Simmons & Simmons LLP
PO Box 79023 1070 NB
Claude Debussylaan 247
1082 MC Amsterdam
The Netherlands

Consultatiedocument met betrekking tot het voorstel van de Wet bevordering digitale weerbaarheid bedrijven (8 juni 2021)

(Geschikt voor publicatie)

Van:

[redacted]

[redacted]

(Advocaten, Simmons & Simmons LLP te Amsterdam)

Aan:

De minister van Economische Zaken en Klimaat

Datum: 22 augustus 2021

Excellentie,

1. Inleiding

Deze reactie in het kader van de internetconsultatie geven wij vanuit het perspectief van de rechtspraktijk, meer in het bijzonder de rechtsbescherming.

Eerder deze maand zeiden drie directeuren van Nederlandse IT-beveiligers in De Volkskrant dat de snelle stijging van het aantal cyberaanvallen met ransomware zich ontwikkelt tot 'een nationale ramp'[1]. De drie pleitten voor een actievere houding van de overheid en in hun visie zouden

[1] Vooraanstaande ict-beveiligers: 'Ransomware gaat richting nationale crisis, overheid moet meer doen' | De Volkskrant, 4 augustus 2021.

overheidsdiensten veel meer informatie moeten uitwisselen en delen met andere partijen. Het onderhavig wetsvoorstel, dat ziet op het niet-vitale bedrijfsleven en bedrijven die geen digitaledienstverleners zijn als bedoeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni), beantwoordt naar onze mening aan die oproep en voorziet in het invullen van een wettelijke leemte. Het meest sprekende voorbeeld van die leemte was wel de hack in de VPN-software van Pulse Secure in 2020. Het NCSC wist volgens het Financieele Dagblad (FD) dat een groot aantal Nederlandse bedrijven na deze hack nog kwetsbaar was en zelfs was gehackt, maar deed jegens de desbetreffende niet-vitale bedrijven wegens de juridische mogelijkheden en het wettelijk mandaat niets met de voorhanden zijnde informatie[2].

Mede tegen deze achtergrond onderschrijven wij de doelstellingen van het wetsvoorstel en in beginsel ook de wijze waarop de versterking van de digitale weerbaarheid van bedrijven moet worden bereikt, onder andere door het stelsel van (overheids)organisaties met een rol in de digitale weerbaarheid van Nederland verder te bevorderen.

2. Zorgplichten van overheid en bedrijfsleven

Wij zien het voorliggende wetsvoorstel ook als een wijze van invulling van de zorgplichten die de overheid heeft, bijvoorbeeld ten aanzien van de bewoonbaarheid van ons land (als bedoeld in art. 21 Grondwet) en met betrekking tot bepaalde grondrechten (zoals die van de bescherming van de persoonlijke levenssfeer en het bieden van veiligheid). De Memorie van Toelichting (MvT) maakt expliciet melding van de verwachting dat de nieuwe wet de Minister van EZK het bedrijfsleven beter kan voorzien van praktische handvatten waarmee deels invulling kan worden gegeven door bedrijven aan de passende technische en organisatorische maatregelen als bedoeld in artikel 32 van de Algemene Verordening Gegevensbescherming (AVG). In zoverre zien wij in het wetsvoorstel een voor de praktijk nuttig instrument dat mede ter invulling kan dienen van deze (cyber security-)zorgplicht die bedrijven in het kader van de AVG hebben.

Volgens de MvT zijn bedrijven zelf wel primair verantwoordelijk als het gaat om het treffen van maatregelen aangaande de beveiliging van hun systemen. Wij zien in deze passage een implicatie voor de zorgplicht van bedrijven die verder gaat dan alleen het privacy-domein.

'Ieder bedrijf heeft digitale zorgplichten', zo luidde een Handreiking van de Cyber Security Raad (CSR) in 2017[3]. Daarin werd, naast zorgplichten op grond van de verwerking van persoonsgegevens, ook aandacht gevraagd voor zorgplichten op grond van het gebruik van ICT en die, in verband met producten of diensten met een ICT-toepassing. Aan zorgplichten komt ook in het cyber-domein een steeds groter wordende betekenis toe, getuige bijvoorbeeld het feit dat de CSR de zorgplicht van leveranciers voor veilige producten en dienst voor burgers, bedrijfsleven en overheid in zijn adviesrapport uit april 2021 als een van de vijf speerpunten heeft aangemerkt[4].

Los van het civiele recht, zou de voorgestelde wet in onze ogen ook betekenis kunnen krijgen voor het strafrecht. Ofschoon de MvT stelt dat er geen direct toezicht en handhaving op basis van dit

---

[2] Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden (fd.nl), 17 augustus 2020.
[3] Handreiking+'Ieder+bedrijf+heeft+digitale+zorgplichten',+een+handreiking+voor+bedrijven+op+het+gebied+van+cybersecurity.pdf
[4] CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' | Rapport | Cyber Security Raad, 6 april 2021, p. 49 e.v. De Raad betrekt daarbij ook Europese regelgeving.

wetsvoorstel is voorzien, menen wij dat er wel indirect gevolgen voor toepassing van het strafrecht in het verschiet liggen.

