Crimineel of slachtoffer?

De dunne scheidslijn bij cybersecurity-incidenten

Nosh van der Voort & Willemijn Warnaars[1]

Deze bijdrage ziet op de vraag of (benadeelde) bedrijven die hun digitale achterdeur open laten staan voor cybercriminelen in de toekomst moeten vrezen om (ook) als dader aangemerkt te worden. Minister Grapperhaus kondigde al aan dat de overheid harder gaat optreden tegen (niet-gereguleerde) bedrijven die hun internetbeveiliging niet op orde hebben. In deze bijdrage wordt ingegaan op de huidige cybersecurity-wetgeving, op de vraag of de theoretische strafrechtelijke handhaving ook in de praktijk werkbaar is en wordt afgerond met enkele beschouwingen voor de toekomst.

1. Inleiding

Cybercriminelen proberen meer en meer munt te slaan uit de disruptie en angst die er heerst wegens de uitbraak van het coronavirus. Er is een significante toename van *phishing* e-mails, waarbij thuiswerkende werknemers wordt gevraagd in te loggen op een webpagina van hun werkgever die hun werkgever helemaal niet blijkt te zijn.[2]

Nog voordat het coronavirus in rap tempo wereldwijd en in Nederland om zich heen greep, was voor het eerst in een lange tijd in Nederland al sprake van een aanzienlijke stijging van cybercriminaliteit, zo blijkt uit de jaarcijfers 2019 die de politie op 15 januari 2020 openbaarde en het CBS op 2 maart 2020 publiceerde op basis van de Veiligheidsmonitor.[3] Deze trendvoortzetting is terug te zien in het begin van het nieuwe jaar. Een greep uit de recente berichtgeving van de media leert ons dat de digitale weerbaarheid van Nederlandse bedrijven op zijn zachtst gezegd niet overal op orde is.[4]

Illustratief is het nieuws dat vele Nederlandse bedrijven en overheidsinstanties (o.a. de Luchtverkeersleiding Nederland, ziekenhuizen en het Ministerie van Justitie en Veiligheid zelf) kwetsbaar waren voor hackers, doordat een update na meerdere waarschuwingen van het Nationaal Cyber Security Center (NCSC) niet werd uitgevoerd om een lek bij VPN-aanbieder *Pulse Secure* te verhelpen. Bovendien was er de nog recentere berichtgeving aangaande de onveilige Citrix-verbindingen[5] hetgeen tot gevolg had dat duizenden Citrix-servers wereldwijd kwetsbaar waren voor een hack.[6] Een *wake up call* voor bedrijven, zou men denken. De werkelijkheid is echter anders.

Een *wake up call* voor bedrijven, zou men denken. De werkelijkheid is echter anders

De genoemde problemen met Citrix waren al bekend sinds 17 december 2019, maar ondanks adviezen van het NCSC en de enorme media-aandacht zijn de waarschuwingen voor dovemans oren bestemd. Zo meldde *NRC Handelsblad* op 4 februari 2020 dat nog zeker zeventig Citrix-servers in Nederland het risico lopen gehackt te worden. Uit de door *NRC Handelsblad* verkregen informatie bleek dat de servers van deze bedrijven nog volledig kwetsbaar

Auteurs

1. Mr. N. van der Voort en mr. W.M. Warnaars zijn beiden werkzaam als advocaat bij Simmons & Simmons Amsterdam op de afdeling Crime, Fraud & Investigations.

Noten

2. S. van Gils, 'Cybercrimineel mikt op corona. Uw kantoor gaat even dicht klik hier om thuis te werken', *Het Financieele Dagblad (FD)* 12 maart 2020.

3. In 2019 is 4.690 keer aangifte gedaan van cybercrime. Dat is een stijging van 64% vergeleken met 2018 (2860 aangiftes). CBS, 'Minder traditionele criminaliteit, meer cybercrime', *CBS.nl*, 2 maart 2020.

4. G. de Groot & E. Engel, 'De Nederlandse kwetsbaarheid voor cybercriminaliteit', *FD* 25 februari 2020; S. van Gils, 'Cybercriminaliteit grijpt om zich heen in Nederland', *FD* 16 januari 2020; W. Heck & R. W. Wassens, 'Nederlandse bedrijven nog kwetsbaar voor hack', *NRC* 15 januari 2020; en V. Sondermeijer 'Ook Tweede Kamer schakelt Citrix-systeem uit', *NRC* 17 januari 2020.

5. Citrix is een softwaresysteem dat (wereldwijd) door veel organisaties wordt gebruikt voor thuiswerken. Door in te loggen in het Citrix-systeem hebben werknemers altijd en overal toegang tot werkgegevens.

