redelijk handelend vakgenoot gedragen.[413] Deze zorgplicht kan vergaande consequenties hebben voor de aansprakelijkheid van een IT-dienstverlener bij beveiligingsgebreken. Illustratief is opnieuw de uitspraak van de rechtbank Amsterdam. In die casus had de IT-leverancier nota bene voorgesteld om extra beveiligingsmaatregelen te treffen in de vorm van een firewall en andere back-up structuur, maar had de klant deze maatregelen van de hand gewezen omdat deze te duur zouden zijn. In dat geval, zo oordeelt de rechtbank, had de leverancier de opdracht wegens onuitvoerbaarheid moeten weigeren,

411 Koers 15 september 2021.

412 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2018:10124. Een jaar later oordeelde diezelfde rechtbank dat een klant van een professioneel IT-dienstverlener mag verwachten dat deze werkt met inachtneming van de ISO/IEC 25010 standaard voor softwarekwaliteit, ook als dit niet expliciet is afgesproken, zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2019:9635.

413 P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', Computerrecht 2018/160.

alternatieven moeten aandragen, of indringend en herhaaldelijk moeten waarschuwen over de risico's.

Kelderluik-criteria

In 1961 viel een coca-cola bezorger in een Amsterdams café door een openstaand kelderluik en brak zijn been. De Hoge Raad formuleerde vervolgens de zogenoemde Kelderluik-criteria. Aan de hand hiervan kan worden beoordeeld of het creëren of laten voortbestaan van een gevaarlijke situatie dermate onzorgvuldig is dat sprake is van een onrechtmatige daad (artikel 6:162 BW). Rekening moet worden gehouden met de waarschijnlijkheid van onvoorzichtig gedrag, de kans dat ongevallen ontstaan, de ernst van de gevolgen en hoe bezwaarlijk het is om veiligheidsmaatregelen te treffen.

Voor zover bekend bevat de jurisprudentie geen voorbeelden van IT-leveranciers die op basis van deze doctrine aansprakelijk zijn gesteld voor gebrekkige informatiebeveiliging, maar ondenkbaar is het niet: de 'Kelderluik-jurisprudentie' is eerder met succes in stelling gebracht in aardbevingsschade-[414] en klimaatschade zaken[415].

ThermosX aansprakelijk als producent?

Naast het algemene leerstuk van de onrechtmatige daad kent de wet nog enkele bijzondere regelingen voor buitencontractuele aansprakelijkheid, waaronder die voor de producent van een gebrekkige zaak (artikel 6:185 e.v. BW). Deze regeling roept een risicoaansprakelijkheid in het leven voor fabrikanten ten faveure van consumenten. De huidige Nederlandse regeling over productaansprakelijkheid is gebaseerd op de Europese productaansprakelijkheid richtlijn (Richtlijn 85/374/EEG). Die regeling is in meerdere opzichten aan een update toe.

Zo gaat de richtlijn uit van een duidelijk onderscheid tussen enerzijds producten en anderzijds diensten. Kenmerkend voor de digitale revolutie is nu juist dat de scheidslijn tussen producten en diensten steeds meer is komen te vervagen. Producten en dienstverlening zijn steeds meer met elkaar verweven geraakt. Software wordt in toenemende mate geleverd 'als dienst' en is tegelijkertijd op allerlei manieren geïntegreerd in producten of daarmee verbonden. Dit betekent dat software een materieel product gebrekkig kan maken en tot fysieke schade kan leiden. Denk aan gebrekkige autosoftware als gevolg waarvan een rempedaal niet werkt en een ongeluk ontstaat.

Een producent is nu bovendien niet aansprakelijk wanneer het gebrek niet bestond op het tijdstip waarop het product in het verkeer werd gebracht. Dit uitgangspunt is logisch en begrijpelijk voor de traditionele producent. Een meubelmaker die een fauteuil verkoopt verliest daarmee de controle over het product,

414 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2019:1278.
415 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2021:5337.

zodat gebreken die nadien ontstaan niet voor zijn risico behoren te komen. De fabrikant van een IoT-apparaat daarentegen behoudt ook na verkoop controle over het product, doordat hij de mogelijkheid heeft (beveiligings)updates uit te brengen. In dat geval bestaat er geen (in ieder geval minder) reden de risicoaansprakelijkheid voor gebreken te beperken tot die gebreken die bestonden op het tijdstip waarop het product in omloop werd gebracht.[416]

Tot deze conclusies komt ook de Europese Commissie in een verslag over de vraag of de huidige kaders voor aansprakelijkheid voldoende zijn toegerust op ontwikkelingen als kunstmatige intelligentie (KI), het internet der dingen (IoT) en robotica.[417] Het Europees Parlement heeft de Commissie inmiddels opgeroepen de richtlijn op bovengenoemde en andere punten te heroverwegen.[418]

Geen vermogensschade vergoeding

Terug naar onze casus. De vermogensschade die Boerhaave heeft geleden als gevolg van de hack komt niet voor vergoeding in aanmerking op grond van productaansprakelijkheid, maar de gezondheidsschade van Herman eventueel wel. Herman zal in dat geval moeten aantonen dat de thermostaat "*niet de veiligheid biedt die men daarvan mag verwachten*" (artikel 6:186 eerste lid BW). Van een producent van IoT-apparaten lijkt verwacht te mogen worden dat firmware beschermt tegen veel voorkomende kwetsbaarheden. Toch zou het nog weleens lastig en kostbaar kunnen zijn voor Herman om aan te tonen hoe de schade is ontstaan en dat ThermosX als producent daar (deels) voor verantwoordelijk is. Reden waarom de Uniewetgever ook nadenkt over het vergemakkelijken van de bewijslast voor slachtoffers van KI/IoT-gerelateerde schade.

Privacyschending?

Herman is ten slotte verbolgen over het feit dat zijn medische gegevens met naam en toenaam online zijn gezet. Op grond van de Algemene verordening gegevensbescherming (AVG) heeft eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de AVG "*het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade*" (artikel 82 AVG). In dit geval is Boerhaave verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens van Herman en is ComputerAssistent bij de verwerking daarvan betrokken als verwerker. Herman zou kunnen overwegen

416 Vgl. EU Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and other emerging digital technologies, 2019.

417 VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD EN HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ, Verslag over de gevolgen van kunstmatige intelligentie, het internet der dingen en robotica op het gebied van veiligheid en aansprakelijkheid, COM/2020/64 final.

418 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

om een van hen, of hen beide, aan te spreken op grond van artikel 82 AVG. Daarvoor is kort samengevat nodig dat Herman aantoont dat deze partijen nagelaten hebben passende beveiligingsmaatregelen te treffen overeenkomst artikel 32 AVG. Uit de rechtspraak blijkt dat immateriële schadevergoeding kan worden toegekend voor een overtreding van de AVG, maar de omvang daarvan is doorgaans beperkt: meestal niet meer dan enkele honderden euro's.[419]

Conclusie

Uit de fictieve casus van ziekenhuis Boerhaave blijkt dat het Nederlandse recht diverse gronden kent op basis waarvan een IT-leverancier aansprakelijk gesteld kan worden voor een digitaal beveiligingsgebrek. In dit artikel zijn achtereenvolgens de revue gepasseerd: wanprestatie, onrechtmatige daad, productaansprakelijkheid en aansprakelijkheid op grond van de AVG. Toch is het aantal rechtszaken over gebrekkige informatiebeveiliging in Nederland (en overigens ook elders in de Europese Unie en in de Verenigde Staten) nog altijd betrekkelijk gering. Hoe komt dat?

Een deel van de verklaring zal te maken hebben met een gebrek aan *normering*. Voorwaarde voor het ontstaan van aansprakelijkheid is steeds dat op enigerlei wijze een norm is geschonden (een contractuele afspraak, een ongeschreven zorgvuldigheidsnorm, een AVG-verplichting, et cetera). Zonder normschending geen aansprakelijkheid. Lange tijd bestonden dergelijke normen niet of waren normen onduidelijk of onbekend. Maar inmiddels ontstaat een steeds fijnmaziger en gestroomlijnd normenkader. Denk aan de ISO/IEC 27002 standaard voor informatiebeveiliging, de OWASP Top 10 voor beveiliging van webapplicaties of de richtsnoeren voor beveiliging van persoonsgegevens van het College Bescherming Persoonsgegevens (CBP). Dergelijke normen vertegenwoordigen een brede consensus over beveiligingsrisico's en te treffen veiligheidsmaatregelen. Deze normen kunnen expliciet van toepassing worden verklaard op een overeenkomst of in stelling worden gebracht ter onderbouwing van een onrechtmatige daadsactie. Denk ook aan de methode Grip op Secure Software Development die binnen het Centrum Informatiebeveiliging en Privacybescherming (CIP) van de overheid is ontwikkeld en dat bestaat uit concrete, testbare en in aanbestedingen en contractmanagement afdwingbare productеisen.[420] Of aan het onderzoek dat nu wordt uitgevoerd door de Onderzoeksraad voor Veiligheid (OVV) naar de gang van zaken rondom een beveiligingslek in de software van Citrix.[421]

Deze en andere initiatieven zijn aanbevelenswaardig en zouden nog meer navolging moeten krijgen. Met behulp van standaarden en *best practices* op het gebied van informatiebeveiliging kunnen inkopers scherper over digitale veiligheid con-

419 Zie bijvoorbeeld http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RVS:2020:898.
420 https://www.cip-overheid.nl/media/1500/20200720-ssd-normen-v30.pdf.
421 https://www.onderzoeksraad.nl/nl/page/17171/beveiligingslek-citrix.

tracteren en kunnen juristen beter adviseren over de haalbaarheid van claims. Dit alles vergemakkelijkt uiteindelijk de gang naar die ultieme normsteller: de rechterlijke macht.

Attentiepunten

- **100% veiligheid bestaat niet.** Een hack als zodanig betekent niet automatisch dat de leverancier van de software of de beheerder van het netwerk aansprakelijk is.[422] Daarvoor is nodig dat de IT-leverancier een norm op het gebied van informatiebeveiliging heeft geschonden.

- **Zorgplicht**. De overeenkomst op basis waarvan IT-diensten worden verleend kwalificeert vaak als een overeenkomst van opdracht zodat de IT-dienstverlener de zorg van een goed opdrachtnemer in acht moet nemen. Dit kan betekenen dat op de IT-dienstverlener een vergaande waarschuwingsplicht rust, ook ten aanzien van beveiligingsrisico's. Het niet in acht nemen van deze waarschuwingsplicht kan leiden tot aansprakelijkheid.

- **Productaansprakelijkheid**. De regeling voor productaansprakelijkheid is geschreven voor traditionele producten en businessmodellen die niet goed aansluiten bij de manier waarop moderne leveranciers van digitale technologie hun producten aan de man brengen. Een update van de regeling is inmiddels wenselijk.

422 Zo erkende het Hof Arnhem-Leeuwarden in 2019 dat uiteindelijk ieder computersysteem gehackt kan worden, zodat een klant in principe geen volledig 'hackvrij' systeem mag verwachten, zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2018:7967.