Jaargang 10
Editie 2
2023/2024

CYBERCRIME

E-MAGAZINE

LISA Law & ICT Students' Association

INHOUD

NORD

VOORWOORD

Beste lezer,

In een wereld waarin onze levens steeds meer verweven raken met technologie, vormt cybercrime een angstaanjagende realiteit die ons allemaal treft. Met elke klik op een link of elke transactie online, worden we geconfronteerd met de dreiging van hackers die klaar staan om onze gegevens te stelen, onze privacy te schenden en zelfs complete systemen te ontwrichten.

In dit e-magazine onderzoeken wij deze wereld van cybercrime. We verdiepen in de wereld van gijzelsoftware, hetgeen in 2021 leveringsproblemen bij Albert Heijn veroorzaakte en de KNVB dwong tot betaling van vermoedelijk 1 miljoen euro losgeld, terwijl statistieken aangeven dat één op de vijf grote bedrijven vorig jaar losgeld betaalde na een ransomware-aanval. Het stuk behandelt de impact van gijzelsoftware, de betaling van losgeld, cyberverzekeringen en beveiligingstips, gevolgd door de meldplicht en de rol van de AP en AVG. Daarnaast verdiept het e-magazine in de juridische vraagstukken rondom poortscanning als potentiële voorloper van computervredebreuk, met een focus op de interpretatie van 'binnendringen' volgens artikel 138ab Sr. Het onderzoekt het verschil in inzicht tussen rechtspraak en de conclusie van Advocaat-Generaal Vegter, en reflecteert kritisch op mogelijke tekortkomingen van de jurisprudentie. Dit juridisch-dogmatische onderzoek belicht de onduidelijkheid rondom de strafrechtelijke status van poortscanning, terwijl het fenomeen in een wereld van groeiende cybercriminaliteit aan relevantie wint. Centraal in het e-magazine staat ook het interview met Nynke Vellinga, zij is werkzaam bij de Rijksuniversiteit Groningen als onderzoeker. In het interview neemt zij ons mee in de juridische wereld van zelfrijdende auto’s en de problemen die de snelgroeiende techniek met zich meebrengt.

Afgelopen tijd is er wederom gewerkt aan het creëren van een e-magazine omtrent de wereld van cybercrime. Ik wil mijn commissie bedanken voor hun toewijding de afgelopen weken aan het neerzetten van ons tweede e-magazine. Met trots presenteren wij dan ook de tweede editie van het E-magazine van Lisa Law & ICT Students’ Association: ‘Cybercrime’.

In een wereld waarin elke klik een potentieel risico vormt en elke byte waardevolle informatie draagt, hopen wij met deze artikelen u als lezer wellicht te informeren hoe u uzelf kunt beschermen tegen deze vormen van cybercriminaliteit.

Namens de Carrièrecommissie,

Esther Bergsma
Voorzitter

• **Voorzitter**	Esther Bergsma
• **Secretaris**	Manon Hospers
• **Hoofdredacteur**	Chris Truong
• **Commissaris extern**	Roos den Boogert
• **Commissaris Promotie**	Nathan Porsoufi

NORD

Poortscanning in het kader van het strafrecht

Er raast een cyberoorlog in Europa: hackerscollectief *Anonymous* heeft de cyberoorlog aan de Russische Federatie verklaard.[1] Het hackerscollectief lanceerde cyberaanvallen waarmee Russische websites tijdelijk uit de lucht werden gehaald.[2] Een dergelijke cyberaanval vormt echter enkel de apotheose; meestal worden cyberaanvallen voorafgegaan door een poortscan om eerst informatie te vergaren over het doelwit.[3] Het zijn deze poortscans die tot een juridisch vraagstuk hebben geleid, namelijk of een poortscan op zichzelf voldoende is om te voldoen aan de bestanddelen 'wederrechtelijk binnendringen' van computervredebreuk in de zin van art. 138ab Sr. En zo niet, of wel sprake is van een poging daartoe als bedoeld in art. 45 Sr. De term 'binnendringen' is een vaag begrip waarvan niet altijd even duidelijk is of daaraan is voldaan in geval van een poortscan. De vraag of poortscanning kan worden geclassificeerd als computervredebreuk is niet bijzonder duidelijk beantwoord in de rechtspraak, maar de rechtspraak wat wel bestaat heeft desalniettemin kunnen rekenen op een verschil in inzicht met de Advocaat-Generaal.[4] Er bestaat onduidelijkheid omtrent de strafrechtelijke status van poortscanning, terwijl het gebruik daarvan toeneemt in een wereld waar cybercriminaliteit een opmars maakt.[5] Kortom, de rechtszekerheid omtrent dit actuele vraagstuk schiet tekort.

Dit stuk zal definiëren wat technisch wordt verstaan onder poortscanning, beschrijven in hoeverre de jurisprudentie van de Hoge Raad poortscanning ziet als een wederrechtelijke binnendringing in de zin van art. 138ab Sr en hoe dit zich verhoudt met de conclusie van Advocaat-Generaal Vegter, en ten slotte kritisch reflecteren op mogelijke tekortkomingen van de rechtspraak aan de hand van de literatuur. Kortom, het fenomeen poortscanning zal worden geplaatst in het huidig geldend recht via een juridisch-dogmatische onderzoeksmethode. Via deze methode zal het verschil in inzicht tussen juristen omtrent poortscanning en art. 138ab Sr worden beschreven en geëvalueerd. Dit stuk zal inzoomen op het delict computervredebreuk en het bestanddeel 'binnendringen'.

In hoeverre kan poortscanning worden gekwalificeerd als een wederrechtelijke binnendringing in een computersysteem met als gevolg (poging tot) computervredebreuk ex art. 45 en 138ab Sr?

Wat is poortscanning?

De eerste stap van vele misdrijven is een verkenning van het doelwit en in het geval van een digitale *locus delicti* wordt deze stap vormgegeven middels een poortscan. Het primaire doel van een poortscan is het vergaren van informatie van bepaalde poorten van het doelwit, vaak met de gedachte erachter om potentiële zwakke punten in de beveiliging te treffen en deze vervolgens te exploiteren in een cyberaanval om de aanval te versterken en preciseren.[6]

Ter illustratie: een typische poortscan opereert door het sturen van een internet pakketje richting een internetpoort van het doelwit. Een internetpoort is de ontvanger en verzender van internet pakketjes en via deze pakketjes vindt communicatie plaats tussen computersystemen op het internet.[7] Vervolgens zal het doelwit automatisch een respons terugsturen, en deze respons wordt vervolgens geanalyseerd door de poortscanner. Op basis van deze analyse kan onder andere bepaald worden of de poort open of dicht is.[8] Via deze informatie kan een cyberaanvaller gerichter zijn aanval uitvoeren op het doelwit.