Volgens de MvT ontstaat geen verplichting voor bedrijven in Nederland om gebruik te maken van de informatie van het ministerie van EZK (paragraaf 4). Voorts wordt benadrukt dat ondernemen risico's afwegen en risico's nemen is, zodat bedrijven, behoudens wettelijke kaders, autonoom zijn om beslissingen te nemen over hun bedrijfsvoering (paragaaf 6). In de situatie dat een bedrijf op de voet van het voorgestelde artikel 2, eerste lid, onder c (objectieve) informatie aangereikt krijgt op basis waarvan het zelf kan beoordelen of en in welke mate het maatregelen moet treffen ter mitigatie van een kwetsbaarheid of ter afwering van een dreiging en het bedrijf doet niets of handelt niet adequaat en wordt door cybercriminelen aangevallen, dan zou in onze visie hiermee een omstandigheid gecreëerd kunnen zijn die als grove schuld (nalatigheid, onvoorzichtigheid, roekeloosheid, etc.) kan kwalificeren in de zin van het misdrijf van artikel 350b Sr. Deze strafbepaling ziet op de situatie waarin het aan iemands schuld te wijten is dat wederrechtelijk – kort gezegd – computergegevens (o.a.) worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt en daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt.

Voor zover ons bekend, heeft het Openbaar Ministerie nog geen personen of bedrijven vervolgd op grond van dit wetsartikel uit het Wetboek van strafrecht. De uitwerking van de onderhavige nieuwe wet, in concreto dus het delen van specifieke informatie door het Digital Trust Center (DTC) met een bedrijf, zou na een cyberaanval van dat bedrijf evenwel een bijdrage kunnen leveren aan of de aanleiding kunnen zijn voor strafrechtelijk onderzoek jegens dat bedrijf als vermoedens van (grove) nalatigheid rijzen.[5]

3. Het omgaan met 'vertrouwelijke' gegevens

In het voorstel is voorzien hoe de minister om moet gaan met vertrouwelijke gegevens die verstrekt zouden kunnen worden (artikel 4). Bij artikel 1, 'Begripsbepalingen' is echter geen definitie opgenomen van wat onder 'vertrouwelijke gegevens' moet worden verstaan. In de artikelsgewijze toelichting van de MvT worden echter wel voorbeelden gegeven van vertrouwelijke gegevens met betrekking tot bedrijven: 'gegevens over de identiteit van een bij een incident betrokken bedrijf of specifieke gegevens over de beveiliging van een elektronisch informatiesysteem van een bedrijf.' Veel concreter wordt het niet.

Gelet op het feit dat het voldoen aan een verzoek om informatie niet leidt tot een wettelijke verplichting tot medewerking (zie de artikelsgewijze toelichting bij artikel 3), lijkt het ons raadzaam als aan de definitie van het begrip 'vertrouwelijke gegevens' meer aandacht wordt besteed. Dat is naar onze mening ook dienstig als gelet wordt op het legaliteitsbeginsel.

Het voorgestelde artikel 4, lid 1, letters a en b, bepalen nu dat de minister geen verkregen vertrouwelijke gegevens met betrekking tot een bedrijf verstrekt, als de geheimhouding van die gegevens onvoldoende is gewaarborgd of onvoldoende is gewaarborgd dat zij uitsluitend worden

[5] In de VS werden onlangs de CISO, de voormalige CEO van het gehackte Solar Winds en het bedrijf zelf door boze aandeelhouders aangeklaagd. In de aanklacht wordt onder meer gesteld dat SolarWinds al was gewaarschuwd voor onveilige zaken in zijn IT-infrastructuur (zie: CISO van SolarWinds aangeklaagd - AG Connect, 16 augustus 2021). Naast strafrechtelijke acties, kunnen in ons land ook dit soort civielrechtelijke acties wegens gestelde grove nalatigheid ontstaan, die mede gebaseerd kunnen worden op de informatieverschaffing door het DTC aan het desbetreffende gehackte of aangevallen bedrijf.

gebruikt voor het doel waarvoor zij worden verstrekt. Hoe dit in de praktijk gestalte of inhoud wordt gegeven, is ons niet duidelijk geworden.

Ook vanuit het oogpunt van effectiviteit van wetgeving lijkt het ons raadzaam indien over de zojuist besproken vragen verder wordt nagedacht en een adequate regeling wordt getroffen. Ter versterking van de digitale weerbaarheid van bedrijven in ons land met deze wet is immers voor het niet-vitale bedrijfsleven een belangrijke rol weggelegd. De doelgroep van deze wet, die in een leemte voorziet, moet niet worden afgeschrikt door onduidelijke regelgeving.

4. Afronding

Wij vinden het voorliggende wetsvoorstel een interessante ontwikkeling die voorziet in een maatschappelijke behoefte. Vanuit de optiek van de rechtspraktijk verwachten wij een ruime en adequate werking van deze wet, mits er een goede balans tussen rechtsbescherming en effectiviteit wordt gevonden. De verdere discussies in het wetgevingsproces zullen wij met grote interesse op de voet blijven volgen.

[redacted]

[redacted]

[Dit document is enkel elektronisch aangemaakt en zal om die reden niet worden ondertekend]