

van [Y] van 7 maart 2017 (prod. 8.5). Het verweer dat causaal verband zou ontbreken wordt dan ook verworpen.

2.10.2. Het bedrag aan losgeld staat naar het oordeel van het hof in causaal verband met de tekortkoming; deze schadepost kan bovendien als gevolg van de tekortkoming aan [geïntimeerde] worden toegerekend. [appellante] werd immers als gevolg van het ontbreken van een back-up ertoe gedwongen het losgeld te betalen.

2.10.3. Voldoende aannemelijk acht het hof voorts dat ook [appellante] zelf, mede in aanmerking genomen zijn schadebeperkingsplicht, de nodige uren heeft moeten spenderen aan het oplossen van de problemen waartoe het ontbreken van de back-up had geleid. De gespecificeerde urenspecificatie (80 uur à € 80,- per uur; prod. 10) is naar het oordeel van het hof toereikend. De door [appellante] uitgesproken verwachting dat de productie op 22 juli 2016 hervat kon worden, brengt niet mee dat [appellante] na die datum geen kosten heeft moeten maken ter beperking van de schade; het hof verwijst naar de urenspecificatie.

2.10.4. Het vorenstaande brengt mee dat alle schadeposten in causaal verband staan met de tekortkoming en dat deze als gevolg ervan aan [geïntimeerde] kunnen worden toegerekend.

2.11. [geïntimeerde] heeft betoogd dat (een groot deel van) de schade het gevolg is van feiten en omstandigheden die moeten worden toegerekend aan [appellante] zelf. Op goede gronden wijst [geïntimeerde] erop dat [appellante] zelf ervoor heeft gekozen het nieuwe contract met [Y] in te laten gaan op 1 augustus 2016; dat was bijna zes weken na het einde van de SLA. Toen het bedrijf van [appellante] op 19 juli 2016 werd gehackt, was [geïntimeerde] bijna een maand niet meer verantwoordelijk voor de beveiliging van het systeem. Tegen die achtergrond acht het hof het feit dát [appellante] gehackt kon worden in overwegende mate aan [geïntimeerde] zelf toe te rekenen. Ook indien wel een back-up van (kort voor) 21 juni 2016 aanwezig was geweest, had [geïntimeerde] enige schade geleden die in dat geval geheel aan haar zou zijn toe te rekenen. De omstandigheid dat [appellante] niet onmiddellijk losgeld heeft betaald, maar pas op het moment dat de teller letterlijk bijna op nul stond – de hackers dreigden het systeem van [appellante] onherstelbaar te beschadigen op het moment dat de klok naar nul was afgelopen – acht het hof evenwel niet een omstandigheid die aan [appellante] moet worden toegerekend; naar [appellante] onbestreden heeft aangevoerd, had de politie haar met klem aangeraden helemaal geen losgeld te betalen.

Een en ander afwegend, komt het hof tot de slotsom dat twee/derde van de door [appellante] geleden schade het gevolg is van feiten en omstandigheden die aan haarzelf kunnen worden toegerekend.

(...)

2.18. De grieven 1 en 6 slagen. Het vonnis waarvan beroep zal worden vernietigd, voor zover dit betrekking heeft op de vordering van [appellante] op [geïntimeerde]. [geïntimeerde] zal worden veroordeeld tot schadevergoeding als hierna te bepalen. De vordering tot betaling van

btw zal worden afgewezen, nu over een schadevergoeding geen btw verschuldigd is. [geïntimeerde] zal als in het ongelijk gestelde partij worden verwezen in de kosten van het geding in beide instanties.

3. *Beslissing*

Het hof:

3.1. vernietigt het vonnis waarvan beroep, voor zover dit betrekking heeft op de vordering van [appellante] op [geïntimeerde], en in zoverre opnieuw rechtdoende:

3.1.1. veroordeelt [geïntimeerde] tot betaling, binnen veertien dagen na betekening van dit arrest, van een bedrag groot € 5.754,09 aan schadevergoeding, te vermeerderen met wettelijke rente over dat bedrag met ingang van 10 maart 2017 tot aan de dag van voldoening;

3.1.2. veroordeelt [geïntimeerde] tot betaling in de onderzoekskosten van deskundigen [Z] IT, groot € 2.011,63, te vermeerderen met de wettelijke rente, indien niet binnen veertien dagen na betekening van dit arrest aan deze veroordeling is voldaan;

3.2. bekrachtigt het vonnis waarvan beroep voor het overige;

(...)

