Hof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3529

Oerlemans, J.J.

Hof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3529, *Computerrecht* 2019/51, m.nt. J.J. Oerlemans

Noot

1. Het arrest van het Hof Den Haag van 19 december 2018 is om twee redenen lezenswaardig en een annotatie waard: 1. Het Hof gaat in op de reikwijdte van de netwerkzoeking en beantwoordt de vraag of deze ook na een doorzoeking van een plaats mag plaatsvinden en 2. Het Hof legt uit hoe moet worden omgegaan met het 'hackverweer' in strafzaken. In deze noot worden eerst de interessante feiten van de zaak kort weergegeven, vervolgens wordt uitgelegd hoe het Hof vanaf nu omgaat met het hackverweer in strafzaken en ten slotte volgt een analyse van de overwegingen met betrekking tot de netwerkzoeking.

De feiten

2. De verdachte heeft zich schuldig gemaakt aan computervredebreuk, diefstal, oplichting en het voorhanden hebben van malware met het oogmerk computervredebreuk te plegen. De verdachte verstuurde uit naam van Ziggo een groot aantal phishing-mails. Ten eerste heeft de verdachte met een Ziggo-phishing mail 150 mensen verleidt met hun Ziggo-account in te loggen op een nagemaakte Ziggo-website teneinde de nieuwe Samsung Galaxy te claimen ter ere van het achtjarig bestaan van Ziggo. De verdachte heeft met de verkregen inloggegevens bestellingen geplaatst uit naam van de slachtoffers, telefoonverkeer gevoerd en 'online credits' aangeschaft. Ten tweede heeft de verdachte een namaak Ziggo-mail verstuurd met daarin de melding van een betalingsachterstand die zou zijn ontstaan van 40 euro als gevolg van het niet-betalen van een factuur van Ziggo. Zodra de klant op de in de mail gevoegde link klikte, werd hij doorgelinkt naar een website en werd de computer waarop de link werd geopend besmet met malware (genaamd 'NanoCore'). Via de keylogfunctie van de malware (het registreren van toetsaanslagen) heeft de verdachte gebruikersnamen en wachtwoorden van verschillende internetdiensten van deze slachtoffers verkregen. De verdachte heeft met gebruikmaking van PayPal-inloggegevens in minstens drie gevallen eten besteld via Thuisbezorgd.nl en eten besteld bij 'Eazie'. Hij wordt veroordeeld tot een gevangenisstraf van 17 maanden, waarvan zes maanden voorwaardelijk. De vordering van geleden materiële schade van € 89.585,95 door Ziggo moet bij de burgerlijke rechter worden aangebracht.

Het hackverweer

3. Door en namens de verdachte is vrijspraak bepleit. Daartoe is aangevoerd dat een ander misbruik heeft gemaakt van de Lenovo laptop van de verdachte. Ter onderbouwing van dit verweer heeft de verdediging een deskundigenrapport van Fox-IT ingebracht. In dit rapport is onder meer beschreven op welke manier een hacker toegang kan krijgen tot een computer en wat de gevolgen hiervan kunnen zijn.

4. Het Hof Den Haag stelt in r.o. 2.2 e.v. voorop dat bij de beoordeling van een dergelijk verweer als maatstaf dient te worden aangelegd of – alle feiten en omstandigheden in ogenschouw nemende – dit verweer al dan niet in meer of mindere mate *aannemelijk* is geworden.[1] Het is aan de verdachte om die feiten en omstandigheden aan te voeren. De rechter mag ervan uitgaan, behoudens sterke aanwijzingen voor het tegendeel, dat op een computer (of in een beveiligde online omgeving) aangetroffen gedownloade of gekopieerde bestanden daarop zijn geplaatst door de gebruiker van die computer. De rechter mag er ook vanuit gaan dat, behoudens sterke aanwijzingen voor het tegendeel, wanneer uit nadere (meta)data blijkt dat bepaalde websites of bepaalde bestanden zijn geopend, die handelingen zijn verricht door de gebruiker van die computer. Het Hof overweegt ook dat niet hoeft worden aangetoond dat kan worden *uitgesloten* dat een bepaalde computer is gehackt. Aangetroffen sporen van malware op een computer leveren niet noodzakelijkerwijs een aannemelijke verklaring voor de aanwezigheid van bepaalde (digitale) delictsporen, zoals opgeslagen browser- of communicatieactiviteiten en kinderpornografische afbeeldingen. Een (deskundigen)verklaring met een beschrijving van de mogelijkheid dat de betreffende computer is gehackt, zonder dat daarbij tevens een specifieke relatie wordt gelegd met de feiten uit de betreffende zaak en het daarin verrichtte (digitaal-forensische) onderzoek, is in de regel op zichzelf onvoldoende

[1] Het verwijst daarbij naar HR 16 maart 2010, ECLI:NL:HR:2010:BK3359.

redengevend voor de conclusie dat min of meer aannemelijk is geworden dat ook in het voorliggende geval de computer is gehackt.[2]

5. Voor de beoordeling of een hackverweer in meer of mindere mate aannemelijk is geworden geeft het Hof Den Haag de volgende zes overwegingen mee: (1) de aan- of afwezigheid van digitale sporen met betrekking tot het daadwerkelijk (kunnen) binnendringen door derden in de betreffende computer, zoals '*remote acces tools*'; (2) het niveau van fysieke en digitale bescherming van de computer tegen gebruik door derden/(digitaal) binnendringen, zoals beveiligingssoftware; (3) de aan- of afwezigheid van digitale sporen waaruit, bijvoorbeeld vanwege de inhoud, kan worden afgeleid wie (ook) op of omstreeks het moment van plegen van de strafbare gedragingen de gebruiker van de computer was, zoals e-mails en chats (4) de mate waarin, en het moment waarop, de verdachte medewerking heeft verleend aan eventueel nader onderzoek naar zijn verweer, zoals het al dan niet (tijdig) verstrekken door de verdachte van bijvoorbeeld wachtwoorden en toegangscodes, welke nodig zijn voor het verrichten van (nader) digitaal-forensisch onderzoek; (5) andere feiten en omstandigheden die wijzen op een bijzondere (inhoudelijke) betrokkenheid van de verdachte of een derde bij de op of via de betreffende computer gepleegde gedragingen, zoals gephiste creditcard gegevens) en (6) de aan- of afwezigheid van een motief voor derden om in de computer van de verdachte binnen te dringen.

6. In casu is het hackverweer volgens het Hof Den Haag op geen enkele wijze aannemelijk geworden. In het rapport van Fox-IT wordt slechts in zijn algemeenheid aangegeven dat er mogelijkheden bestaan voor een kwaadwillende om in te breken op de computer van een ander. Een relatie met de concrete omstandigheden van het onderhavige geval is niet gelegd en daarover bevat het rapport dan ook geen conclusies. Het Hof nam ook in aanmerking dat de verdachte niet het wachtwoord van zijn router afgaf en een foutieve inlogcode voor zijn iPhone 6, waardoor het apparaat vergrendeld raakte en geen nader forensisch onderzoek op het apparaat kon worden uitgevoerd. Daartegenover is uit chatgesprekken op de laptop van de verdachte af te leiden dat de verdachte de laptop gebruikte en had de verdachte chatverkeer met de Ziggo Helpdesk over de (frauduleuze) bestellingen uit naam van slachtoffers vanaf het schoolaccount van de verdachte op een schoolcomputer in het leslokaal waar de verdachte op dat moment aanwezig was.

Reikwijdte van de netwerkzoeking

7. De verdachte werd geïdentificeerd op basis van het IP-adres dat herleidbaar is tot de woning van de verdachte. Het desbetreffende IP-adres werd geregistreerd tijdens de bestellingen en chatgesprekken die verdachte met Ziggo heeft gevoerd. Ook het afleveradres voor de via internet bestelde maaltijd is het huisadres van de verdachte. Na de doorzoeking in de woning van de verdachte en inbeslagname van de Lenovo laptop van de verachte, is op de computer bewijs van de phishingmails en het gebruik van de malware gevonden, zoals gebruikersnamen en wachtwoorden van slachtoffers. Bij het onderzoek aan de laptop is een e-mailadres als zoekwoord ingevoerd. Dat leverde als resultaat op een bestand op. Uit de gegevens van dat bestand bleek dat de gebruiker van de Lenovo laptop zich met behulp van de internetbrowser Google Chrome had aangemeld met dat e-mailadres.

8. Vervolgens heeft de politie onder leiding van het Openbaar Ministerie een *netwerkzoeking op het politiebureau* uitgevoerd, in plaats van de woning van de verdachte. Met toestemming van de rechter-commissaris is de inhoud van de mailbox van het Hotmail-account van de verdachte gekopieerd (8643 e-mails). Vervolgens is een met toestemming van de rechter-commissaris ook de inhoud van de mailbox van een Gmail account van de verdachte gekopieerd (1001 e-mails). Direct na het inzichtelijk maken van de e-mails zag de verbalisant dat diverse e-mails gerelateerd konden worden aan phishing. Vier e-mails zijn geopend en daarin waren IP-adressen, namen en wachtwoorden opgenomen.