6. H. Modderkolk, 'Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open'; *de Volkskrant* 28 september 2019; 'Waarschuwing voor hacks bij Citrix-servers na beveiligingslek', *NOS* 13 januari 2020.

© Shutterstock

waren en de beheerders zelfs geen mitigerende maatregelen hadden toegepast.[7]

In de kern ziet deze bijdrage op de vraag of (benadeelde) bedrijven die hun digitale achterdeur open laten staan voor cybercriminelen in de toekomst moeten vrezen om (ook) als dader aangemerkt te worden. Als het aan Minister Ferdinand Grapperhaus van Justitie en Veiligheid ligt, is het antwoord eenduidig. Op 1 oktober 2019 kondigde hij in het *FD* immers al aan dat de overheid harder gaat optreden tegen (niet-gereguleerde) bedrijven die hun internetbeveiliging niet op orde hebben.[8] Redenen hiervoor (volgens Grapperhaus) zijn onder meer de grote gevolgen van verstoring en sabotage van bedrijven. Deze activiteiten kunnen een (langdurig) ontwrichtend effect hebben op de maatschappij en mogelijk zelfs impact hebben op de nationale veiligheid, zeker wanneer vitale processen en partijen geraakt worden.[9] De genoemde Citrix-problematiek maakte blijkens de op 20 maart 2020 verschenen kabinetsreactie nogmaals duidelijk dat incidenten bij organisaties die niet als vitaal zijn aangemerkt tot overlast of onrust kunnen leiden en dat de noodzaak groot is om aanvullende maatregelen te nemen.[10] Niet voor niets deed de Wetenschappelijke Raad voor het Regeringsbeleid in een eerder stadium (onder meer) de aanbeveling om een helder afgebakende wettelijke bevoegdheid voor digitale hulptroepen te creëren en de noodzaak van een aparte regeling voor overheidshandelen gericht op tegengaan van verdere escalatie te onderzoeken.[11] Het voorgaande in ogenschouw nemende, gaan wij in deze bijdrage in op de huidige cybersecuritywetgeving (par. 2), op de vraag of de theoretische strafrechtelijke handhaving ook in de praktijk werkbaar is (par. 3) en ronden wij af met enkele beschouwingen voor de toekomst.

2. De Wet beveiliging netwerk- en informatiesystemen

Om een ontwrichtend effect op de maatschappij en nationale veiligheid te voorkomen is voor vitale aanbieders[12] en digitaledienstverleners[13] reeds in (oktober) 2018 aanvullende wetgeving in werking getreden: De *Wet beveiliging netwerk- en informatiesystemen* (Wbni).[14] De Wbni is de Nederlandse implementatie van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (de NIB-Richtlijn). De Wbni beoogt de digitale weerbaarheid van Nederland, en in het bijzonder die van vitale aanbieders, digitaledienstverleners en de Rijksoverheid te bevorderen.[15]

De groep vitale aanbieders is onder te verdelen in twee categorieën: aanbieders van een essentiële dienst (AED), zoals de Luchtverkeersleiding Nederland of ziekenhuizen, en andere aangewezen vitale aanbieders (AAVA), zoals telefoonnetbeheerders en Schiphol.[16]

Voor AED's en digitaledienstverleners (hierna tezamen: aanbieders) geldt op grond van de Wbni een zorgplicht en een meldplicht. Uit de Kamerbrief van minister Grapperhaus kan worden afgeleid dat in de toekomst ook de AAVA's onder het volledige regime van de Wbni zullen

worden gebracht en de zorg- en meldplicht aldus ook voor hen geldt.[17] De zorgplicht is geregeld in de artikel 7 en 8 Wbni en valt uiteen in een tweetal verplichtingen:

- Artikel 7 Wbni verplicht de aanbieders om passende en evenredige maatregelen te nemen om beveiligingsrisico's van hun ICT-systemen te beheersen. Deze maatregelen hebben in ieder geval betrekking op de beveiliging van systemen en voorzieningen, de behandeling van incidenten, beheer van de bedrijfscontinuïteit, op toezicht (*monitoring*), controle (*auditing*) en testen, en op inachtneming van de internationale normen.[18]
- Artikel 8 Wbni bevat de verplichting voor de aanbieders om passende maatregelen te nemen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken om zo de continuïteit van de dienst te waarborgen.