3.4. verklaart deze veroordelingen uitvoerbaar bij voorraad;

3.5. wijst af het meer of anders gevorderde.

Noot van de redactie

Zie de annotatie van mr. C.K. van Lavieren, onder *Computerrecht 2022/7*.

Computerrecht 2022/9

HOF DEN HAAG

26 augustus 2021, 22-000130-18

(Mrs. Chr.A. Baardman, J.W. van den Hurk en F.W. van Lotum)

m.nt. M. Berndsen¹

(Art. 94, 95, 96, 104 lid 1, 148, 359a Sv; art. 8 EVRM; art. 7, 8, 11 Handvest)

ECLI:NL:GHDHA:2021:1873

Vervolg op de smartphonearresten van de Hoge Raad. Het hof verfijnt het besliskader voor onderzoek aan gegevens. Als te voorzien is dat door onderzoek van die gegevens een min of meer compleet beeld van aspecten van het privéleven van de gebruiker wordt verkregen, gelden nadere regels. De rechter-commissaris dient dan

¹ Mr. M. Berndsen is strafrechtadvocaat bij Meijers Canatan Advocaten te Amsterdam en specialiseert zich onder meer in cybercrime.

te beoordelen of bepaalde beperkingen aan dat onderzoek worden verbonden. Het arrest noemt beperkingen die de R-C kan aanbrengen en gezichtspunten die daarbij kunnen worden betrokken. Dit arrest lijkt de bevoegdheid van de officier van justitie om zulk onderzoek te gelasten verder te beperken.

Arrest in de zaak van 26 augustus 2021 (onderzoek 26Mei-berg)

Tenlastelegging

[...]

Dit betreft kort samengevat dat de verdachte:

Feiten 1, 2 en 3 (Marktplaats)

zich in de periode van 13 maart 2014 tot en met 26 oktober 2015 schuldig heeft gemaakt aan het in vereniging plegen van:

- oplichting door middel van phishing ten aanzien van 319 Marktplaats- of Admarkt-accounts (feit 1);
- computervrederebreuk ten aanzien van 319 Marktplaats- of Admarkt-accounts (feit 2);
- manipulatie van computergegevens ten aanzien van 319 Marktplaats- of Admarkt-accounts (feit 3);

feit 4 (BCC)

zich in de periode van 13 maart 2014 tot en met 26 oktober 2015 schuldig heeft gemaakt aan het in vereniging plegen van oplichting van minstens 96 personen met behulp van malafide webwinkels die leken op webwinkels van BCC;

feit 5 (Dixons)

zich in de periode van 2 juni 2014 tot en met 26 oktober 2015 schuldig heeft gemaakt aan het in vereniging plegen van oplichting van minstens 131 personen met behulp van malafide webwinkels die leken op webwinkels van Dixons;

feit 6 (GSM-wijzer)

zich schuldig heeft gemaakt aan het in vereniging plegen van oplichting van minstens 46 personen met behulp van een malafide webwinkel die leek op een webwinkel van GSM-wijzer, pleegperiode 17 december 2014 tot en met 26 oktober 2015 en/of aan poging tot oplichting van een of meerdere onbekend gebleven personen met behulp van malafide webwinkels die leken op webwinkels van GSM-wijzer, gepleegd op of omstreeks 12 maart 2015;

feiten 7 en 8 (Scrypt.cc)

zich in de periode van 19 tot en met 22 juni 2015 schuldig heeft gemaakt aan het in vereniging plegen van:

- computervrederebreuk ten aanzien van Scrypt.cc (feit 7);
- diefstal van BTC 629,95 van Scrypt.cc (feit 8);

feiten 9 en 10 (Hoogstra Autosport)

zich schuldig heeft gemaakt aan het in vereniging plegen van:

- computervrederebreuk ten aanzien van Hoogstra Autosport, pleegperiode 1 tot en met 12 juni 2015 (feit 9);
- poging tot afpersing van Hoogstra Autosport en [slachtoffer 1], pleegperiode 5 tot en met 12 juni 2015 (feit 10);

feiten 11 t/m 14 (Phonespot)

zich in de periode van 11 november 2014 tot en met 31 mei 2015 schuldig heeft gemaakt aan het in vereniging plegen van:

- computervrederebreuk ten aanzien van Phonespot, pleegperiode 11 november 2014 tot en met 31 mei 2015 (feit 11);
- oplichting door middel van phishing van minstens 8 personen met behulp van de webwinkel van Phonespot, pleegperiode 11 november 2014 tot en met 26 oktober 2015 (feit 12);
- het voorhanden hebben van toegangscodes tot geautomatiseerde werken van Phonespot, pleegperiode 11 november 2014 tot en met 31 mei 2015 (feit 13);
- poging tot afpersing van Phonespot, Media Center Rotterdam en [slachtoffer 2], pleegperiode 11 tot en met 17 november 2014 (feit 14);

feit 15 (witwassen)

zich in de periode van 13 maart 2014 tot en met 26 oktober 2015 schuldig heeft gemaakt aan het in vereniging plegen van witwassen.

[...]

Namens de medeverdachte [verdachte 1] is een verweer gevoerd met betrekking tot de rechtmatigheid van het onderzoek van zich op digitale gegevensdragers bevindende gegevens en daarmee samenhangend de bruikbaarheid van de bevindingen uit dat onderzoek voor het bewijs. Nu deze bevindingen ook relevant zijn voor (onderdelen van) de bewijsoverwegingen met betrekking tot de verdachte zal het hof zich in dit geval ambtshalve omtrent deze kwestie uitlaten.

In de eerste plaats dient te worden beoordeeld of, zoals door het openbaar ministerie is betoogd, indien eenmaal sprake is van rechtmatig door de rechter-commissaris in beslag genomen voorwerpen, uit (de uitoefening van) die bevoegdheid zonder meer voortvloeit dat de gegevens op die gegevensdragers ongeclausuleerd mochten worden onderzocht.

Hoewel een dergelijk standpunt in zijn algemeenheid houdbaar is, geldt dat niet onverkort – zo begrijpt het hof de arresten van de Hoge Raad van 4 april 2017 (ECLI:NL:HR:2017:584; ECLI:NL:HR:2017:588; ECLI:NL:HR:2017:592) – indien het onderzoek van de gegevens op een digitale gegevensdrager zo verstrekkend is dat op voorhand is te voorzien dat een min of meer compleet beeld kan worden verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van die gege-

vensdrager. In dat geval zal door de rechter-commissaris die de inbeslaggenomen gegevensdragers voor onderzoek overdraagt aan een opsporingsdienst, moeten worden bepaald of wel of niet beperkingen aan dat onderzoek worden verbonden. Bij die beslissing en bij het bepalen van aard en omvang van die eventuele beperkingen zullen factoren als de ingrijpendheid van de inbreuk op de persoonlijke levenssfeer van de gebruiker van de betreffende gegevensdragers door het onderzoek en de proportionaliteit en subsidiariteit van de te verrichten onderzoekshandelingen in relatie tot de aard en omvang van de verdenking waarop het onderzoek betrekking heeft een rol kunnen spelen. Daarbij kan onder meer worden gedacht aan beperkingen betreffende het aantal te onderzoeken gegevensdragers, beperkingen betreffende de te onderzoeken gegevens (zoals afbeeldingen, communicatie, internetgedrag et cetera) en beperkingen betreffende de periode waarbinnen de te onderzoeken gegevens zijn gegenereerd of op de betreffende digitale-gegevensdrager terecht zijn gekomen. Ook kan worden gekozen voor fasering van toegestane onderzoekshandelingen doordat de rechter-commissaris eventueel tussentijds beslist tot uitbreiding of (verdere) beperking van het toegestane onderzoek.

In het onderhavige geval heeft een dergelijke toetsing niet kenbaar plaatsgevonden. Het proces-verbaal van doorzoeking bij de medeverdachte [verdachte 1] vermeldt slechts dat na telefonische opening en sluiting van de doorzoeking door de rechter-commissaris de in beslag genomen voorwerpen voor nader onderzoek zijn overgedragen aan de teamleider van het onderzoeksteam Meiberg. Tegen die achtergrond is thans slechts een beoordeling achteraf mogelijk van de vraag of de rechter-commissaris toestemming zou hebben gegeven voor het onderzoek van de gegevens op de digitale gegevensdragers van verdachte en de medeverdachte [verdachte 1], zoals dat heeft plaatsgevonden. Daartoe overweegt het hof het volgende.

Op basis van het dossier laat dit onderzoek zich in drie fasen onderverdelen.

In de eerste fase is op 24 februari 2016 hoofdzakelijk een aantal Skype-gesprekken onderzocht die waren vastgelegd op de Asus laptop en de SD-kaart. Op dat moment was de verdachte nog niet als zodanig aangemerkt. Uit het proces-verbaal waarin over dit onderzoek wordt gerelateerd blijkt dat dit niet specifiek op de verdachte was gericht, maar op de namen van enkele medeverdachten dan wel op specifieke strafbare feiten die in het onderzoek Meiberg aan de orde waren. Dit onderzoek had derhalve geen betrekking op de medeverdachte [verdachte 1], waardoor het eventueel ten onrechte ontbreken van toestemming daarvoor van de rechter-commissaris niet onrechtmatig jegens hem was.

In de tweede fase zijn op 13 april 2016 de hiervoor weergegeven digitale gegevensdragers onderzocht louter ter vaststelling van de identiteit van de gebruiker daarvan. Bij gebreke van andere mogelijkheden voor die vaststelling dan het onderzoeken van een beperkt aantal gegevens op de verschillende digitale gegevensdragers had de rech-

ter-commissaris hiervoor toestemming mogen geven, zodat het hof dit onderzoek niet onrechtmatig.

Nadien zijn alle gegevensdragers uitvoerig onderzocht. Gegeven de zeer forse omvang van de strafbare feiten waarop het tegen de verdachte ingestelde onderzoek betrekking had en de vrijwel uitsluitend digitale aard van die strafbare feiten en daarmee ook van de mogelijke aanwijzingen van betrokkenheid van de verdachte daarbij, had de rechter-commissaris ook hiervoor toestemming mogen geven, zodat het hof ook dit onderzoek niet onrechtmatig acht.

Het hof is van oordeel dat, indien de materiële vereisten ingevolge artikel 126nba Sv toegepast zouden worden, voorgaande oordelen identiek zouden uitvallen.

[...]

Beslissing

Het hof:

[...]

Vernietigt het vonnis waarvan beroep en doet opnieuw recht:

Verklaart niet bewezen dat de verdachte het onder 7, 8, 11, 12, 14 en 15 tenlastegelegde heeft begaan en spreekt de verdachte daarvan vrij.

Verklaart zoals hiervoor overwogen bewezen dat de verdachte het onder 1, 2, 3, 4, 5, 6 en 13 tenlastegelegde heeft begaan.

Verklaart niet bewezen hetgeen de verdachte meer of anders is tenlastegelegd dan hierboven is bewezenverklaard en spreekt de verdachte daarvan vrij.

Verklaart het onder 1, 2, 3, 4, 5, 6 en 13 bewezenverklaarde strafbaar, kwalificeert dit als hiervoor vermeld en verklaart de verdachte strafbaar.

Veroordeelt de verdachte tot een **gevangenisstraf** voor de duur van **21 (eenentwintig) maanden**.

Beveelt dat de tijd die door de verdachte vóór de tenuitvoerlegging van deze uitspraak in enige in artikel 27, eerste lid, van het Wetboek van Strafrecht bedoelde vorm van voorarrest is doorgebracht, bij de uitvoering van de opgelegde gevangenisstraf in mindering zal worden gebracht, voor zover die tijd niet reeds op een andere straf in mindering is gebracht.