Poortscanning in de rechtspraak

De rechtspraak van Nederland is op het gebied van poortscanning ambigu. De Hoge Raad oordeelde dat het enkel poortscannen op zichzelf niet zonder meer een wederrechtelijke binnendringing tot gevolg heeft zoals computervredebreuk dit vereist.[9] De Hoge Raad had *in concreto* opgemerkt dat het gebruik van een poortscan die werd geblokkeerd door de geautomatiseerde beveiliging van het doelwit onvoldoende was om een binnendringing aan te tonen. De enkele mogelijkheid dat de verdachte toegang had verkregen tot bestanden in het systeem is onvol-

1 Dubois & Vanhecke, *Het Nieuwsblad* 26 februari 2022.

2 Idem.

3 Long e.a. 2006, p. 96.

4 HR 9 april 2019, ECLI:NL:HR:2019:560 (concl. A-G P.C. Vegter), r.o. 2.4, *NJ* 2019/358, m.nt. N. Rozemond.

5 Dutta e.a. 2022, p. 159.

6 Long e.a. 2006, p. 96.

7 Kernighan 2017, p. 152.

8 Long e.a. 2006, p. 101.

9 HR 9 april 2019, ECLI:NL:HR:2019:560 (concl. A-G P.C. Vegter), r.o. 2.4, *NJ* 2019/358, m.nt. N. Rozemond.

doende. Uit deze uitspraak kan dus worden afgeleid dat een poortscan op zichzelf onvoldoende is om te classificeren als een binnendringing en dat het blijft bij een poging tot computervredebreuk in de zin van art. 138ab Sr.[10] Er zal dus echt sprake moeten zijn van verworven toegang en niet enkel een poortscan. Deze interpretatie wordt ook aangehaald als *de facto* rechtsregel in de literatuur.[11]

Daarentegen kwam Advocaat-Generaal Vegter tot een heel andere conclusie. Vegter wees erop dat de poortscan zou zijn verricht *in* het doelwit en dat de verdachte via deze poortscan binnen het systeem zocht naar poorten waarmee hij toegang kon verkrijgen naar privégegevens. De verdachte zou met zijn poortscan dus al in de website zijn geweest en werd zelfs geblokkeerd door het beveiligingssysteem van het slachtoffer, wat zou betekenen dat het systeem had gereageerd op de binnendringing. Hierbij redeneerde Vegter op analoge wijze door de bestanddelen wederrechtelijk binnendringen te vergelijken met huisvredebreuk in de zin van art. 138 Sr. Daaruit volgt namelijk dat al sprake is van een voltooide binnendringing in het geval iemand via inklimming toegang tot een woning verschaft, en gezien de poortscan was verricht in het doelwit is dit vergelijkbaar met een succesvolle inklimming. Dus is er wel degelijk sprake van een voltooide wederrechtelijke binnendringing in een geautomatiseerd werk.[12]

Er zijn dus twee tegenstrijdige stromingen ontstaan omtrent de strafbaarheid van poortscanning met het oog op art. 138ab Sr. Aan de ene kant staat de opvatting van de Hoge Raad, die poortscanning op zichzelf onvoldoende acht om te spreken van binnendringing. Hier tegenover staat de strengere opvatting van Vegter die erop wijst dat een poortscan plaatsvindt binnen een systeem en dus ook kan worden geclassificeerd als een binnendringing in de zin van art. 138ab Sr.

Poortscanning in de literatuur

De vraag of er sprake is van binnendringing in de zin van art. 138ab Sr met enkel een poortscan is ook aan de orde geweest in de literatuur. Rozemond heeft in zijn noot vraagtekens gezet omtrent de redenatie van Vegter.[13] Rozemond bekritiseert allereerst de analoge vergelijking van Vegter door erop te wijzen dat het wellicht klopt dat inklimming leidt tot binnendringing van een woning, maar dat dit niet te vergelijken is met het enkel bezoeken van een openbare website en daarop een poortscan uit te voeren. Als het enkel bezoeken van een openbare website al zou leiden tot een binnendringing, dan zou dit betekenen dat iedere bezoeker een website binnendringt in de zin van art. 138ab Sr. Teleologisch gezien zou dit niet de bedoeling moeten zijn geweest van de bepaling en is hij het dus niet eens met de stelling van Vegter dat een poortscan op zichzelf leidt tot een voltooide wederrechtelijke binnendringing.[14]

Rozemond komt vervolgens met een eigen analogie die aansluit bij de heersende leer van de Hoge Raad en deze zelfs aanvult. Volgens Rozemond moet een poortscan ingebeeld worden als het onderzoeken of een raam of deur open staat vanaf de openbare weg, aangezien een poortscan in veel gevallen, net zoals in casu, zal plaatsvinden op een openbare website. Er kan dus pas sprake zijn van een binnendringing in de zin van art. 138ab Sr in het geval dat de dader via de poortscan een open poort vindt en deze ook daadwerkelijk gebruikt om te infiltreren.[15] Deze gedachtegang sluit zich aan bij andere literatuur. Van Kempen beschrijft net zoals Rozemond dat binnendringing vereist dat er sprake moet zijn van een verwezenlijkte binnendringing waarmee werkelijke toegang moet zijn verworven tot het medium.[16] Daarnaast zou het woord 'binnendringing' volgens Van Kempen naar normaal taalgebruik impliceren dat een vorm van weerstand wordt overwonnen.[17] Een dergelijke overwinning of toegangsverwerving vindt nog niet plaats bij een poortscan. Een dergelijke gedachtegang van Rozemond en Van Kempen wijst er dus op dat het enkel gebruikmaken van een poortscan onvoldoende is om te kunnen spreken van een binnendringing in de zin van art. 138ab Sr en bevestigt dus de geïmpliceerde rechtsregel van de Hoge Raad.