Naar aanleiding van de Citrix-problematiek is een ontwerp-wijziging van het Bbni in procedure.[19] Blijkens de conceptwijziging is ter nadere invulling van de zorgplicht opgenomen dat aanbieders voor wat betreft beveiligingsadviezen van relevante instanties, zoals het NCSC, moeten beoordelen of aanvullende beveiligingsmaatregelen nodig zijn om de risico's te reduceren. Tevens zal een *'pas toe of leg uit'*-beleid gaan gelden, hetgeen impliceert dat vitale aanbieders bij dringende adviezen van het NSCS uitleg moeten geven aan een toezichthouder of een andere geschikte aangewezen partij wanneer zij deze beveiligingsadviezen niet opvolgen.[20]

De passende en evenredige maatregelen dienen ertoe dat de netwerk- en informatiesystemen van de aanbieders zijn opgewassen tegen acties die de digitale veiligheid van de opgeslagen gegevens, of de daaraan gerelateerde diensten die via die systemen worden aangeboden of toegankelijk zijn, in gevaar brengen.[21]

Indien zich desalniettemin een cyberincident voordoet, is een aanbieder op grond van de Wbni verplicht om dit te melden. Een incident wordt in de NIB-richtlijn gedefinieerd als *'elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen'*.[22] Niet ieder incident hoeft gemeld te worden; er moet sprake zijn van een incident met aanzienlijke gevolgen. Er gelden drempelwaarden om te bepalen of hiervan sprake is en of het incident aldus gemeld moet worden.[23] Zo dient een incident gemeld te worden als de dienst in de Europese Unie (EU) meer dan 5.000.000 gebruikersuren niet beschikbaar was.[24] Een ander voorbeeld is dat het incident voor meer dan 100.000 gebruikers binnen de EU negatieve gevolgen moet hebben gehad.[25]

Als deze drempels zijn genomen, dienen de aanbieders het incident bij verschillende instanties te melden. Door het wijd verspreide toezichtsveld ontbreekt een centrale instantie. Zo zijn de digitaledienstverleners verplicht om incidenten te melden bij het betreffende *Computer Security Incident Response Team* (CSIRT) alsmede bij de daartoe bevoegde autoriteit.[26] AED's zijn verplicht om incidenten te melden bij het NCSC en bij de daartoe bevoegde autoriteit. De AAVA's melden daarentegen alleen bij de Minister van Justitie en Veiligheid. Tijdens de Citrix-problematiek werd duidelijk dat er nog veel sectoren zijn die niet over een eigen computercrisisteam of samenwerkingsverband beschikken. Minister Grapperhaus meent dat uiteindelijk elk bedrijf en elke organisa-

Tijdens de Citrix-problematiek werd duidelijk dat er nog veel sectoren zijn die niet over een eigen computercrisisteam of samenwerkingsverband beschikken

7. R. Wassens 'Nog zeventig Nederlandse Citrix-systemen kwetsbaar', *NRC Handelsblad* 4 februari 2020. Het is mogelijk dat deze bedrijven op het moment van publicatie van deze bijdrage inmiddels wel mitigerende maatregelen hebben toegepast.
8. S. Olsthoorn & U. Jonker, 'Justitie wil ingrijpen bij bedrijven die digitale beveiliging niet op orde hebben', *FD* 1 oktober 2019.
9. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2019*, Den Haag: juni 2019, p. 16.
10. *Kamerstukken II* 2019/20, 26643, 673 (Kamerbrief), p. 2-3.
11. Wetenschappelijke Raad voor het Regeringsbeleid, *Voorbereiden op digitale ontwrichting,* WRR-Rapport 101, Den Haag: WRR 2019, p. 90.
12. Vitale aanbieders zijn overheidsorganisaties of privaatrechtelijke rechtspersonen die diensten aanbieden waarvan de continuïteit, volgens de Nederlandse overheid, van vitaal belang is voor de Nederlandse samenleving. Te denken valt aan energiebedrijven, drinkwaterbedrijven en banken.
13. Digitaledienstverleners zijn aanbieders van clouddiensten, online zoekmachines en online marktplaatsen. Als een organisatie een van deze digitale diensten verleent, geldt de Wbni nog niet automatisch. De wet is namelijk niet van toepassing op micro- of kleine ondernemingen, maar alleen op (middel)grote ondernemingen.
14. Wet houdende regels ter implementatie van Richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen), *Stb*. 2018, 387.
15. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2019*, Den Haag: juni 2019.
16. In het Besluit beveiliging netwerk- en informatiesystemen (Bbni) staat vermeld welke bestuursorganen een AED zijn en welke een AAVA.
17. *Kamerstukken II* 2019/20, 26643, 673 (Kamerbrief), p. 9.
18. Deze maatregelen zijn verder uitgewerkt in art. 2 Uitvoeringsverordening (EU) 2018/151.
19. De internetconsultatie is op 6 maart 2020 gesloten.
20. Zie *Kamerstukken II* 2019/20, 26643, 673 (Kamerbrief), p. 4-5.
21. Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners, *rijksoverheid.nl*, 1 september 2018, www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk-en-informatiesystemen-wbni-voordigitale-dienstverleners; Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2019*, Den Haag: juni 2019.
22. Art. 5 lid 7 Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.
23. De drempelwaarden zijn opgenomen in een Uitvoeringsverordening (EU) 2018/151 en gelden zodoende in alle EU-lidstaten.
24. Onder gebruikersuren wordt verstaan: 'het aantal gebruikers in de Europese Unie x het aantal uren dat de digitale dienst niet beschikbaar is'.
25. Zie voor de criteria art. 14 Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.
26. Agentschap Telecom houdt in Nederland toezicht op de AED's die vallen onder het Ministerie van Economische Zaken en Klimaat en de aangewezen digitaledienstverleners. De Inspectie voor de Leefomgeving en Transport doet dit voor de onder het Ministerie van Infrastructuur en Water vallende AED's.

