> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Programma Nederland Digitaal Veilig

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
2955213

Bijlagen
2

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 29 juni 2020
Onderwerp Beleidsreactie CSBN 2020 en voortgangsrapportage NCSA

Hierbij bied ik uw Kamer het Cybersecuritybeeld Nederland 2020 (CSBN 2020) en mijn reactie hierop aan, en informeer ik u over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA).

Cybersecuritybeeld Nederland 2020
Het CSBN 2020 schetst opnieuw een zorgwekkend beeld. Cyberincidenten hebben de potentie om grote schade aan te richten en in uiterste gevallen maatschappelijke ontwrichting te veroorzaken. De digitale dreiging van statelijke actoren en cybercriminelen heeft inmiddels een permanent karakter gekregen. Onze maatschappij is in grote mate afhankelijk van digitale processen, en analoge terugvalopties zijn niet altijd voorhanden. De kans op digitale incidenten met gevolgen in de fysieke wereld en de impact daarvan nemen daardoor toe. Dit geldt zowel voor incidenten die ontstaan door moedwillig misbruik van kwetsbaarheden als door uitval als gevolg van storingen. Door de situatie die is ontstaan door COVID-19 is onze afhankelijkheid van digitale middelen nog verder toegenomen.

Het afgelopen jaar hebben zich verschillende incidenten voorgedaan die het beeld uit het CSBN 2020 illustreren. Hierbij valt te denken aan kwetsbaarheid in producten van Citrix, besmetting met ransomware bij de Universiteit Maastricht en de onbereikbaarheid van 112 naar aanleiding van een storing bij KPN.

Het beeld dat naar voren komt uit het CSBN 2020 is niet nieuw en mag geen verrassing zijn. Het sluit aan bij eerdere edities van het CSBN en andere publicaties, zoals het rapport ‘Voorbereiden op digitale ontwrichting’ van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).[1] Maatschappelijke ontwrichting door cyberaanvallen of door grootschalige uitval heeft zich in Nederland nog niet voorgedaan. Toch valt dat in de toekomst zeker niet uit te sluiten. De digitale weerbaarheid blijft daarom vragen om onze voortdurende aandacht. Ook zonder dat er sprake is van (potentiële) maatschappelijke ontwrichting kan de maatschappelijke en economische schade

[1] Wetenschappelijke Raad voor het Regeringsbeleid, ‘Voorbereiden op digitale ontwrichting’ (rapport nr. 101, 2019).

van incidenten groot zijn. Cyberaanvallen via bijvoorbeeld ransomware vormen nog altijd een aantrekkelijk verdienmodel voor criminelen. Daarom blijft ook de aanpak van cybercriminaliteit onverminderd van belang. Over de voortgang van de integrale aanpak cybercriminaliteit informeer ik u gelijktijdig via een aparte brief.

Nederlandse Cyber Security Agenda als leidraad Nederlandse cybersecurityaanpak
De kabinetsbrede aanpak op cybersecurity is vastgelegd in de NCSA.[2] De uitvoering daarvan wordt ondersteund met investeringen die oplopen tot 95 miljoen euro structureel. In de bijlage van deze brief is een voortgangsrapportage gevoegd met de belangrijkste resultaten die het afgelopen jaar zijn bereikt onder de zeven ambities van de NCSA.

In de NCSA is het belang benadrukt van een adaptieve benadering van cybersecurity. Om in te kunnen spelen op technologische en maatschappelijke ontwikkelingen en actuele dreigingen en risico's, kunnen de maatregelen uit de NCSA in de loop van de tijd verder worden uitgewerkt en versterkt. Dit is sinds de verschijning van de NCSA in april 2018 ook meerdere keren gebeurd. De zeven ambities uit de NCSA blijven hierbij het uitgangspunt. In mijn beleidsreactie op het CSBN 2019 heb ik vorig jaar vier versterkingssporen aangekondigd, om de structurele en adaptieve risicobeheersing binnen vitale sectoren verder te verbeteren.[3] Het kabinet heeft daarnaast in haar reactie op het WRR-rapport over digitale ontwrichting in april 2020 een lijst met aanvullende maatregelen gepubliceerd om het cybersecuritystelsel in Nederland verder te versterken.[4] Deze aanvullende maatregelen zijn voornamelijk gericht op het verbeteren van de digitale slagkracht en het verhogen van de digitale weerbaarheid, en dragen zo bij aan de verdere uitvoering van ambities 1 en 4 uit de NCSA.