Maar houdt deze analogie stand op technisch vlak? Een poortscan bestaat uit het versturen van een internet pakketje naar een poort envervolgens het checken van reactie van een poort.[18] Dit impliceert dat er dus wel meer wordt gedaan dan enkel vanaf de openbare weg kijken naar een poort; er wordt actief gehandeld om een poort te controleren, dit kan naar analogie vergeleken worden met het trekken aan de deurhendel om te checken of de deur open is. Echter bestaat hier een mogelijke weerlegging op. Het internet communiceert en functioneert immers voor een aanmerkelijk deel door het sturen van *IP*-pakketjes om informatie te vergaren en op het internet te

10 Gritter & Wolswijk 2021, p. 243.

11 Van Kempen, *DD* 2021/62, p. 793.

12 Concl. A-G P.C. Vegter, ECLI:NL:HR:2019:560, bij HR 9 april 2019, *NJ* 2019/358, m.nt. N. Rozemond.

13 Rozemond, *NJ* 2019/358, par. 1 (online Kluwer Navigator).

14 Rozemond, *NJ* 2019/358, par. 2 (online Kluwer Navigator).

15 Idem.

16 Van Kempen, *DD* 2021/62, p. 793.

17 Idem.

18 Long e.a. 2006, p. 96.

surfen.[19] Het verzenden en versturen van dergelijke pakketjes kan dus worden gezien als het gebruik van zintuigen op het internet; op deze wijze neemt een computersysteem waar. Wat dat betreft is het versturen van pakketjes als onderdeel van een poortscan toch vergelijkbaar met het enkel kijken naar poorten vanaf de openbare weg.

Kortom, de analogie van Rozemond lijkt enigszins technisch correct te zijn, maar wellicht wel wat kort door de bocht. Het is ambigu; beide analogieën kunnen aangehaald worden maar de in de vorige alinea besproken deurhendelanalogie versterkt wel het standpunt dat al sprake is van een begin van uitvoering, maar Rozemond heeft dit dilemma onbesproken gelaten. Desalniettemin zou dit verschil in analoge visie niet direct tot een verschillende conclusie leiden; ook al zou na het trekken aan de deurhendel de poort open blijken, is er nog geen sprake van binnendringen als de verdachte vervolgens niet naar binnen gaat.

Poortscanning en poging

De Hoge Raad heeft dus bepaald dat een enkele poortscan onvoldoende is om te spreken van een voltooide binnendringing, omdat daarmee nog niet vaststaat dat daadwerkelijk toegang is verworven. kan worden herleid dat volgens de Hoge Raad wel sprake is van een poging tot binnendringing in de zin van art. 45 en 138ab Sr.[20] Om te kunnen spreken van een poging in de zin van art. 45 lid 1 Sr moet er sprake zijn van een begin van uitvoering. Daar is sprake van indien is voldaan aan het Cito-criterium.[21] Volgens Rozemond is dat het geval bij een poortscan; een poortscan naar zwakke punten in de beveiliging is "een gedraging die naar haar uiterlijke verschijningsvorm in voldoende concrete mate is gericht op het voltooien van het binnendringen in een geautomatiseerd werk of een deel daarvan".[22] De poortscan zou namelijk volgens Rozemond speciaal ontworpen zijn om open poorten te vinden en die te exploiteren om toegang te verwerven tot privébestanden of netwerken van een website.[23]

Bovendien kan met de hierboven voorgestelde analogie, namelijk dat een poortscan vergeleken dient te worden met het actief controleren van de deur middels het trekken aan de deurhendel, het argument worden versterkt dat een poortscan de kenmerken toont van een pogingshandeling. Het drukken tegen een deur om deze te checken lijkt naar uiterlijke verschijningsvorm meer gericht op het voltooien van het binnendringen dan enkel het onderzoeken van een poort vanaf de openbare weg.

Kortom, de conclusie lijkt te zijn dat een poortscan wegens zijn uiterlijke verschijningsvorm een begin van uitvoering vormt van het binnendringen in de zin van art. 45 en 138ab Sr. De literatuur sluit wat dat betreft aan bij de rechtspraak en wordt ook ondersteund door meerdere technische analogieën.

Conclusie

Al met al, waar de Advocaat-Generaal van mening was dat een poortscan wel degelijk een voltooide wederrechtelijke binnendringing opleverde in de zin van art. 138ab Sr, oordeelde de Hoge Raad het tegenovergestelde. Een poortscan is op zichzelf onvoldoende om te kunnen spreken van een voltooide binnendringing, wel is er sprake van een poging daartoe.[24] De literatuur sloot zich aan bij de Hoge Raad; zo beweren Rozemond en Van Kempen dat een binnendringing een daadwerkelijke toegangsverwerving vereist en niet enkel een poortscan.[25] *A fortiori*, Rozemond beschrijft ook hoe een poortscan over de kenmerken beschikt van een pogingshandeling in de zin van art. 45 Sr wegens de uiterlijke verschijningsvorm van een scan.[26]

Daarnaast kan op technisch vlak een poortscan worden vergeleken met het trekken aan de deurhendel om te checken of hij open is of niet wegens de inherente actieve handeling die een poortscan vereist door het versturen van internet pakketjes. Deze nieuwe analogie strekt verder dan die van Rozemond maar blijft genuanceerd ten aanzien van die van Vegter, en schetst met het oog op de techniek het meest correcte beeld. Middels deze analogie en de genoemde argumenten van de Hoge Raad en literatuur kan een poortscan dus worden gekwalificeerd als een poging tot wederrechtelijke binnendringing in de zin van art. 138ab Sr, maar nog niet als een voltooid delict. De poortscanners van Anonymous schilderen zichzelf wellicht af als anonieme hulpverlener, maar het recht ziet ze wel degelijk als pogende cybercrimineel.

Namens de Carrièrecommissie,

Chris Truong

19 Kernighan 2017, p. 150.

20 Gritter & Wolswijk 2021, p. 243.

21 HR 24 oktober 1978, ECLI:NL:PHR:1978:AC6373, r.o. 3, *NJ* 1979/52, m.nt. Th.W. van Veen (Uitzendbureau Cito).

22 Rozemond, *NJ* 2019/358, par. 3 (online Kluwer Navigator).

23 Idem.

24 HR 9 april 2019, ECLI:NL:HR:2019:560 (concl. A-G P.C. Vegter), r.o. 2.4, *NJ* 2019/358, m.nt. N. Rozemond.

25 Rozemond, *NJ* 2019/358, par. 2 (online Kluwer Navigator); Van Kempen, *DD* 2021/62, p. 793.

26 Rozemond, *NJ* 2019/358, par. 3 (online Kluwer Navigator).

Een interview met Nynke Vellinga

Veel rechtenstudenten nemen zich voor om na hun studie de advocatuur in te gaan, maar er is natuurlijk veel meer mogelijk. Zo heeft Nynke Vellinga ervoor gekozen om het onderzoek in te gaan. In dit interview geeft Nynke Vellinga een beeld van hoe het is om onderzoekster aan de RUG te zijn en vertelt ze over haar juridisch onderzoek naar zelfrijdende auto's.

Wat houden uw werkzaamheden aan de RUG precies in?

Ik ben postdoc onderzoeker aan de faculteit Rechtsgeleerdheid van de Rijksuniversiteit Groningen en ik zit bij de STeP onderzoeksgroep. De Secu§rity, Technology & e-Privacy onderzoeksgroep is een groep onder leiding van Joe Cannataci, hoogleraar van de Universiteit van Malta, en Jeanne Mifsud Bonnici, hoogleraar aan de Rijksuniversiteit Groningen. Ik doe onderzoek naar de juridische aspecten van autonoom vervoer, in het bijzonder zelfrijdende auto's. Daar ben ik destijds ook aan de RUG op gepromoveerd. Van 2016 tot 2020 heb ik aan mijn proefschrift gewerkt. Daarna heb ik deze postdoc plaats gekregen.

Mijn onderzoek wordt voor meerdere doeleinden gebruikt. Het is natuurlijk wetenschappelijk onderzoek, dus het wordt gepubliceerd en daar volgen discussies op en dergelijke. Ik heb ook een aantal keer geschreven voor het Ministerie van Infrastructuur en Waterstaat, daar wordt het gebruikt in trajecten waarin beleid wordt gemaakt. Dit geeft dus concrete gevolgen aan wat ik achter mijn bureau zit te doen, dat is altijd wel heel fijn.

Naast mijn werkzaamheden bij de RUG, heb ik ook een fellowship aan de Universiteit van Milaan. Dit is onbezoldigd, iets wat je ernaast doet. De eisen die er aan je kunnen worden gesteld, zijn daarmee ook relatief beperkt. Het is met name een onderzoekscommunity waarin ideeën worden uitgewisseld en waarin je ideeën kan testen. In juni komt er een congres van deze fellowship waarop ik spreek en zo help je elkaar door uitwisseling van kennis en ideeën. De Nederlandse aanpak is namelijk niet hoe het in Italië gebeurt, en in de VS is het weer heel anders, zo kan je een hoop van elkaar opsteken. Als het om zelfrijdende auto's gaat, zie je dat er een bepaalde lijn is binnen Europa, bepaalde dingen worden op Europees niveau geregeld, maar heel veel dingen ook niet. Met Duitsland is het verschil bijvoorbeeld heel groot. Zij hebben er een speerpunt van gemaakt en hebben gezegd nieuwe wetgeving te gaan ontwikkelen. Daar zijn bepaalde technologieën dus al toegestaan. Maar je rijdt hier wel de Nederlandse grens over, wat dan? Daar moet Nederland dan dus op reageren. Nederland kan leren van de Duitse aanpak en beoordelen of ze dat ook hier zouden willen zien.

Of dat je denkt dat het niet op nationaal niveau moet worden aangepakt, maar op Europees niveau of op nog hoger niveau. De VS is natuurlijk van oudsher de voorloper op dit vlak, maar daar verschilt wetgeving per staat op dit punt. Er zijn dus een hele hoop verschillende benaderingen, die ook weer kunnen leiden tot ideeën voor wat hier in Nederland zou kunnen werken.

Hoe ziet een werkdag er voor u uit?

Ik zit eigenlijk best veel achter mijn bureau onderzoek te doen, wat allemaal moet resulteren in een paper of een onderwerp. Eigenlijk een soort scriptie schrijven, maar dan op een hele grote schaal. Hierbij gebruik ik voornamelijk digitale bronnen. Daarnaast heb ik ook een paar onderwijstaken, zoals het spreken met scriptiestudenten over hun onderzoeksplan en zo nu en dan geef ik ook hoorcolleges.

Welke studie heeft u gevolgd?

Ik heb mijn studie ook in Groningen afgerond. Ik heb de bachelor Nederlands recht gedaan, maar dus geen IT-recht of iets in het Engels. En ik heb ook de master Nederlands recht gevolgd, met als specialisatie privaatrecht. Het is dus een beetje een samenloop van omstandigheden dat ik hier bij deze baan terecht ben gekomen. Voor mijn master heb ik een scriptie geschreven over de aansprakelijkheidsaspecten van zelfrijdende auto's. Dat was toen nog heel nieuw, amper nog iemand die er wat van af wist. Er was ook heel weinig literatuur beschikbaar. Mensen hadden over zelfrijdende auto's vooral het beeld dat dat alleen in films gebeurt, maar tegenwoordig is dat natuurlijk aan het veranderen.

Waarom heeft u ervoor gekozen het onderzoeksveld in te gaan?

Voor mij was het heel eenvoudig, want ik vind onderzoek doen ontzettend leuk. Het mooie van onderzoek vind ik ook dat je vooruit kunt lopen op de muziek. Je kunt ontwikkelingen eerder waarnemen en daar al iets mee doen voordat het tot problemen heeft geleid. Je hebt ook een zekere mate van vrijheid daarin. Je kan je gedachten de vrije loop laten en kijken wat je in de ideale wereld graag zou willen zien. En dan vervolgens jezelf afvragen of we dat in de huidige wereld kunnen inpassen. Dat ik dit zo leuk vond, kwam ik vooral achter tijdens het schrijven van mijn scriptie.

Hoe wordt er in voertuigen rekening gehouden met privacy en cybersecurity?

Het is zo dat de voertuigen het best functioneren als er een verbinding is met de omgeving, dus een digitale vorm van communicatie met de omgeving. Dit betekent dat het voertuig niet alleen met zijn camera's waarneemt dat een stoplicht rood is, maar dat dit het voertuig ook wordt verteld. Tesla heeft bijvoorbeeld het probleem gehad dat een auto stopte voor een volle maan, dat kan uiteindelijk voor gevaarlijke verkeerssituaties zorgen.

Met al die digitale communicatielijnen komen ook kwetsbaarheden. Alles wat je kunt gebruiken voor vertrouwde informatie kun je ook gebruiken voor kwaadaardige communicatie. Hackers kunnen in deze voertuigen komen en bepaalde commando's geven. In 2015 heeft een journalist van Wired, een Amerikaans tijdschrift over technologie, met twee ethische hackers een Jeep gehackt. De hackers zijn via het entertainmentsysteem het systeem van de auto binnengekomen. Zij waren in staat om de motor van de auto volledig uit te schakelen, terwijl deze reed op de snelweg. Dat is natuurlijk levensgevaarlijk. Je kunt je voorstellen dat als dat al lukt bij een voertuig uit 2015, waarbij de enige verbinding met het internet plaatsvond via het entertainmentsysteem, de kwetsbaarheden steeds meer toenemen nu de technologie in voertuigen verder ontwikkeld is. Je moet ook aan scenario's denken waarbij een hacker uit naam van een terroristische organisatie werkt, meerdere voertuigen tegelijkertijd hackt en daarmee een aanslag pleegt. Dat zijn hele enge scenario's.

Er bestaat wel wat wet- en regelgeving op het gebied van cybersecurity in voertuigen, maar deze is pas laat in 2022 in werking getreden. Deze wet- en regelgeving is echter nog vrij beperkt. Bijvoorbeeld, als een hacker eenmaal het voertuig is binnengedrongen, is er geen vereiste isolatie tussen veiligheidskritische delen van de auto en niet-veiligheidskritische delen, waardoor het nog steeds mogelijk is om het voertuig uiteindelijk te besturen door het hacken van het entertainmentsysteem. Actie op dit gebied is dan ook nog steeds nodig.

Denkt u dat het haalbaar is om op lange termijn cybersecurity te waarborgen in voertuigen?

De regelgeving is op dit moment te mild. Er moeten concretere en duidelijkere regels komen om het voertuig te beveiligen en cybersecurity te waarborgen. Als je alleen al naar de definitie van cybersecurity zoekt, vind je er zo veertig, aldus er moet een vaste lijn in komen. Ook omdat cybersecurity voorheen enkel gold voor computers, maar het nu ook een verkeersveiligheidskwestie is geworden.

Dilemma: met alle kennis die u in uw onderzoeken heeft vergaard in gedachten, zou u op dit moment de voorkeur hebben voor een volledig autonome auto?

Momenteel is de technologie nog niet zo ver ontwikkeld; dat zal nog even duren. In de VS zijn er wel testmechanismen waarbij voortdurend stappen worden gezet om autonome voertuigen te verbeteren, maar waar zich ook tal van problemen voordoen. Sommige bedrijven verliezen hun vergunning om te testen vanwege ongelukken. Wanneer de technologie veilig genoeg lijkt, zou mijn voorkeur uitgaan naar een autonome auto. Echter, eerlijk gezegd, zou ik ook instappen in een auto die door jullie wordt bestuurd. Dit betekent echter niet dat je gegarandeerd goed en veilig kunt rijden, en hetzelfde geldt voor een autonome auto. De autonome auto wordt uitvoerig getest en gekeurd voordat mogelijk wordt vastgesteld dat deze veilig genoeg is om te rijden. Als er zich echter een software-update of ander probleem voordoet waar we niet op hadden gerekend, is dat inherent aan de risico's van nieuwe technologische ontwikkelingen. Dingen kunnen misgaan, maar uiteindelijk vinden deze ontwikkelingen plaats omdat menselijke bestuurders lang niet zo goed zijn als we denken.

In 90-94% van de gevallen van ongelukken is menselijk falen de oorzaak of heeft het er sterk aan bijgedragen. Het is eigenlijk best eng om bij een mens in een voertuig te stappen, hoewel dat momenteel de beste optie is die we hebben. Als we de mens uit de auto kunnen halen, kunnen we het aantal ongelukken mogelijk verminderen. De reactietijd van een zelfrijdende auto is namelijk vele malen sneller dan die van menselijke bestuurders. Een mens heeft ongeveer een seconde nodig om nieuwe informatie te verwerken en daarop te reageren, terwijl een zelfrijdende auto in milli- of nanoseconden reageert. Wanneer een mens een noodstop maakt, gebruikt hij slechts 40% van de totale remkracht van de auto, terwijl een zelfrijdende auto een volledige noodstop kan maken. De samenwerking tussen menselijke bestuurders en zelfrijdende auto's belooft in de toekomst erg interessant te worden.

Maar als er nu een zelfrijdende auto voor komt rijden, dan slaat u die dus wel nog even over?
Ja, die sla ik misschien nog wel even over. Ook ten behoeve van het andere wegverkeer. Zo'n zelfrijdende auto zou in een land als Nederland met alle fietsers stilstaan en 'huilen'.

Welke ontwikkelingen op het gebied van zelfrijdende auto's zijn er in de Verenigde Staten?
In bijvoorbeeld Arizona en Nevada is het mogelijk om mensen te vervoeren in zelfrijdende auto's, en Californië is zelfs hèt voorbeeld op het gebied van technologische ontwikkelingen met betrekking tot zelfrijdende auto's. San Francisco fungeert als een soort testhoofdstad op het gebied van zelfrijdende auto's in de VS. Ongeveer zes bedrijven hebben daar een vergunning om deze tests uit te voeren.

Ziet u dat op het gebied van zelfrijdende auto's Nederland zich terughoudender opstelt ten opzichte van de Verenigde Staten?
Ja, over het algemeen wel. In Nederland worden er andere eisen gesteld. Zo is het mogelijk om te testen met zelfrijdende auto's, maar met een bestuurder die de mogelijkheid heeft om van buitenaf de controle over te nemen. Hier is nog steeds een bestuurder nodig, terwijl sommige staten in de Verenigde Staten van dit vereiste zijn afgestapt.

Verwacht u nog lang in dit onderzoeksveld werkzaam te zijn of denkt u op een gegeven moment een andere richting te willen inslaan?
Eigenlijk wel. Er is nog veel te doen, dus ik zal me nog lange tijd kunnen vermaken. Ik kan gemakkelijk uitbreiden naar andere vormen van vervoer, zoals het gebruik van autonome software in vliegtuigen of autonome scheepvaart. Dit zijn allemaal onderwerpen die mijn onderzoek aansnijden en gebieden waar ik inspiratie uit kan halen. Hetzelfde geldt voor het aantal rechtsgebieden dat van toepassing is op autonome auto's. Het omvat privaatrecht, strafrecht, bestuursrecht; het is allemaal van toepassing. Ik heb talloze mogelijkheden om verschillende routes in te slaan. Het onderzoek is eindeloos, maar op een positieve manier

Namens de Carrièrecommissie,

Roos den Boogert en Esther Bergsma

Gijzelsoftware

Wellicht kan u het zich nog wel herinneren: in 2021 kon er dagenlang minder voedsel worden geleverd aan onder andere Albert Heijn. Het gevolg was boze klanten en lege kaasschappen. Dit keer was de oorzaak geen staking door boeren of werknemers. Nee, de oorzaak was gijzelsoftware. Deze gijzelsoftware, ook wel ransomware genoemd, zorgde ervoor dat de automatiseringssystemen uitvielen en alles met de hand moest worden gedaan.[1] Een ander slachtoffer van een gijzelsoftware-aanval is de Koninklijke Nederlandse Voetbalbond (hierna: KNVB). De KNVB kreeg twee opties: onderhandelen of niet onderhandelen. Om te voorkomen dat gegevens openbaar werden gemaakt, besloot de voetbalbond te onderhandelen en losgeld te betalen. Hoeveel er is betaald, is niet bekendgemaakt, maar vermoedelijk ging het om zo'n 1 miljoen euro. De KNVB was niet de enige die losgeld betaalde.[2] Uit cijfers van de politie en beveiligingsbedrijven blijkt dat vorig jaar één op de vijf bedrijven (met meer dan 100 werknemers) losgeld betaalde na een aanval met gijzelsoftware.[3] In dit stuk wordt eerst behandeld wat gijzelsoftware inhoudt. Ten tweede wordt de betaling van losgeld behandeld. Als derde worden de cyberverzekeringen behandeld, en worden tips gegeven om uzelf te beschermen tegen een aanval. Daarna wordt de meldplicht behandeld. Bij deze meldplicht is er bijzondere aandacht voor de Autoriteit Persoonsgegevens (hierna: AP) en Algemene Verordening Gegevensbescherming (hierna: AVG). We sluiten af met een conclusie.

Wat is gijzelsoftware?

Gijzelsoftware is een vorm van malware. Dat is een verzamelnaam voor ongewenste kwaadaardige software. Bij gijzelsoftware vergrendelen hackers databestanden op een computernetwerk: de bestanden en alle daarin opgeslagen gegevens worden 'gegijzeld'. Ransomware beperkt zich niet alleen tot mobiele telefoons of laptops. Ook gegevens die in de Cloud zijn opgeslagen of back-ups kunnen versleuteld worden.[4]

De gijzelsoftware kan binnenkomen op verschillende manieren. Bijvoorbeeld door zwakheden in het IT-systeem of door middel van *phishing*. Via de e-mail komt phishing het meeste voor. Hierbij lijkt het alsof de e-mail is verstuurd door een vertrouwd contact: het slachtoffer wordt bijvoorbeeld aangesproken op een betrouwbare manier en de e-mail is afkomstig van een bekende domeinnaam. Vervolgens wordt in zo'n e-mail gevraagd om gegevens achter te laten op een ogenschijnlijk legitieme website of wordt gevraagd om op een bepaalde link te klikken of om gegevens te sturen. Deze blijken echter in het geval van gijzelsoftware kwaadaardige software te bevatten. Daardoor kunnen hackers de computer binnendringen. Na een verkenning, en soms het stelen van data, wordt de gijzelsoftware actief: de bestanden zijn 'gegijzeld'. Dit heeft als gevolg dat je niks meer kunt doen met de bestanden. Om dit op te heffen zit er volgens de hackers maar één ding op: betalen. Vaak gaat het dan om het betalen van een groot geldbedrag.[5]

De Universiteit van Maastricht was slachtoffer van zo'n phishing via e-mail. Toen medewerkers van de universiteit op de link in de e-mail klikten, konden de hackers via een virus binnenkomen op het netwerk. Uit forensisch onderzoek bleek dat deze hackers twee maanden in het netwerk van de universiteit zaten. Zo konden zij het netwerk goed in kaart brengen en de gijzelsoftware effectief uitrollen. Hierbij werden ook de back-ups van de universiteit ontoegankelijk gemaakt, waardoor bestanden niet meer konden worden teruggezet. Om onder andere te voorkomen dat studenten niet konden afstuderen betaalde de universiteit 30 bitcoin aan de hackers: op dat moment hadden die een waarde van 200.000 euro.[6]

De betaling van losgeld

Alhoewel er dus vaak losgeld wordt betaald, zit de overheid juist in de maag met bedrijven die los-

1 'Geen kaas: hoe een hack zorgt voor lege schappen in de AH', rtlnieuws.nl.

2 'Cybersecuritywereld over geslaagde afpersing KNVB: 'Dit maakt het alleen maar erger'', parool.nl.

3 'Een op de vijf bedrijven betaalde losgeld na aanval met gijzelsoftware', nos.nl.

4 'Ransomware (gijzelsoftware) voorkomen en verwijderen, consumentenbond.nl.

5 'Ransomware', digitaltrustcenter.nl.

6 'Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald', nos.nl.

geld betalen. Hoewel er geen wettelijk verbod is, raadt het Ministerie van Justitie en Veiligheid dan ook af om losgeld te betalen.[7] Zo is er geen enkele garantie dat men na betaling weer toegang heeft tot de gegevens en de gijzelsoftware ook daadwerkelijk uit het netwerk is. Hierdoor kunnen de hackers maanden later weer toeslaan. Als uw volledige IT-omgeving is gehackt, bent u nog verder van huis. Er moet dan onder andere forensisch onderzoek worden gedaan, alles moet worden opgeschoond en vaak moet alles zelfs opnieuw worden opgebouwd.[8] Daarnaast houdt het betalen van losgeld de zwendel in stand. Als er in alle gevallen geen losgeld meer wordt betaald, is het voor hackers ook niet meer lucratief om aan te vallen. Nu wordt het 'verdiende' geld meteen weer gebruikt voor nieuwe aanvallen. Daarnaast wordt het geld gebruikt om de techniek voor de aanvallen verder te verfijnen.[9] De reden dat veel bedrijven toch losgeld betalen?

Het ontsleutelen van gegevens is tijdrovend en lastig en in sommige gevallen zelfs onmogelijk. Als er bijvoorbeeld geen back-ups zijn gemaakt of de back-ups ook gegijzeld zijn. In sommige gevallen is het zelfs goedkoper dan alle herstelwerkzaamheden, die weken tot maanden kunnen duren. Vaak dreigen de hackers de persoonsgegevens en informatie zonder betaling openbaar te maken. Daarbij zorgt het stilleggen van de bedrijfsvoering vaak voor aanzienlijk omzetverlies en moeten aan gedupeerden vaak schadevergoedingen worden betaald. Bedrijven kunnen anders zelf failliet gaan. Om nog niet eens te spreken over de (mogelijke) reputatieschade.[10] Niet voor niets noemde de vicevoorzitter van de Universiteit van Maastricht de keuze voor het wel of niet betalen van het losgeld een 'duivels dilemma'.[11]

Cyberverzekeringen

De vergoeding van losgeld is om die reden zelfs onderdeel van sommige verzekeringen. Deze cyberverzekeringen bieden niet alleen hulp bij het herstel van data, maar bieden ook een (gedeeltelijke) vergoeding voor het losgeld. Ook boetes die zijn opgelegd door de AP kunnen onder de verzekering vallen. Bijvoorbeeld doordat een datalek te laat of niet is gemeld. Vooral om de vergoeding van het losgeld en het betalen van de boetes is veel te doen geweest.

Het zal u niets verbazen dat deze cyberverzekeringen punt van discussie zijn in de samenleving en literatuur. Zo heeft de overheid de mogelijkheid onderzocht om losgebeldbetalingen van verzekeraars te verbieden.[8] Sommige experts stellen dat hackers hierdoor hogere bedragen gaan vragen, wat leidt tot meer aanvallen. Daarentegen stelt jurist Nynke Brouwer, die promoveerde op een proefschrift over cyberverzekeringen, dat een dergelijk verbod weinig zin heeft. In haar onderzoek werd geen duidelijk verband gevonden tussen de beslissing van een bedrijf om te betalen en het hebben van een verzekeringsdekking voor het betaalde losgeld.[12] 'Verzekerd of niet, bedrijven betalen omdat ze niets anders kunnen'. Daarbij is een verzekering een overeenkomst, waarbij contractsvrijheid geldt. Een verbod op zo'n verzekering vormt een vergaand ingrijpen daarop. Op dit moment is het verbod op een dergelijke verzekering er (nog) niet. Hoe dan ook blijft de betaling van losgeld problematisch: zowel met als zonder verzekering.[13]

Voor hackers zijn de aanvallen met ransomware daarentegen bijzonder lucratief. Dat blijkt ook uit het feit dat er volledige bendes actief zijn. Eén van de grootste wereldwijde hackersgroepen is Lockbit. Lockbit is onder andere verantwoordelijk voor de gijzelsoftware-aanval op de KNVB. De schatting is dat ze alleen al van Amerikaanse organisaties minstens 84 miljoen dollar hebben geëist. Het probleem daarbij is dat deze groepen steeds professioneler worden. Zo heeft Lockbit zelfs een klantenservice om bedrijven waarvan hun data is gegijzeld te assisteren en drempels bij de betaling weg te nemen. Mocht een bedrijf niet weten hoe zij via bitcoin kunnen betalen, helpt Lockbit daarbij.[14] Afgelopen februari kwam naar buiten dat de website van Lockbit neer is gehaald door een coalitie van internationale opsporingsdiensten. Uiteindelijk werden twee verdachten opgepakt.[15] Destijds gaf Rolf van Wegberg, onderzoeker aan de Technische Universiteit Delft, al aan dat het vooral belangrijk is dat de mensen achter het platform worden gearresteerd. 'Sommige hackers zijn sleutelfiguren. Mochten zij opgepakt worden, is het voor anderen moeilijker om met de bestaande software door te gaan. Het blijft echter lastig deze personen op te pakken, omdat zij vaak in meerdere landen zitten. Verder zitten ze vaak in landen als Rusland, dat onderdanen

7 Aanhangsel Kamervragen II 2021-2022, nr. 225, p.1.

8 'Om je te weren tegen ransomware moet je de keten snappen', nscs.nl.

9 Cybersecuritybeeld Nederland (CSBN) 2021, p.29.

10 'Overheid in actie tegen betalen van losgeld aan ransomware-criminelen', nos.nl.

11 Universiteit Maastricht, *Reactie op rapport Fox-IT*, 5 februari 2020, te raadplegen op https://www.maastrichtuniversity.nl/file/49830/download?token=ouU_YJC4.

12 Nynke Brouwer, *De cyberverzekering vanuit civielrechtelijk perspectief*, juni 2021, te raadplegen op: https://repository.ubn.ru.nl/bitstream/handle/2066/237797/237797.pdf?sequence=1&isAllowed=y.

13 'Advocaat Nynke Brouwer promoveert op onderzoek naar cyberverzekeringen', dirkzwager.nl.

14 'Grote hackersgroep Lockbit deels opgerold door internationale politie', trouw.nl.

15 'Law enforcement disrupt world's biggest ransomware operation', europol.europa.eu.

niet uitlevert'.[16] Met het nieuws leek het alsof een van de grootste bendes is opgedoekt. Maar na een week was de site alweer online. Op de site staan zelfs alweer nieuwe slachtoffers, zoals een Brits staalbedrijf.[17]

Tips om uzelf te beschermen

Al met al kunnen gijzelsoftware-aanvallen aanzienlijke financiële schade veroorzaken. De laatste jaren is daarbij een nieuwe trend zichtbaar: hackers voeren meer gerichte gijzelsoftware-aanvallen uit, op doelwitten die een hoger losgeld bedrag kunnen betalen.[18] De verwachting is zelfs dat de financiële schade in 2024 42 miljard dollar zal bedragen tot naar verwachting 160 miljard dollar in 2028.[19] Daarbij maken de hackers een afweging: als de systemen heel goed beveiligd zijn, weegt dit niet op tegen de tijd en moeite en zullen ze waarschijnlijk eerder hun aanval staken. Ondanks deze verschuiving blijft het risico op een aanval voor iedereen bestaan.[20] Daarom zijn hier enkele tips om uzelf te beschermen tegen een dergelijke aanval.[21]

- Maak een back-up. Het liefst volgens de 3-2-1 regel. Deze regel stelt dat u ten minste drie kopieën van uw gegevens moet hebben; twee van de back-ups moeten worden opgeslagen op verschillende soorten media, waarvan ten minste één offline of in de Cloud wordt opgeslagen. Zo voorkomt u dat bij een aanval ook de back-up wordt versleuteld.[22]
- Schakel bestandsextententies in. Gijzelsoftware is vaak een uitvoerbaar exe-bestandvermomd als een ander bestand, bijvoorbeeld een pdf-document. Door het inschakelen van bestandsextensies kunt u zien met wat voor bestand u te maken heeft.
- Klik niet zomaar op links en bijlagen in e-mails, tenzij je er zeker van bent dat het vertrouwd is.
- Installeer een goede virusscanner.
- Houd alle software up-to-date. Bijvoorbeeld de internetbrowser, besturingssystemen en browseraanvullingen.

Meldplicht bij aanval

Mocht er sprake zijn van een gijzelsoftware-aanval wordt sterk aangeraden aangifte te doen bij de politie. De politie werkt namelijk samen met internationale partijen, zoals Interpol en het Nationaal Cyber Security Systeem (hierna: NCSC). Heeft de gijzelsoftware gegevens versleuteld die persoonsgegevens bevatten? Dan is er sprake van een datalek. In principe moet een datalek binnen 72 uur na ontdekking worden gemeld bij de AP zoals voorgeschreven in de AVG, tenzij het niet waarschijnlijk is dat deze lek een risico oplevert voor de vrijheden en rechten van betrokkenen, bijvoorbeeld de bescherming van persoonsgegevens en de persoonlijke levenssfeer.[23] Daarnaast moeten de slachtoffers worden geïnformeerd als een datalek een hoog risico voor hen oplevert. Daar is onder andere sprake van wanneer bijzondere persoonsgegevens zijn getroffen door de gijzelsoftware. Deze gegevens hebben een hogere impact op de privacy. Voorbeelden hiervan zijn politieke opvattingen, seksueel gedrag of lidmaatschap van een vakbond.[24]

16 'Grote hackersgroep Lockbit deels opgerold door internationale politie', trouw.nl.

17 'Hackersbende Lockbit keert terug en dreigt met aanvallen met overheidssector', nu.nl.

18 Ministerie van Justitie en Veiligheid, *Maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval*, 30 juni 2020, te raadplegen op: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwie4Pag1f6EAxXa_7sIHVlPC-8QFnoECB4QAQ&url=https%3A%2F%2Fwww.ncsc.nl%2Fbinaries%2Fncsc%2Fdocumenten%2Ffactsheets%2F2020%2Fjuni%2F30%2Ffactsheet-ransomware%2F71059_NCSC_FS%2BRansomeware%2BNL_WEB.pdf&usg=AOvVaw2T1epCt3OCcW1_jusHHLqQ&opi=89978449.

19 'Cybercrime gevaarlijker door AI: 5 trends en 5 tips voor 2024, vodafone.nl.

20 'Verkenning risicofactoren ransomware-aanvallen', wodc.nl.

21 'Bescherm jezelf tegen ransomware met deze 5 tips', kvk.nl.

22 'Maak back-ups', ncsc.nl.

23 Artikel 33 AVG.

24 Artikel 34 AVG.

Naast de meldplicht uit de AVG bestaan er nog meer meldplichten in verschillende sectorale wetgeving, bijvoorbeeld op basis van:

- De Wet financieel toezicht. Deze wet verplicht financiële instellingen bij een incident die betrekking heeft op een van de onderwerpen in de artikelen van deze wet te melden aan de Autoriteit Financiële Markten en/of de Nederlandsche Bank.[25]
- De Telecommunicatiewet. Deze wet verplicht openbare elektronische communicatiediensten bij een incident melding te doen bij de AP,[26] en
- De Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze wet verplicht aanbieders van essentiële digitale dienstverleners en diensten maatregelen te nemen om hun ICT te beveiligen tegen incidenten. Bij ernstige incidenten geldt een meldplicht. Vitale aanbieders moeten daarbij ook de Minister van Justitie en Veiligheid informeren als er sprake is van een cyberincident.[27] Vitale aanbieders bieden een dienst aan waarvan de continuïteit van essentieel belang is voor de Nederlandse samenleving. Een mogelijke manipulatie van deze diensten zal dermate ernstige gevolgen hebben dat deze de nationale veiligheid kunnen schaden. De vitale aanbieders hebben op basis van de wet recht op bijstand van het NCSC. Voorbeelden van vitale aanbieders zijn de drinkwatervoorziening, inzet van politie, vervoer van personen en goederen over (hoofd) spoorweginfrastructuur en de communicatie met en tussen hulpdiensten middels C2000 en middels 112.[28]

Concluderend vormt gijzelsoftware een groeiende dreiging voor zowel individuen als organisaties, met ernstige gevolgen voor de getroffenen. Hoewel er geen garantie is dat betaling daadwerkelijk tot herstel leidt of tot het voorkomen van nieuwe aanvallen, voelen veel bedrijven zich genoodzaakt losgeld te betalen. Onder andere door de dreiging van reputatieschade, omzetverlies en gegevensverlies. Daarbij worden aanvallen steeds geavanceerder en gerichter, met hogere bedragen aan losgeld als doelwit. Deze aanvallen worden uitgevoerd door professionele organisaties, die soms zelfs over een klantenservice beschikken. Maar met de betaling van losgeld en het terugzetten van een back-up ben je er nog niet. Zo moet je forensisch onderzoek laten doen, alles opschonen en vaak helemaal opnieuw opbouwen. Ook in dit geval geldt dan ook weer: beter voorkomen, dan genezen. Het biedt geen 100% garantie, maar zorg in ieder geval voor een goede beveiliging. Met onze tips bent u daar in ieder geval een stuk verder in! En mocht u dit nu een interessant onderwerp vinden, raad ik u van harte aan de documentaire 'ik weet je wachtwoord' te kijken. Daarin spreekt RTL Nieuwsjournalist Daniël Verlaan zelfs met een sleutelfiguur van hackersgroep Lockbit.[29]

Namens de Carrièrecommissie,

Manon Hospers

25 Artikel 3:10 jo. 4:11 Wet op het financieel toezicht.

26 'Zo meldt u een datalek', autoriteitpersoonsgegevens.nl.

27 Artikel 10 Wet beveiliging netwerk- en informatiesystemen.

28 'Vitale aanbieders', nctv.nl.

29 'Documentaire', ikweetjewachtwoord.nl.