tie ergens terecht moet kunnen voor informatie en advies. Volgens hem moeten de computercrisisteams en samenwerkingsverbanden in beginsel worden opgericht door de sectoren zelf, alhoewel de verantwoordelijke vakministers een belangrijke rol spelen bij het aanjagen en faciliteren hiervan. Daarnaast zal het aantal organisaties dat wordt aangewezen als computercrisisteam of koepelorganisatie om andere organisaties of het publiek over dreigingen te informeren verder worden uitgebreid. Hierdoor kan het NCSC bepaalde vertrouwelijke informatie aan die aangewezen organisaties verstrekken, met als gevolg dat de beveiligingsadviezen alle organisaties bereiken.

Tevens bleek dat de organisaties niet altijd wisten wat de verschillende verantwoordelijkheden binnen het stelsel zijn. Grapperhaus kondigde daarom aan dat een handreiking LDS (landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden) wordt opgesteld, waarin wordt ingegaan op de verschillende rollen binnen het stelsel en de verantwoordelijkheid van het NCSC en de sectorale cybersecurityorganisaties bij het doorgeleiden van beveiligingsadviezen. Tussen krachtens de Wbni aangewezen cybersecurityorganisaties en het NCSC worden hierover aanvullende afspraken gemaakt.[27]

Dat er overigens (in de praktijk) een aantal hordes te nemen is voordat de aanbieders daadwerkelijk wettelijk verplicht zijn tot het doen van een melding, blijkt wel uit de rapportage *Cybersecuritybeeld Nederland 2019*: in de periode mei 2018 tot en met januari 2019 is immers slechts één melding gedaan door een organisatie uit een vitale sector.[28]

Mochten de toezichthoudende diensten besluiten om ten aanzien van de aanbieders over te gaan tot handhaving, dan kunnen zij op grond van de Wbni gebruikmaken van een viertal bevoegdheden.[29] Indien een aanbieder haar wettelijke zorgplicht schendt, kan haar een *beveiligingsaudit*[30] (artikel 26 Wbni) opgelegd worden, alsmede een *bindende aanwijzing*[31] (artikel 27 Wbni) worden gegeven. Tevens bestaat voor de toezichthoudende diensten de mogelijkheid om een last onder bestuursdwang of een last onder dwangsom op te leggen. Tot slot biedt de Wbni de mogelijkheid om een bestuurlijke boete op te leggen. Afhankelijk van de soort overtreding kan deze boete oplopen tot een bedrag van maximaal een of vijf miljoen euro.

Bij het schrijven van dit artikel voorziet de Nederlandse wet- en regelgeving vooralsnog niet in een (laagdrempelige) mogelijkheid (voor de overheid) om bij de aanbieders en andere bedrijven te controleren of zij hun beveiliging op orde hebben en om eventueel in te grijpen. Grapperhaus meldde onlangs dat het kabinet zich voorbereidt op digitale incidenten en dat de wettelijke bevoegdheden van de overheid bij digitale crisissituaties in kaart worden gebracht, zodat bezien kan worden waar eventuele aanvullingen nodig zijn.[32] Overigens dient nogmaals benadrukt te worden dat bovengenoemd kader enkel en alleen van toepassing is op vitale aanbieders en digitaledienstverleners. Ontspringen andere (niet-gereguleerde) bedrijven hierdoor de dans?[33]

Ontspringen andere (niet-gereguleerde) bedrijven hierdoor de dans?