Voortzetting cybersecurityaanpak komende periode
De ervaring met incidenten die zich het afgelopen jaar hebben voorgedaan en publicaties zoals het hierboven genoemde WRR-rapport hebben het inzicht in onze digitale veiligheid verder verdiept. Het beeld van onze digitale veiligheid is op basis van de ontwikkelingen die het CSBN 2020 schetst niet fundamenteel gewijzigd. Dit sterkt mij in het voortzetten van de huidige cybersecurityaanpak binnen de NCSA. Het voorkomen van maatschappelijke ontwrichting door incidenten binnen vitale processen heeft de hoogste prioriteit. Het kabinet werkt aan een 'pas toe of leg uit'- systematiek voor vitale aanbieders en de Rijksoverheid. Bij ernstige kwetsbaarheden, zoals in het geval van een high-high beveiligingsadvies van het NCSC, dienen deze partijen mitigerende maatregelen te nemen of uit te kunnen leggen aan een door de verantwoordelijke minister gemandateerde organisatie (bijvoorbeeld een toezichthouder) waarom ze deze niet nemen. Dit draagt bij aan een adequatere opvolging van de beveiligingsadviezen van het NCSC. Tegelijkertijd moeten we voorbereid zijn op een situatie waarin het toch mis gaat. Het Nationaal Crisisplan Digitaal is geactualiseerd en cyberoefeningen worden steeds meer de norm. Daarnaast moeten organisaties tijdig kunnen beschikken over de juiste informatie om hun eigen verantwoordelijkheid op digitale beveiliging te kunnen nemen. Binnen het Landelijk Dekkend Stelsel (LDS) van cybersecuritysamenwerkingsverbanden zijn stappen gezet om ook de informatie-uitwisseling met niet-vitale organisaties te verbeteren. Dit gebeurt onder meer via het aanwijzen van computercrisisteams krachtens de Wbni voor bijvoorbeeld de zorg en het hoger onderwijs waarmee het NCSC ook bepaalde vertrouwelijke informatie kan delen, en het omzetten van het Digital Trust Center voor het niet-vitale bedrijfsleven naar een permanente organisatie. Dit stelsel zal het komende jaar nog verder worden versterkt.

Het CSBN 2020 meldt verder dat er sinds de start van de COVID-19-pandemie aanwijzingen zijn dat actoren de situatie misbruiken om 'gethematiseerde' cyberaanvallen uit te voeren op bijvoorbeeld ziekenhuizen, farmaceuten en onderzoekscentra. Om deze organisaties in Nederland gedurende de uitbraak van COVID-19 zo goed mogelijk bij te staan, is onlangs spoedwetgeving tot

[2] Kamerstukken II 2017/18, 26643, nr. 536
[3] Kamerstukken II 2018/19, 26643, nr. 625
[4] Kamerstukken II 2019/20, 26643, nr. 673