9. In de machtiging tot een netwerkzoeking (art. 125j Wetboek van Strafvordering (Sv)) overwoog de rechter-commissaris op basis van een notitie van de officier van justitie dat veel bestanden tegenwoordig op het internet staan opgeslagen en het maken van een image van de computer

[2] In Hof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3528 volgt dezelfde uiteenzetting van overwegingen omtrent het hackverweer.

en onderzoek in genetwerkte computers dagenlang zou vergen en een onnodige belasting zou opleveren voor de bewoners van de woning. De advocaat-generaal pleit ervoor om in te gaan op deze machtiging tot netwerkzoeking op het politiebureau en dat het hof vaststelt dat rechter-commissaris in redelijkheid tot zijn oordeel omtrent de door hem afgegeven machtiging terzake van voormelde netwerkzoeking heeft kunnen komen.

10. Het Hof Den Haag gaat mijns inziens terecht *niet* mee het pleidooi voor het toelaatbaar achten van een netwerkzoeking op afstand op basis van de wet. Kort gezegd legt het hof uit dat in de wetsgeschiedenis blijkt dat de wetgever geen ruimte heeft willen bieden voor de toepassing van een netwerkzoeking op een later moment en op een andere locatie dan (ten tijde van) de plaats van doorzoeking. Daarnaast is in artikel 125j Sv[3] de netwerkzoeking gekoppeld aan de doorzoeking van een plaats ter vastlegging van gegevens.[4] Het Hof Den Haag overweegt dat de netwerkzoeking daarmee los staat van de inbeslagnemingsbevoegdheden, in die zin dat niet kan worden gezegd dat de bevoegdheid tot inbeslagneming reeds de bevoegdheid tot het doen van een netwerkzoeking impliceert. Ook hierin ligt een argument besloten voor het oordeel dat de netwerkzoeking niet pas na de feitelijke inbeslagname van een gegevensdrager (alsnog) mag worden toegepast, en derhalve op een later moment en op een andere locatie, zoals in casu wel is gebeurd.

11. Naar mijn weten is in twee andere gevallen gepleit voor het mogelijk maken inloggen op een webmailaccount van de verdachte vanaf het politiebureau, maar dan op grond van art. 126ng lid 2 Sv (kortgezegd de bevoegdheid tot het vorderen van opgeslagen gegevens bij een communicatiedienstaanbieder). In de eerste beschikking keurde de rechter-commissaris de aanvraag tot inloggen niet goed, omdat artikel 126ng lid 2 Sv ziet op het vorderen van opgeslagen gegevens bij een elektronische communicatiedienstaanbieder en niet op een zoeking en overnemen van gegevens op afstand.[5] In de tweede (recente) beschikking gaf de rechter-commissaris wél een machtiging – na tussenkomst van de officier van justitie – aan een opsporingsambtenaar om in te loggen op de verschillende e-mailadressen en datingsites.[6] De rechter-commissaris achtte zich, op grond van artikel 181 Sv, bevoegd om deze beslissing te nemen, hoewel ook wordt opgemerkt dat de wet (nog) niet voorziet in een specifieke bevoegdheid om in te loggen op e-mailadressen en websites en gegevens vast te leggen. De Rechtbank Den Haag overweegt ten eerste dat het verschil tussen een vordering tot de gegevens en het inloggen en overnemen van gegevens op afstand 'niet wezenlijk' is, omdat het om dezelfde soort gegevens gaat. Ten tweede is het inloggen op de e-mailadressen en websites met vooraf beschikbare gebruikersnamen en wachtwoorden een eenvoudige en weinig risicovolle wijze van binnendringen in een geautomatiseerd werk. Ten derde is de inbreuk voor de betrokkene niet groter bij het inloggen en vastleggen van gegevens dan bij het vorderen van gegevens bij de aanbieder. *"Met andere woorden: aan de eisen van proportionaliteit en subsidiariteit is voldaan*", aldus de rechtbank. Dat mag zo zijn, maar aan de bepalingen in Strafvordering waarin wordt voorgeschreven wat de politie en het OM wel en niet mogen, wordt nu mijns inziens niet voldaan. Het is overigens wél toegestaan achteraf op een account in te loggen met de hackbevoegdheid op basis van art. 126nba lid 1 sub d Sv, dat wil zeggen: zodra de Wet computercriminaliteit III in werking treedt. In dat opzicht is het vreemd dat deze problematiek en een oplossing daarvoor niet in de Wet computercriminaliteit III is meegenomen.

12. Terug naar het onderhavige arrest. Het Hof Den Haag stelt in deze zaak vast dat de uitvoering van de netwerkzoeking op een andere locatie en op een later moment dan die waarop de doorzoeking heeft plaatsgevonden niet in de huidige wet is voorzien. In scherpe bewoordingen legt het Hof uit dat zij de ruime uitleg van de advocaat-generaal van art. 125j Sv niet accepteert,

---

[3] Artikel 125j lid 1 Sv: *"In geval van een doorzoeking kan vanaf de plaats waar de doorzoeking plaatsvindt, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar in dat werk opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen, dan kunnen zij worden vastgelegd"* (onderstreping toegevoegd).

[4] Zie ook C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5, nr. 1, p. 23-32.

[5] Rb. Rotterdam 1 januari 2018, ECLI:NL:RBROT:2018:8017.

[6] Rb. Den Haag 11 januari 2019, ECLI:NL:RBDHA:2019:1329.

omdat dat een afweging van politieke aard is die de rechtsvormende taak van de rechter overstijgt. Daarmee is sprake van een onherstelbaar vormverzuim. Naar vaste jurisprudentie over vormverzuimen komt het Hof Den Haag echter tot de conclusie dat de verdachte niet daadwerkelijk in zijn verdediging is geschaad en daarom volstaat zij met de vaststelling van het vormverzuim. Deze sanctie lijkt mij in deze zaak terecht. Wel vraag ik mij af of de sanctie hetzelfde moet blijven als blijkt dat de netwerkzoeking op afstand *structureel* wordt ingezet, hetzij op grond van art. 125j Sv, hetzij op grond van art. 126ng lid 2 Sv. De structurele inzet van een ingrijpende onwetmatige opsporingsmethode kan niet door de beugel. Het is een kernprincipe van de rechtsstaat is dat de burger weet onder welke omstandigheden de overheid opsporingsbevoegdheden mag inzetten. Dat dient de rechtszekerheid en voorkomt misbruik van bevoegdheden. Tegelijkertijd ligt deze toepassing duidelijk in het verlengde van de bestaande doorzoekings- en inbeslagnameregelingen. Onder bepaalde omstandigheden kan de inzet van de opsporingsmethode noodzakelijk zijn om bewijs te verzamelen. Het bovenstaande pleit des te meer voor een regeling in het Wetboek van Strafvordering.

Toekomstige wetgeving

13. De 'Commissie Modernisering opsporingsonderzoek in het digitale tijdperk' (hierna: Commissie-Koops) heeft in haar rapport bovenstaande problematiek ook behandeld.[7] De Commissie-Koops stelt in het rapport vast dat de netwerkzoeking op een andere locatie dan waar de doorzoeking plaatsvindt niet is toegestaan en dat een nieuwe regeling noodzakelijk is. De Commissie constateert dat "*nu, maar zeker in de toekomst, de meeste gezochte gegevens zich niet meer fysiek in de omgeving van het subject maar ergens in de cloud bevinden*".[8] De Commissie-Koops stelt voor de voorgestelde regeling in artikel 2.7.4.2.2 Boek 2 Sv aan te passen en daarmee het onderzoek op afstand na inbeslagname van een voorwerp mogelijk te maken. Met aanpassing van de regeling kunnen opsporingsambtenaren vanaf het politiebureau met rechtmatig verkregen inloggevens en eventueel met behulp van forensische software, bewijs uit accounts van een verdachte veilig stellen. Een machtiging van een rechter-commissaris is volgens de Commissie-Koops noodzakelijk, als te verwachten is dat tijdens het onderzoek berichten worden aangetroffen in een geautomatiseerd werk van een aanbieder (zoals webmail).[9] Mijns inziens is de waarborg van een machtiging van een rechter-commissaris bij een netwerkzoeking te allen tijde wenselijk.[10]

14. Volgens de Commissie-Koops is de nood tot het mogelijk maken van deze opsporingshandelingen zo hoog, dat deze zo snel mogelijk in werking moeten treden en dus niet kan worden afgewacht op de implementatie van het conceptwetsvoorstel in het Wetboek van Strafvordering (naar verwachting in 2023-2024). Het is nu afwachten of een wetsvoorstel naar de Tweede Kamer wordt gestuurd om deze inbeslagnameregeling aan te passen. Dit arrest van het Hof Den Haag zou daar enige druk achter kunnen zetten.

[7] Het rapport is 'Regulering van opsporingsbevoegdheden in een digitale omgeving' is beschikbaar op: https://www.rijksoverheid.nl/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving (laatst geraadpleegd op 15 februari 2019).
[8] Commissie-Koops 2018, p. 111.
[9] Commissie-Koops 2018, p. 93-94.
[10] Zie J.J. Oerlemans, *Investigating Cybercrime*, diss. Leiden, Amsterdam: Amsterdam University Press 2017, p. 267-268.