3. Strafrechtelijke handhaving?

In theorie dient het antwoord hierop ontkennend te luiden. In artikel 350b Wetboek van Strafrecht (Sr) is de vangnetbepaling opgenomen die kort gezegd vernieling of onbruikbaar maken van computergegevens door schuld strafbaar stelt.[34] Bij de strafrechtelijke term 'schuld' moet men denken aan verwijtbare nalatigheid, onachtzaamheid, onvoorzichtigheid, onoplettendheid, e.d.[35] Dit artikel beschermt het ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens.[36] In tegenstelling tot de Wbni geldt deze strafbepaling voor alle organisaties (en individuen) die te maken hebben met de beveiliging van netwerk- of informatiesystemen. In het bijzonder geldt dit dus ook voor bedrijven die – ondanks de beschikbaarheid van beveiligingsmaatregelen – hun ICT-beveiligingssystemen niet op orde hebben, zoals dit bij het Citrix-lek het geval was.

Zo meldde het Nederlands Security Meldpunt op 3 februari 2020 dat nog ruim 8000 Citrix-systemen kwetsbaar zijn voor aanvallen.[37] De Nederlandse privacy waakhond Autoriteit Persoonsgegevens heeft over deze concrete kwestie laten weten dat (slechts) negenentwintig organisaties tot nu toe een melding hebben gemaakt van eventuele datalekken die door de beveiligingslekken in de Citrix-systemen zijn veroorzaakt.[38] De vraag is of bedrijven die waarschuwingen over kwetsbaarheden in IT-systemen in de wind slaan door niet, niet tijdig of niet behoorlijk de beveiliging van hun systemen op orde te brengen, strafrechtelijk kunnen worden aangepakt wegens toerekenbare, verwijtbare nalatigheid. In dat kader lijkt op het eerste gezicht vervolging via artikel 350b Sr daarvoor in aanmerking te komen.

Artikel 350b lid 1 Sr vereist dat sprake moet zijn van i) gegevens die middels een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, ii) deze gegevens moeten zijn veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, of waaraan andere gegevens zijn toegevoegd, iii) die handeling moet wederrechtelijk zijn gebeurd, iv) waardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt en v) dit te wijten is aan de schuld van de dader.

Hoewel voor strafbaarheid op grond van het eerste lid een dubbel causaal verband is vereist,[39] lijken de eerste drie voorwaarden geen al te hoge juridische drempels te vormen voor een bewezenverklaring. Het open laten staan van het netwerk waardoor een cybercrimineel binnendringt in het computersysteem zal immers als gevolg hebben dat elektronische gegevens die zijn opgeslagen op (een reeks van) computers of netwerken (voorwaarde 1)[40] worden veranderd of gewist etc. (voorwaarde 2), terwijl daarvoor geen toestemming is verkregen (voorwaarde 3).

Verder is vereist dat door het veranderen, wissen, etc., van de gegevens ernstige schade is veroorzaakt (voorwaarde 4). Ingevolge jurisprudentie van de Hoge Raad is van 'ernstige schade' sprake wanneer het functioneren van het

informatiesysteem gedurende geruime tijd geheel of nagenoeg geheel is uitgesloten, waarbij 'geruime tijd' duidt op enige uren.[41] Het plaatsen van gijzelsoftware (*ransomware*) heeft als gevolg dat een computer wordt geblokkeerd of bestanden worden versleuteld en dat deze weer bruikbaar zijn op het moment dat losgeld is betaald. Ter illustratie kan gewezen worden op de Universiteit van Maastricht, die in februari 2020 bijna € 200.000 aan losgeld betaalde om de gehackte universitaire computersystemen weer toegankelijk te krijgen. Het is bovendien een feit van algemene bekendheid dat aan computersystemen grote schade kan worden toegebracht als gevolg van handelingen van zogenoemde 'hackers'.[42] Zodoende zal de vierde voorwaarde eveneens bewijstechnisch geen probleem vormen.

Blijkens de wetsgeschiedenis is voor het bestanddeel 'schuld' grove schuld (*culpa lata*) vereist.[43] Gelet op vaste jurisprudentie moet aldus sprake zijn van een 'verwijtbare aanmerkelijke onvoorzichtigheid': de dader moest onder bepaalde omstandigheden anders handelen (dit kan tevens nalaten zijn) én kon ook anders handelen.[44] Met andere woorden: er is sprake van grove schuld indien de systeembeheerder van een bedrijf zich de schade die de cybercriminelen aan het kantoorsysteem kunnen aanbrengen niet (afdoende) realiseert, maar hij hieraan – gezien het aantal waarschuwingen – redelijkerwijs had moeten denken en om die reden wél de beschikbare update had moeten uitvoeren.

Het niet opvolgen van de door de Cyber Security Raad opgestelde *Best Practices*-handreiking kan hierbij handvatten bieden en mogelijk een opmaat zijn voor het kunnen vaststellen van deze 'grove schuld' ex artikel 350b Sr. Deze handreiking geeft een overzicht van de belangrijkste juridische zorgplichten op het gebied van cybersecurity voor (niet-gereguleerde) bedrijven en geeft handvatten om deze plichten in te vullen. De handreiking is beknopt, op hoofdlijnen en niet sectorspecifiek.[45]

Naast de systeembeheerder is het tevens denkbaar dat (de feitelijke leidinggever van) het bedrijf strafrechtelijk aansprakelijk kan worden gesteld. Op grond van artikel 51 Sr kan immers ook (de leiding van) een rechtspersoon een strafbaar feit begaan. Het bedrijf dat besluit om de oproep te negeren om een update uit te voeren en op die manier zijn digitale deuren openhoudt voor cybercriminelen, waardoor het ICT-systeem bijvoorbeeld als gevolg van een ingebracht computervirus (tijdelijk) ontoegankelijk is, handelt – indien overigens aan de door de Hoge Raad gestelde eisen voor redelijke toerekening om te komen tot daderschap van rechtspersonen, zoals neergelegd in het zogeheten *Drijfmest*-arrest,[46] is voldaan – in strijd met artikel 350b Sr. Aan die strafbare gedraging van de rechtspersoon kunnen vervolgens verantwoordelijke managers en bestuurders strafbaar feitelijk leiding hebben gegeven.

Het tweede lid van artikel 350b Sr stelt culpose *malware*-verspreiding strafbaar. Indien het aan iemands schuld te wijten is dat gegevens wederrechtelijk ter beschikking worden gesteld of worden verspreid die zijn bestemd om schade aan te richten in een geautomatiseerd werk, is diegene eveneens mogelijk strafbaar. Hoewel enige tijd geleden binnen de literatuur onduidelijkheid bestond over de vraag of de wetgever met dit tweede lid bedoeld heeft beveiligingsmaatregelen af te dwingen,[47] zijn wij van mening dat het – gezien de groeiende kwetsbaarheid van de samenleving voor digitale verstoringen en het daarmee gepaard gaande ontwrichtende effect – niet anders kan dan dat het niet naleven van de beveiligingsplicht als culpoos (en soms, bij het bestaan van voorwaardelijk opzet in de zin van het welbewust aanvaarden van de kwade kans, doleus)[48] delict moet worden beschouwd. Met andere woorden: als het aan de schuld van het bedrijf te wijten is dat zijn computersystemen geïnfecteerd raken met *malware* en zodoende de privacygevoelige persoonsgegevens openbaar worden

27. *Kamerstukken II* 2019/20, 26643, 673 (Kamerbrief), p. 3.

28. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2019*, Den Haag: juni 2019, p. 29.

29. Hoofdstuk 6 van de Wbni is niet van toepassing op AAVA's.

30. Dit impliceert dat een externe deskundige onderzoekt (en rapporteert aan de betrokken toezichthouder) of de genomen maatregelen voldoen aan de eisen zoals genoemd in art. 7 en 8 Wbni, waarbij de aanbieder in principe de kosten draagt van dit onderzoek.

31. Deze aanwijzing verplicht het bedrijf om binnen een daarbij te stellen redelijke termijn de voorgeschreven maatregelen te nemen.

32. *Kamerstukken II* 2019/20, 26643, 673 (Kamerbrief), p. 5.

33. Deze bijdrage bespreekt enkel de handhavingsmogelijkheden ten aanzien van niet-gereguleerde bedrijven. Zorginstellingen, financiële instellingen en andere gereguleerde bedrijven hebben hun eigen regelgevingskader inzake informatiebeveiliging. Zie o.a. De Nederlandsche Bank, '*Good Practice informatiebeveiliging 2019/2020*', te raadplegen via: www.toezicht.dnb.nl/5/50-237689.jsp.

34. Art. 350b Sr bevat de culpose variant van art. 350a Sr (opzettelijke gegevensbeschadiging). De laatste wetswijziging geschiedde bij de Wet computercriminaliteit II van 1 juni 2006, *Stb.* 2006, 300 (i.w.tr. op 1 september 2006).

35. *Smidt I*, p. 83-84.

36. *Kamerstukken II* 1989/90, 21551, 3, p. 23.

37. 'Nog ruim 8.000 Citrix-systemen kwetsbaar voor aanvallen', *Security.nl* 3 februari 2020.

38. D. Metselaar, '29 mogelijke datalekken gemeld na hackpoging Citrix-software', *NRC Handelsblad* 22 januari 2020.

39. Ten eerste moeten de elektronische gegevens zijn veranderd, gewist, etc. door de gedraging (doen of nalaten) van de dader en ten tweede moet door het veranderen, wissen, etc., van de gegevens ernstige schade met betrekking tot die gegevens zijn veroorzaakt. Indien de (culpose) gedraging van de dader zelf bestaat uit het veranderen, wissen, etc., van gegevens, hoeft niet afzonderlijk het eerstgenoemde causaal verband te worden vastgesteld.

40. Blijkens vaste jurisprudentie van de Hoge Raad dienen onder het begrip 'geautomatiseerd werk ook computers en netwerken van aan elkaar verbonden computers te worden begrepen. Zie bijv. HR 22 februari 2011, ECLI:NL:HR:2011:BN9287.

41. HR 19 januari 1999, ECLI:NL:HR:1999:ZD1308, *NJ* 1999/251. In deze zaak was sprake van ernstige schade, nu het binnengedrongen computersysteem ongeveer twaalf uur ontoegankelijk was.

42. Hof 's-Hertogenbosch 5 augustus 2008, ECLI:NL:GHSHE:2008:BE9060.

43. *Smidt I*, p. 83-84.

44. Zie bijv. HR 17 september 2002, ECLI:NL:HR:2002:AE4201, *NJ* 2002/549 en HR 29 juni 2010, ECLI:NL:HR:2010:BL5630, *NJ* 2010/674, m.nt. Mevis. Zie voor de geschiedenis van *culpa lata* de conclusie van A-G Vellinga bij het arrest van de Hoge Raad *NJ* 2008/440.

45. P. Wolters & C. Jansen, 'Ieder bedrijf heeft zijn eigen zorgplichten. Een handreiking voor bedrijven op het gebied van Cybersecurity', *Cyber Security Raad* 2017.

46. HR 21 oktober 2003, ECLI:NL:HR:2003:AF7938, *NJ* 2006/328, m.nt. Mevis (*Drijfmest*).

47. Zo menen Chr.H. van Dijk & J.M.J. Keltjens, *Computercriminaliteit*, Zwolle: W.E.J. Tjeenk Willink 1995, p. 176-177 dat in art. 350b Sr geen algemene beveiligingsplicht mag worden ingelezen. H. Franken, H.W.K. Kaspersen & A.H. de Wild, *Recht en Computer* (Recht en Praktijk; nr. 36). Deventer: Kluwer 2001, p. 401 en 412, bepleiten van wel.

48. Zoals strafbaar is gesteld in art. 350a Sr.

gemaakt, heeft het bedrijf zich in beginsel schuldig gemaakt aan artikel 350b lid 2 Sr. Daarnaast kunnen de systeembeheerder of de leiding van de onderneming via daderschaps- en deelnemingsvormen daar eveneens strafrechtelijk voor aansprakelijk worden gesteld.

De rechtspersoon of voornoemde systeembeheerder riskeert na een geslaagde vervolging op grond van artikel 350b Sr een maximale geldboete van € 4350 respectievelijk één maand gevangenisstraf. Deze sanctie zal het gewenste effect niet sorteren. Het primaire doel van de aangekondigde aanpak van minister Grapperhaus is immers zorgen dat bedrijven de cybersecurity op orde brengen. Toch kan dit in de praktijk mogelijkerwijs bereikt worden door het gebruik van de transactie, de belangrijkste rechtsfiguur in de huidige Nederlandse schikkingspraktijk. Deze buitengerechtelijke modaliteit is neergelegd in artikel 74 lid 1 Sr waarin wordt bepaald dat de officier van justitie voor aanvang van de terechtzitting door het stellen van één of meer voorwaarden voor overtredingen en misdrijven met een gevangenisstraf van maximaal zes jaren, strafvervolging van de verdachte kan voorkomen. Gedragsaanwijzingen of -voorwaarden kunnen niet bij een transactie worden opgelegd door het Openbaar Ministerie, maar de afgelopen jaren is echter een trend te ontdekken die inhoudt dat een 'compliance voorwaarde' of een verbeterplan onderdeel van de door het Openbaar Ministerie aangeboden schikking kan zijn.[49] Het lijkt er aldus op dat in de huidige Nederlandse schikkingspraktijk wel degelijk compliance-gerelateerde afspraken onderdeel uitmaken van transactieovereenkomsten tussen een verdachte rechtspersoon en het Openbaar Ministerie. De relatief lage sanctie voor overtreding van artikel 350b Sr kan op deze manier een 'haakje' bieden voor het Openbaar Ministerie om in een schikking een aanvullende voorwaarde te stellen van als het ware een *cybermonitor*. Het instellen van een dergelijke verplichting waarin een onderneming een deugdelijk cybersecurityprogramma dient te incorporeren als voorwaarde van een schikking met het Openbaar Ministerie, kan in deze kwesties uitkomst bieden.

4. Afrondende beschouwingen

Dat cybercriminaliteit zich blijft ontwikkelen staat buiten kijf. Criminelen anticiperen op nieuwe technologische ontwikkelingen en het plegen van digitale misdrijven wordt eenvoudiger door *cybercrime-as-a-service*. Criminelen die niet de kennis of resources hebben om hun activiteiten te ondersteunen, kunnen tegenwoordig zelfs cybercrime-producten en -diensten aanschaffen. Op die manier kunnen actoren met relatief weinig ICT-kennis voor een cyberaanval diensten inkopen op criminele platforms, veelal te vinden op het *dark web*. Op deze manier wordt het begaan van een *cyberdelict* eenvoudiger door de laagdrempelige en gebruiksvriendelijke manier waarop deze diensten worden aangeboden. Hiertegenover staat het lucratieve karakter van cybercriminaliteit, in de vorm van het eisen van losgeld na het succesvol plaatsen van *ransomware*.

Door deze ontwikkelingen en toenemende complexiteit van het ICT-landschap in de digitale maatschappij komt de weerbaarheid van bedrijven steeds verder onder druk te staan, als zij niet meelopen met de technologische ontwikkelingen op ICT-gebied en niet tijdig iets doen aan gesignaleerde kwetsbaarheden in hun systemen. Wettelijke maatregelen, zoals de Wbni voor aparte groepen van bedrijven, benadrukken het belang voor organisaties om de weerbaarheid te verhogen. Maar zijn niet-gereguleerde bedrijven zich wel voldoende bewust van deze zorgplicht en mogelijke risico's die zij dragen? Worden bedrijven naast slachtoffer ook (onbedoeld) dader van cyberdelicten als zij aantoonbaar laks en nalatig zijn geweest in het op een adequaat niveau brengen van hun ICT-beveiliging? Naast de eigen verantwoordelijkheid van bedrijven ligt er een rol in het verschiet voor de overheid in de strijd tegen cybercriminaliteit. Is de aanval de beste verdediging? De in 2019 in werking getreden hackbevoegdheid voor opsporingsdiensten kan mogelijk een doeltreffend wapen zijn. De effecten van de aangekondigde aanpak zullen in de komende jaren zichtbaar moeten worden.

Ondanks deze mogelijkheid van het grijpen naar het strafrecht, dient men desalniettemin voor ogen te houden dat dit een *ultimum remedium* is

Bovendien kijken wij uit naar het vervolg op de vermanende woorden '*Als je het zelf niet regelt dan komen wij het wel doen*' van minister Grapperhaus. De geopperde mogelijkheid tot het opleggen van boetes is voor justitie (in theorie) al mogelijk. De vraag is echter of de maximale op te leggen geldboete van € 4350 een voldoende stok achter de (digitale) deur is om bedrijven te waarschuwen voor het nakomen van hun zorgplicht. De vraag stellen, is hem beantwoorden: hier ligt mogelijk een rol voor de wetgever in de modernisering van het Wetboek van Strafrecht in het verschiet. De praktische uitvoering van de handhaving zou echter nu al gevonden kunnen worden in een combinatie van vervolging voor het misdrijf van artikel 350b Sr en de buitengerechtelijke afdoening daarvan door middel van een transactie ex artikel 74 Sr. Hoewel gedragsaanwijzingen of -voorwaarden in beginsel niet bij een transactie kunnen worden opgelegd, maakt in de Nederlandse schikkingspraktijk bij financieel-economische strafzaken een 'compliance voorwaarde' of een verbeterplan de afgelopen jaren echter vaak onderdeel uit van de transactieovereenkomst. In navolging daarvan kan het incorporeren van een deugdelijk cybersecurityprogramma als voorwaarde van een schikking met het Openbaar Ministerie, in deze gevallen uitkomst bieden.

Ondanks deze mogelijkheid van het grijpen naar het strafrecht, dient men desalniettemin voor ogen te houden dat dit een *ultimum remedium* is. Draconisch of noodzakelijk? De tijd zal het leren. '*Veni Vidi Virus...*' •

49. N. van der Voort, 'Geschikt, maar afgekeurd', *website voor Bijzonder Strafrecht*, 14 februari 2019, te raadplegen via: www.bijzonderstrafrecht.nl/home/column-geschikt-maar-afgekeurd.