stand gebracht, die het NCSC de taak geeft om deze organisaties[5] bij digitale dreigingen en incidenten bijstand te verlenen. Daarnaast laat het CSBN 2020 zien dat door de ontwikkelingen rond COVID-19 de potentiele impact van uitval van netwerk- en informatiesystemen nog verder is toegenomen. Dit maakt het belang van digitale weerbaarheid en een samenleving die adequaat kan reageren op digitale incidenten alleen nog maar groter. Ik heb eerder aangegeven voorstander te zijn van een stelsel waarin ruimte is voor expertise en eigen verantwoordelijkheid. Daar staat tegenover dat we moeten waken voor een te versnipperd landschap qua regie en informatievoorziening vanuit de overheid. Daarom zijn in de kabinetsreactie op het WRR-rapport verschillende maatregelen opgenomen die als doel hebben het huidige stelsel in kaart te brengen, tekortkomingen te signaleren en indien nodig wetswijzigingen door te voeren. Hiertoe zie ik de volgende tijdslijn: komend halfjaar zal ik, in samenspraak met andere betrokken ministers, de huidige wettelijke taken en bevoegdheden in kaart brengen die het mogelijk maken informatie te delen en/of in het uiterste geval in te grijpen dan wel te sturen op de digitale weerbaarheid bij rijksoverheid, vitale aanbieders en niet-vitale organisaties. De minister van BZK zal de wijze waarop de medeoverheden zijn toegerust op digitale ontwrichting en kaders die nodig zijn bij de medeoverheden verkennen. Hieruit zal blijken of en welke sturingsinstrumenten ontbreken, die ontwikkeld zouden moeten worden. Deze bevindingen zal ik bundelen en in januari 2021 met uw Kamer delen. De uitkomsten zal ik, waar relevant, betrekken bij de wijziging van de Wbni. Dit traject zal starten in de eerste helft van 2021.

Tenslotte, het CSBN 2020 laat opnieuw zien dat de onderlinge afhankelijkheid door digitalisering steeds meer toeneemt. Hierdoor vervaagt het traditionele onderscheid tussen vitaal en niet-vitaal steeds verder. De uitval van netwerk- of informatiesystemen bij een toeleverancier of onderaannemer kan door de onderlinge afhankelijkheid enorme gevolgen hebben voor de continuïteit van een vitaal proces. Dit betekent dat het vaststellen van de te beschermen belangen binnen de samenleving steeds complexer wordt, dit vraagt om een bredere blik op wat nodig is om maatschappelijke ontwrichting te voorkomen. In de versterkte aanpak vitale infrastructuur, waarover ik uw Kamer de tweede helft van 2020 zal informeren, zal daarom ook aandacht zijn voor wederzijdse afhankelijkheden.

Voortgang NCSA en resultaten

Met de implementatie en verdere uitwerking van de NCSA worden belangrijke stappen gezet om de digitale weerbaarheid van Nederland te verbeteren. Deze aanpak moet zich de komende tijd in de praktijk verder bewijzen.

De uitvoering van de NCSA is inmiddels in volle gang, en dit heeft geleid tot talrijke concrete resultaten. Daarbij is ook met de uitvoering van het versterkingsprogramma een goede start gemaakt, en worden de maatregelen die recent zijn aangekondigd naar aanleiding van het WRR-rapport momenteel uitgewerkt. Er is een overzicht van de voortgang van de NCSA opgenomen in de bijlage, inclusief vooruitblik voor de komende tijd.

De effecten van de maatregelen uit de NCSA en de verdere versterkingen daarvan zullen in de loop van de tijd duidelijk moeten worden. Voor de NCSA is een evaluatie voorzien voor 2021. Daarnaast zal de Cybersecurity Raad (CSR) aan het einde van dit jaar een advies opleveren over de benodigde investeringen in cybersecurity voor een volgende kabinet.[6]

Conclusie

De komende periode gaat het kabinet, mede door middel van publiek-private samenwerking, verder aan de slag met de uitvoering van de maatregelen van de NCSA, het

[5] Het gaat hier om ziekenhuizen waar intensive care wordt of kan worden verleend, fabrikanten van geneesmiddelen, fabrikanten van medische hulpmiddelen en instellingen die onderzoek verrichten dat gericht is op de diagnostiek van COVID-19.

[6] Hiermee geef ik invulling aan mijn toezegging uit het Algemeen Overleg Cybersecurity (30 oktober 2019), Kamerstukken II 26643-650.

versterkingsprogramma en de beleidsreactie op het WRR-rapport. In de bijlage wordt verder ingegaan op de belangrijkste resultaten die het komende jaar worden voorzien binnen de NCSA. Hierover blijf ik uw Kamer informeren en blijf ik met uw Kamer in gesprek.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus