Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 647

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 oktober 2019

In de aanloop naar het AO Cybersecurity, gepland op 30 oktober, wil ik uw Kamer een actuele stand van zaken geven van de invulling van de aanvullende maatregelen waarover ik uw Kamer in de beleidsreactie van het Cybersecurity Beeld Nederland[1] (CSBN) 2019 van 12 juni jl. informeerde. Die brief was ook de eerste voortgangsrapportage van de Nederlandse Cybersecurity Agenda[2] (NCSA). Hoewel met de implementatie van de eerste NCSA-maatregelen een goede start was gemaakt, schetste het CSBN2019 een dusdanig zorgwekkend beeld dat ik aanvullende maatregelen aankondigde om de regie op cybersecurity te versterken. Zoals ik in die brief aangaf wil ik de regie versterken door de bewustwording van de risico's voor de digitale weerbaarheid te vergroten, het beveiligingsniveau en het toezicht te versterken en meer te oefenen en te testen. Dit alles om het digitale weerbaarheidsniveau structureel te verhogen.

Dat dergelijke maatregelen hard nodig zijn blijkt nogmaals uit de ontwikkelingen op het gebied van cybersecurity sinds het versturen van mijn vorige brief. In september publiceerde de Wetenschappelijke Raad voor het Regeringsbeleid het rapport «*Voorbereiden op Digitale ontwrichting*», waarin wordt gesteld dat we ons moeten voorbereiden op het scenario van grootschalige digitale ontwrichting. Ook sprak ik met uw Kamer tijdens het mondelinge vragenuur van 1 oktober jl. over kwetsbaarheden in VPN-Pulse software, waar veel organisaties, ook mijn eigen ministerie, mee te maken hadden (Handelingen II 2019/20, nr. 7, item 2). Zoals ik uw Kamer liet weten wordt momenteel gewerkt aan een analyse van deze casus en zal ik die uw Kamer zo spoedig mogelijk doen toekomen.

Hoewel de casus nog wordt onderzocht, past dit binnen het geschetste beeld van het CSBN2019 en bevestigt eens te meer het belang van het

[1] Kamerstuk 26 643, nr. 614.
[2] Kamerstuk 26 643, nr. 536.

kst-26643-647
ISSN 0921 - 7371
's-Gravenhage 2019

verhogen van de digitale weerbaarheid van de vitale infrastructuur en de noodzaak om hier stevig regie op te voeren. Daarom neem ik met mijn collega bewindspersonen maatregelen die ons daar beter toe in staat stellen. Hiermee wordt concreet invulling gegeven aan de maatregelen die ik in juni jl. aankondigde.

Versterken toezicht

De *Wet beveiliging netwerk en informatiesystemen* (Wbni) vormt, naast bestaande sectorale wetgeving, een belangrijk instrument om de cyberweerbaarheid van vitale sectoren te verhogen. Primair blijft de weerbaarheid van een organisatie de eigen verantwoordelijkheid. De sectorale toezichthouders spelen hierbij een belangrijke rol. Zij kennen de verschillende sectoren goed en kunnen de afweging maken of organisaties de juiste maatregelen nemen om hun weerbaarheid te verhogen. Vanuit mijn coördinerende rol voor nationale veiligheid en cybersecurity zet ik er op in hen zo goed mogelijk in positie te brengen. Dit gebeurt bijvoorbeeld door de samenwerking met het Nationaal Cybersecurity Centrum (NCSC) te intensiveren, waardoor er waar mogelijk meer concrete dreigingsinformatie ook bij de toezichthouders terecht komt. Mede hierdoor kunnen zij erop toezien of maatregelen worden genomen die toereikend zijn. Daarnaast gaat de Inspectie Justitie en Veiligheid samen met de betrokken toezichthouders dit jaar het eerste intern vertrouwelijke inspectiebeeld opleveren waarmee we indirect een beter beeld krijgen van de algehele staat van de weerbaarheid.

Interventiemogelijkheden

Waar nodig zal gebruik worden gemaakt van de interventiemogelijkheden onder de Wbni als dat nodig is in het kader van nationale veiligheid. Het NCSC zal bijvoorbeeld vaker toezichthouders informeren over situaties waarin een vitale aanbieder beveiligingsadviezen onvoldoende opvolgt waardoor risico's voor de nationale veiligheid blijven bestaan. De VPN-Pulse kwetsbaarheid laat zien dat waarschuwingen en adviezen van het NCSC niet altijd direct worden opgevolgd. In sommige gevallen kan er een goede reden zijn om een dergelijk advies niet of niet volledig op te volgen, maar als het om de nationale veiligheid gaat moet die afweging bewust en inzichtelijk worden gemaakt. Als een beveiligingsadvies door een vitale aanbieder na herhaaldelijk waarschuwen niet wordt opgevolgd en het risico voor de nationale veiligheid blijft bestaan, zal het NCSC de sectorale toezichthouder hiervan op de hoogte stellen. De toezichthouder beslist vervolgens op basis van de eigen verantwoordelijkheid over passende interventies waarbij onder meer de Wbni voldoende handvatten biedt[3]. Indien er verschil van inzicht bestaat over de opvolging door de sectorale toezichthouders, zal ik de desbetreffende Minister hier in het belang van de nationale veiligheid op wijzen.

Verhogen beveiligingsniveau

Voor aanbieders van essentiële diensten (AED's) – vitale organisaties die onder het volledige regime van de Wbni vallen – geldt dat de zorgplicht verder wordt ingevuld door het opstellen van generieke beveiligingsdoelen. Bij de eerste wijziging van het *Besluit beveiliging netwerk- en informatiesystemen* (Bbni), die momenteel in voorbereiding is, wordt de zorgplicht verder gespecificeerd en worden AED's verplicht om waar nodig aanvullende maatregelen te nemen. Hiermee wordt een algemeen basisniveau van beveiligingsdoelen gerealiseerd. De verantwoordelijkheid voor het realiseren van deze beveiligingsdoelen ligt bij de AED's zelf.

[3] Zie Stcrt. 2015, nr. 3151041 Aanwijzingen inzake de Rijksinspecties

Naast de generieke zorgplicht voorziet de genoemde wijziging van het Bbni erin dat, bij regeling van de voor een sector verantwoordelijke Minister, een verdere sectorspecifieke invulling van de zorgplicht kan plaatsvinden. Met het oog op mijn wettelijke taken vindt er nauw overleg met mij plaats bij het opstellen van de sectorspecifieke beveiligingsdoelen. Zo heb ik zicht of de zorgplicht in Ministeriële regelingen voldoende wordt gewaarborgd.

Oefen- en testprogramma

Zoals het WRR-rapport ook betoogt is honderd procent veiligheid, zeker in het digitale domein, een illusie. Ondanks dat dit kabinet maximaal inzet op preventieve maatregelen kan een situatie waarbij sprake is van digitale ontwrichting niet worden uitgesloten. Daarom wordt gewerkt aan een publiek-private oefenagenda om oefenen te stimuleren. Volgend jaar zal bijvoorbeeld onder de naam ISIDOOR 2020 een reeks aan oefeningen op operationeel, bestuurlijk en politiek niveau worden georganiseerd. De komende periode zal de oefenagenda verder worden ingevuld. Daarnaast zal bij de bovengenoemde eerste wijziging van het *Besluit beveiliging netwerk- en informatiesystemen* als maatregel worden opgenomen dat AED's periodiek hun beveiligingsdoelen moeten evalueren. Organisaties kunnen aan de invulling hiervan voldoen door bijvoorbeeld hun processen en systemen te testen en oefeningen uit te voeren. Om vitale partijen te helpen met het testen van systemen werkt het NCSC aan richtlijnen hiervoor.

Optimaliseren instrumentarium digitale weerbaarheid

Bovenstaande acties zijn een concrete invulling van de aanvullende maatregelen die ik voor de zomer aankondigde en dragen in belangrijke mate bij aan de realisatie van de ambities gesteld in de NCSA. De komende tijd zal ik met betrokken bewindspersonen, in het bijzonder die van IenW en EZK, en (vitale) organisaties aan de hand van bevindingen van toezichthouders onderzoeken of deze maatregelen binnen de huidige kaders mij en het kabinet voldoende handvatten bieden om regie te kunnen voeren en toezicht te kunnen houden op de digitale weerbaarheid van de vitale infrastructuur. Ik zal uw Kamer over de voortgang hiervan en over de verdere invulling van de aanvullende maatregelen nader informeren in de kabinetsreactie op het WRR-rapport die ik aanstaande voorjaar aan uw Kamer stuur.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus