Rb. Midden-Nederland 17 juni 2020, ECLI:NL:RBMNE:2020:2277, *Computerrecht* 2020/185, m.nt. J.J. Oerlemans[1]

Annotatie

1. Een 'OV-chipkaart' is een persoonsgebonden of anonieme kaart waarmee personen in Nederland kunnen reizen met het openbaar vervoer (zoals de trein, bus en tram). Op een persoonsgebonden OV-chipkaart staat een pasfoto, naam en geboortedatum vermeld. Het biedt als voordeel met kortingsproducten te reizen. Deze persoonsgegevens staan niet vermeld op een anonieme OV-chipkaart. Met een anonieme OV-chipkaart wordt op een vooraf opgeladen bedrag (saldo) gereisd. De OV-chipkaart bevat een bepaalde chip (de 'Mifare Classic' chip) en heeft een 'Near Field Communication' (NFC) functionaliteit, waardoor de gegevens op de chip eenvoudig en contactloos door een poortje kunnen worden uitgelezen. In de eerste helft van 2019 waren er in Nederland 7,46 miljoen persoonlijke OV-chipkaarten in omloop en 7,36 miljoen anonieme OV-chipkaarten.[2]

2. De verleiding voor hackers om een OV-chipkaart te hacken en daardoor gratis te reizen is blijkbaar groot. Sinds de eerste proeven met een OV-chipkaart in Nederland en de landelijke invoering van OV-chipkaart in 2012 zijn er op www.rechtspraak.nl vier uitspraken verschenen over computervredebreuk en OV-chipkaarten.[3] Daarnaast wordt er ook serieus wetenschappelijk onderzoek uitgevoerd naar de veiligheid van de 'Mifare Classic-chip' in de OV-chipkaarten en komen om de zoveel tijd berichten naar buiten over kwetsbaarheden in die chip.[4] De onderhavige zaak springt er vergeleken met de andere zaken over gehackte OV-chipkaarten uit, vanwege de lange duur dat de twee verdachten gratis konden (zwart)reizen en de hoogte van de toegewezen vordering.

3. De werkwijze van de verdachte en de medeverdachte bestond onder meer uit het plaatsen van de OV-chipkaart op de NFC-kaartlezer en het met een script een 'brute force' aanval op de OV-chipkaart uitvoeren totdat de sleutel ('key') is achterhaald. Met de key kon toegang worden verschaft tot de OV-chipkaart, waarna het saldo kon worden veranderd. Voor het veranderen van het saldo werd het programma 'OVChipAppV6' gebruikt.[5]

---

[1] Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij het Montaigne Centrum voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen van de Universiteit Utrecht.
[2] *Kamerstukken II* 2019/20, 23645, nr. 713 (Voortgangsrapportage NOVB eerste helft 2019).
[3] Zie Rb. Utrecht 8 december 2010, ECLI:NL:RBUTR:2010:BO6723, en ELCI:NL:RBUTR:2010:BO9407, Rb. Rotterdam 6 december 2013, ECLI:NL:RBROT:2013:9579, Hof Den Haag 26 mei 2015, ECLI:NL:GHDHA:2015:1427, Rb. Rotterdam 6 februari 2019, ECLI:NL:RBROT:2019:1101, Hof Den Haag 9 september 2019, ECLI:NL:GHDHA:2019:2426. Rechtspraak.nl is een databank waarop alle gepubliceerde rechtspraak in Nederland is te vinden van de rechtbanken, gerechtshoven en de Hoge Raad. De rechtspraak bepaalt zelf – op basis van het Besluit selectiecriteria uitsprakendatabank – welke rechtspraak wordt gepubliceerd. De genoemde uitspraken in zijn gevonden op basis van een zoekslag op 13 augustus 2020 op de zoektermen "computervredebreuk" en "OV-chip".
[4] Zie Rb. Arnhem 18 juli 2008, ECLI:NL:RBARN:2008:BD7578 over de afwijzing van een verzocht verbod op de publicatie van wetenschappelijk onderzoek van onderzoekers van de Radboud Universiteit Nijmegen naar kwetsbaarheden in een (inmiddels verouderde) Mifare Classic-chip die wordt gebruikt voor de OV-chipkaart. Zie ook Brenno de Winter, 'OV-chipkaart nu door iedereen te kraken', Webwereld.nl, 5 november 2010, 'Nieuwe hack kraakt OV-chipkaart binnen seconden', Webwereld.nl, 4 februari 2011 en Joost Schellevis, 'Student ontdekt kwetsbaarheid in protocol OV-chipkaart', Tweakers.net, 2 april 2015.
[5] Zie voor een meer gedetailleerde uitleg de BNR-podcast 'Onderzoeksraad der dingen', dossier #0010b: zwartrijden.

4. Beide verdachten zijn veroordeeld voor computervredebreuk, valsheid in geschrifte met betaalpassen en voorhanden hebben van gegevens om valsheid in geschrifte te plegen. In deze zaak wordt voor het eerst wordt vervolgd voor het vervalsen van een OV-chipkaart als zijnde een 'waardekaart' (artikel 232 Wetboek van Strafrecht ('Sr')).[6] Hoewel het vervalsen van betaalpassen of waardekaarten mogelijk ook onder het delict valsheid in geschrifte valt, heeft de wetgever met de Wet computercriminaliteit I in 1993 ervoor gekozen om hiervoor een aparte strafbepaling in het leven te roepen. Net als bij valsheid in geschrifte is ook het opzettelijk gebruiken, het opzettelijk afleveren of voorhanden hebben van een valse pas of kaart strafbaar (lid 2).[7] In de uitspraak wordt verder niet ingegaan op het delict computervredebreuk (artikel 138ab Sr). Het Hof Den Haag legt in een eerder arrest uit dat in feite computervredebreuk wordt gepleegd op de NFC chip op de OV-chipkaart, nu deze chip bestemd is (en de technische mogelijkheden heeft) om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.[8] De chip is met andere woorden het 'geautomatiseerde werk' in juridische zin (artikel 80sexies Sr), waarop opzettelijk en wederrechtelijk wordt binnengedrongen.[9]

5. De verdediging voert aan dat de verdachten slechts uit nieuwsgierigheid hebben gehandeld, waardoor het oogmerk op financieel gewin zou ontbreken. De rechtbank gaat hier niet in mee, omdat de verdachten hebben bekend dat zij veelvuldig het saldo van OV-chipkaarten "valselijk" hebben opgeladen. De verdediging voert ook aan dat slechts bestaande software zou zijn doorontwikkeld en niet is 'vervaardigd' in juridische zin. De rechtbank verwerpt dit verweer, omdat het een 'feit van algemene bekendheid' zou zijn dat nieuwe computerprogramma's veelvuldig zijn gestoeld op een basis van reeds ontwikkelde software. Hierdoor ontstaat nieuwe software, waardoor wel degelijk sprake zou zijn van vervaardiging van software, zoals ten laste is gelegd.

6. Het openbaar ministerie kon de verdachten mogelijk ook vervolgen voor het 'voorhanden hebben van een technisch middel of toegangscode met het oogmerk computervredebreuk te plegen' (artikel 139d lid 2 Sr). In een meer recent arrest legt het Hof Den Haag verder uit dat een kaartlezer waarmee saldo kan worden verhoogd niet zonder meer kwalificeert als een technisch hulpmiddel in de zin van artikel 139d Sr.[10] Het hof overweegt kortgezegd dat de kaartlezer een vrij verkrijgbaar elektronisch apparaat is, dat doorgaans wordt gebruikt voor het uitlezen en beschrijven van (onder meer) NFC-chips. Niet blijkt uit de inrichting of de eigenschappen van de kaartschrijver/kaartlezer dat de producent heeft bedoeld een hulpmiddel te produceren dat hoofdzakelijk is ontworpen voor het begaan van delicten als computervredebreuk. De software waarmee OV-chipkaarten kunnen worden gemanipuleerd zijn wél te beschouwen als 'technisch hulpmiddel' in de zin van artikel 139d Sr. Het hof overweegt dat deze software immers specifiek is ontworpen om binnen te dringen in OV-chipkaarten, teneinde het saldo op OV-chipkaarten aan te kunnen passen en daarmee het plegen van computervredebreuk.

7. De verdachten hebben ongeveer 1,5 jaar lang gratis gereisd op eigen anonieme OV-chipkaarten. Translink Systems heeft zich als benadeelde partij in het geding gevoegd en vordert een bedrag van

---

[6] Waardekaarten niet persoonsgebonden, in tegenstelling tot 'betaalpassen'.

[7] Zie ook B.J. Koops & J.J. Oerlemans, 'Materieel strafrecht & ICT', p. 79-80 in: B.J. Koops & J.J. Oerlemans, *Strafrecht & ICT*, Monografieën recht en informatietechnologie, 3e druk, Den Haag: Sdu 2019.

[8] Hof Den Haag 26 mei 2015, ECLI:NL:GHDHA:2015:1427.

[9] Het begrip is overigens met de Wet computercriminaliteit III als volgt gewijzigd: *"Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken."* De chip kwalificeert ook nu als geautomatiseerd werk, evenals de paaltjes waarbij men moet in- en uitchecken en de achterliggende IT-infrastructuur.

[10] Hof Den Haag 9 september 2019, ECLI:NL:GHDHA:2019:2426.

€68.913,73 als materiële schade die zij hebben geleden. Dit schadebedrag is veel hoger dan in voorgaande zaken over het hacken van OV-chipkaarten om gratis te reizen.[11] De rechtbank concludeert dat de schadeberekening van aangeefster niet inzichtelijk is en een aantal fouten bevat en daarom een eigen berekening moet maken. Het bedrag van de schade ziet op het woon-werkverkeer van de verdachten. Bij het berekenen van het bedrag houdt de rechtbank rekening met het gemiddeld aantal vakantiedagen van werknemers in Nederland en de verdachten ook wel eens thuiswerkten. Op basis van 333 dagen en de kosten voor een retourtje Utrecht-Alkmaar van € 28,00 euro komt de rechtbank op een bedrag van € 9.324,00. De medeverdachte heeft minder frequent gebruik gemaakt van de eigen anonieme OV-chipkaart en moet een schadevergoeding betalen van € 5.264,00. De rechtbank verklaart de vordering voor het overige niet-ontvankelijk, omdat deze onvoldoende is onderbouwd. Zo is het onduidelijk hoe het schadebedrag aan de hand van de gegevens uit de tabellen is berekend, zien de tabellen ook op OV-chipkaarten waarvan de keys niet op de computers van verdachte en medeverdachte zijn aangetroffen.

8. In nieuwsartikelen en podcasts die verschenen naar aanleiding van deze zaak komt ten slotte nog interessante informatie over het opsporingsproces naar boven. Het blijkt behoorlijk lastig zijn dit soort OV-chipkaarthackers op te sporen als ze de encryptiesleutel kunnen achterhalen. Het begint met aangifte van Translink Systems: het bedrijf dat de OV-kaarten uitgeeft en transacties met de kaarten verwerkt. Dit bedrijf monitort ook de transacties en detecteert ongeregeldheden die mogelijk fraude betreffen. Na de aangifte zijn de verdachten met “ouderwets recherchewerk” door de politie geïdentificeerd. De verdachten zijn geïdentificeerd met name door het bekijken van camerabeelden op de stations van NS op het moment dat een frauduleus aangemerkte transactie plaats heeft gevonden. Vervolgens zijn de verdachten naar verluid tot hun woning gevolgd en zijn NAW-gegevens opgevraagd. Daarna heeft de politie beide verdachten op heterdaad betrapt bij het inchecken bij een poortje met een gehackte OV-chipkaart na observatie bij een vast reispunt van de verdachte.[12]

9. Als de software en middelen om OV-chipkaarten te hacken voor een breder publiek beschikbaar komen, kunnen we meer van dit soort zaken verwachten. De staatssecretaris van Infrastructuur en Waterstaat heeft in een Kamerbrief van 2 juli 2019 laten weten dat het de bedoeling is dat de OV-chipkaart in 2023 wordt uitgeschakeld.[13] Met een nieuw systeem moet het betaalgemak groter worden, omdat dan ook met andere betaalmiddelen kan worden betaald, zoals een bankpas of mobiele telefoon. Ongetwijfeld zullen hackers dan ook weer hun best doen het systeem te kraken en gratis te reizen.

[11] Zie noot 2. Het hoogste bedrag dat daarvoor was toegewezen aan de benadeelde partij was 2000 euro in Rb. Rotterdam 6 februari 2019, ECLI:NL:RBROT:2019:1101.

[12] Zie de BNR-podcast ‘Onderzoeksraad der dingen’, dossier #0010b en dossier #0010c: zwartrijden. Translink verwerkt per jaar 3 *miljard* transacties.

[13] Brief van 2 juli 2019, ‘Invoering nieuw OV betaalsysteem’, kenmerk IenW/BSK-2019/138197.