Wijst de vorderingen van de navolgende benadeelde partijen toe, vermeerderd met de wettelijke rente (hierna: 'wr') vanaf de genoemde aanvangsdatum tot aan de dag der voldoening op de volgende wijze:

[...]

Noot

1. De verdachte in deze zaak heeft zich volgens de cybercrimekamer van het Gerechtshof Den Haag ruim anderhalf jaar lang schuldig gemaakt aan oplichting en computervredebreuk met gephishte gegevens. Ook was sprake van grootschalige oplichting met nagemaakte webwinkels. Bovendien had de verdachte toegangscodes van ac-

counts van anderen voorhanden en maakte hij zich schuldig aan witwassen. Het hof heeft een gevangenisstraf van 21 maanden opgelegd. In zoverre lijkt deze zaak op andere phishingzaken.

2. Het arrest levert een bijdrage aan de rechtsontwikkeling omdat het voortborduurde op de 'smartphone-arresten' van de Hoge Raad. In de uitspraak wordt het beslismodel over de rechtmatigheid van onderzoek aan digitale gegevensdragers verder verfijnd. Daarbij reikt het hof gezichtspunten aan die de rechter-commissaris kan – of moet? – hanteren bij het beoordelen of, en zo ja in hoeverre, de gegevens op een gegevensdrager mogen worden onderzocht.

3. Om het geheugen op te frissen: in de 'smartphone-arresten' van 4 april 2017² heeft de Hoge Raad beslist dat onderzoek aan gegevensdragers onrechtmatig kan zijn wanneer dat onderzoek zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker ervan. Dat is in het bijzonder het geval wanneer alle gegevens zijn opgeslagen met technische hulpmiddelen. In zulke gevallen is de politie niet zelfstandig bevoegd, maar is toestemming van de officier van justitie vereist. Als voorzienbaar is dat de inbreuk op de persoonlijke levenssfeer "zeer ingrijpend" zal zijn, dan is enkel de rechter-commissaris bevoegd.

4. Terug naar deze zaak. Het OM leidde uit het hierboven genoemde besliskader van de Hoge Raad af dat een rechtmatig door de R-C in beslag genomen gegevensdrager ongeclausuleerd mag worden onderzocht. Dat standpunt is volgens het hof in zijn algemeenheid houdbaar, maar het geldt niet onverkort.

5. Als op voorhand te voorzien is dat het onderzoek een min of meer compleet beeld kan opleveren van bepaalde aspecten van het persoonlijk leven van een gegevensdrager stelt het hof nadere regels. De rechter-commissaris zal dan eerst moeten beslissen of aan het onderzoek aan de gegevensdrager beperkingen worden gesteld, en zo ja, wat de aard en omvang van die beperkingen dan is. Relevante factoren daarvoor zijn o.a. de ingrijpendheid van de inbreuk op de privacy en proportionaliteit en subsidiariteit van het onderzoek in relatie tot de aard en omvang van de verdenking.

6. Beperkingen die de rechter-commissaris kan stellen, zijn bijvoorbeeld beperkingen aan het aantal te onderzoeken gegevensdragers, beperkingen aan de te onderzoeken gegevens (bijvoorbeeld uitsluitend afbeeldingen, communicatie of internetgedrag), of beperking tot een bepaalde periode waar het onderzoek zich op richt. Daarbij kan het aangewezen zijn dat het onderzoek gefaseerd wordt uitgevoerd, waarbij de rechter-commissaris tussentijds uitbreidingen of verdere beperkingen beveelt.

7. Deze situatie, waarin de rechter-commissaris zich over de eventuele beperkingen moet buigen, zal zich

waarschijnlijk vaak voordoen. De Hoge Raad heeft in de eerder genoemde smartphone-arresten immers geoordeeld dat het geautomatiseerd uitlezen en onderzoeken van alle gegevens op een gegevensdrager een vermoeden oplevert dat het onderzoek zo verstrekkend is dat een min of meer compleet beeld van bepaalde aspecten van het privéleven kan worden verkregen. In de praktijk wordt vaak een forensische kopie van een gegevensdrager gemaakt, waarna de gebruikte software in de vastgelegde gegevens zoekt naar relevante data (zoals foto's, locaties, afspraken, contacten, berichten, inloggegevens, et cetera). Wil de recherche die werkwijze hanteren, dan zal de rechter-commissaris zich daar telkens over moeten uitlaten. Dat zal ook gelden indien tijdens een doorzoeking 'live forensics' wordt toegepast.

8. Deze verfijning van het beoordelingskader heeft potentieel een beperkende werking op het onderzoek naar gegevens op een gegevensdrager. Niet langer geldt slecht een binaire beslissing (wel of geen onderzoek), maar kan maatwerk worden geleverd. Vanuit het perspectief van privacy van de verdachte – en niet te vergeten van derden in de omgeving van de verdachte, al benoemt het hof enkel het belang van de 'gebruiker van de gegevensdrager' – is dit een gunstige ontwikkeling. Het legt immers uitdrukkelijk de vraag voor welke gegevens noodzakelijk zijn, en of de inbreuk daartoe beperkt kan blijven.

9. Wil dit besliskader daadwerkelijk effectief en toetsbaar zijn, dan is wel vereist dat de rechter-commissaris dergelijke beslissingen neerlegt in een gemotiveerde beschikking, of ten minste in het proces-verbaal van de doorzoeking. Slechts dan kunnen procespartijen en de rechter in een later stadium adequaat beoordelen of het onderzoek rechtmatig is geweest. Dat zal uiteraard niet goed mogelijk zijn wanneer de recherche volstaat met een opmerking in het proces-verbaal dat bepaald onderzoek is uitgevoerd 'met toestemming van de rechter-commissaris mr. X'. Een adequate beoordeling achteraf veronderstelt dat het proces van besluitvorming ook achteraf inzichtelijk is. Hierover heeft het hof echter niets overwogen.

10. In dat kader is enigszins teleurstellend te noemen dat het hof in de voorliggende zaak de toetsing en motivering zo summier heeft gehouden. Het hof stelt vast dat "alle gegevensdragers uitvoerig [zijn] onderzocht" zonder machtiging van de rechter-commissaris, en passeert dit verzuim onder verwijzing naar de "zeer forse omvang" van de verdenkingen en de vrijwel uitsluitend digitale aard van de feiten. De rechter-commissaris had dan ook toestemming mogen geven, aldus het hof. In het kader van de voorbeeldfunctie van dit arrest was het goed geweest als het hof eerst expliciet zou vaststellen dat het ontbreken van een machtiging een vormverzuim is. Vervolgens was een uitvoeriger motivering wenselijk geweest, bijvoorbeeld onder verwijzing naar de individuele gegevensdragers en de pleegperiode. Het verfijnde besliskader heeft immers alleen toegevoegde waarde als het daadwerkelijk leidt tot concrete afwegingen en toegespitste motiveringen door de rechter-commissaris. Als de feitenrech

² HR 4 april 2017, ECLI:NL:HR:2017:584; ECLI:NL:HR:2014:588 en ECLI:NL:HR:2014:592.

ter het signaal geeft niet zwaar te tillen aan het ontbreken van een machtiging en akkoord te gaan met slechts een algemene verwijzing naar aard en omvang van de verdenking, bestaat het risico dat de beoordeling de facto niet verandert.

11. Tot slot is nog de reikwijdte van dit arrest van belang. Het hof schrijft dit verfijnde besliskader voor in de situatie waarin de rechter-commissaris inbeslaggenomen gegevensdragers overdraagt aan de politie. Zou het nieuwe besliskader alleen dan gelden, en niet wanneer de recherche zelfstandig gegevensdragers in beslag heeft genomen? Dat zou een moeilijk te rechtvaardigen verschil in rechtsbescherming opleveren en ligt dus niet voor de hand. Of zou dit beslismodel in alle gevallen gelden, als maar verwacht wordt dat een min of meer compleet beeld van bepaalde aspecten van het privéleven wordt verkregen? Als dat juist is, leidt dit arrest ertoe dat de officier van justitie in veel gevallen niet langer bevoegd is dergelijk onderzoek te gelasten. Het voornemen om een gegevensdrager geautomatiseerd uit te lezen zet dan de officier van justitie al buitenspel.

M. Berndsen

Computerrecht 2022/10

RECHTBANK MIDDEN-NEDERLAND

14 april 2021, C/16/501952 / HA ZA 20-276

(Mr. J.P. van Driel van Wageningen)

m.nt. G.J. Boeve¹

(Art. 3:35, 3:36, 3:61 lid 2, 6:34, 6:114, 6:116, 6:147 BW)

NJ 2021/293

ECLI:NL:RBMNE:2021:1528

Wie betaalt de rekening van factuurfraude? Annotatie van Brabantia/Bol.com in het licht van Devante/Hascor. Daarin komt ook de vraag aan de orde voor wiens risico het misbruik van het e-mailadres van een schuldeiser komt.

Vonnis in de zaak van:
Brabantia Netherlands B.V.
tegen
Bol.com B.V.

Vonnis

[...]

¹ Gert Jan Boeve was advocaat te Utrecht tot en met 31 december 2021 en is vanaf 1 januari 2022 werkzaam als medewerker van het wetenschappelijk bureau van de Hoge Raad. Gert Jan is tevens als buitenpromovendus verbonden aan de Universiteit Leiden. Deze annotatie is op persoonlijke titel geschreven. De in deze bijdrage genoemde weblinks functioneerden op 22 november 2021.

2 Waar gaat deze zaak over?

2.1 Brabantia Netherlands is een fabrikant van huishoudelijke producten. Bol.com is een webwinkel. Brabantia Netherlands verkoopt met regelmaat producten aan Bol.com. Ook in december 2019 en januari 2020 heeft Brabantia Netherlands huishoudelijke producten verkocht en geleverd aan Bol.com.

[...]

2.2 Najaar 2019 is de mailbox [e-mailadres] @brabantia.com, van mevrouw [A] ([...]), een medewerster van de boekhoudafdeling van Brabantia Netherlands, gehackt door één of meerdere oplichters.

2.3 Vanuit het e-mailadres van [A] is op 25 november 2019 een e-mail aan 'supplierfinance@bol.com' gestuurd met onder meer de volgende inhoud: 'Bijgevoegd vindt u onze nieuwe betalingsroute zoals opgedragen door het management, doe het nodige voor de volgende betaling. Alvast bedankt!' De begeleidende brief bevat kort gezegd een verzoek om betalingen voortaan niet meer over te maken aan de bij Bol.com bekende bankrekening van Brabantia Netherlands maar aan een Spaanse bankrekening die ten name van 'Brabantia International B.V.' zou staan.

2.4 Op 26 november 2019 is er vanuit de mailbox van [A] een e-mail met onder meer de volgende inhoud aan 'supplierfinance@bol.com' gestuurd:

'Beste,

Kunt u bevestigen dat uw crediteurenadministratie is bijgewerkt als bijgevoegd.

Alvast bedankt!'

2.5 Op 27 november 2019 volgde daarop een bericht met onder meer de volgende inhoud (ook vanuit de mailbox van [A] aan 'supplierfinance@bol.com'):

'Goedenmiddag

Uw oprechte antwoord wordt op prijs gesteld, bevestig zo vriendelijk dat u onze boekhouding bij u hebt bijgewerkt.

Alvast bedankt!'

2.6 Daarop is op 6 december 2019 vanuit 'supplierfinance@bol.com' geantwoord (naar e-mailadres '[e-mailadres] @brabantia.com)'). Volgens Brabantia Netherlands is deze reactie haar ontgaan omdat de hacker het ertoe heeft geleid dat alle berichten die afkomstig waren van een e-mailadres met de uitgang '@bol.com' in de e-mailbox van [A] automatisch werden verplaatst naar het mapje 'RSS-feeds' en daarbij wellicht ook als 'gelezen' zijn gemarkeerd. In het bericht staat het volgende:

'Goedemorgen,

Het rekeningnummer [rekeningnummer] is bij ons bekend.'

2.7 Nadat het bankrekeningnummer in de systemen van Bol.com op 4 december 2019 werd gewijzigd, heeft