Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 673 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 maart 2020

Hierbij bied ik uw Kamer de kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek aan[1].

Cybersecurity is een prioriteit van dit kabinet. Met onder andere de uitwerking van de Nederlandse Cybersecurity Agenda (NCSA) worden onder mijn coördinatie maatregelen genomen om de kabinetsbrede cybersecurity-ambities te realiseren. Om te beginnen is structureel 95 miljoen extra geïnvesteerd in cybersecurity. Hiermee zijn belangrijke stappen gezet. Ontwikkelingen volgen elkaar echter in rap tempo op. Het Cybersecuritybeeld Nederland 2019 (CSBN2019) (Kamerstuk 26 643, nr. 614) en andere publicaties van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) lieten al zien dat de dreiging toeneemt, onze weerbaarheid onder druk staat en maatschappelijke ontwrichting op de loer ligt.

Het rapport van de WRR richt zich op risico's van digitalisering voor de maatschappij. Het kabinet onderschrijft de hoofdaanbeveling van de WRR dat de voorbereiding op incidenten een nadrukkelijk onderdeel moet zijn van ons nationale veiligheidsbeleid. Het volledig voorkomen van digitale incidenten is onmogelijk. Digitaal moet evenwel niet worden gezien als een op zichzelf staand domein. Het reguliere beleid, crisispreparatie en crisisrespons zijn ook van toepassing op incidenten met een digitale component. De WRR signaleert daarbij wel dat bepaalde elementen bij incidenten met een digitale component nog onvoldoende geadresseerd worden binnen de huidige structuren. Incidenten hebben door onderlinge afhankelijkheden en door de complexiteit en diversiteit van netwerk- en informatiesystemen sneller grootschalige en grensoverschrijdende effecten. De overheid moet zich daarom in samenwerking met private organisaties voorbereiden op incidenten in de digitale ruimte. Onze

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-673
ISSN 0921 - 7371
's-Gravenhage 2020

onverminderde inzet en investeringen blijven ook de komende jaren nodig om ons land digitaal veilig te houden.

Opbouw

In deze brief sta ik uitgebreid stil bij de constateringen van de WRR en wat deze betekenen in uitbreiding, wijziging of aanvulling op het beleid van dit kabinet. Daarbij betrek ik ook de geleerde lessen uit de Citrix-problematiek en zet ik uiteen hoe dit kabinet zich voorbereidt op digitale incidenten en welke maatregelen worden genomen voor het verhogen van onze digitale weerbaarheid. In de verdere kabinetsreactie wordt in twee hoofdstukken ingegaan op:

I. Respons bij incidenten en crises met digitale elementen

II. Voorkomen van incidenten en verhogen van de weerbaarheid
Als Minister van Justitie en Veiligheid ben ik coördinerend bewindspersoon voor cybersecurity en crisisbeheersing. In ons cybersecuritystelsel werken, onder coördinatie van de NCTV, ministeries, toezichthouders, vitale aanbieders, inlichtingen- en veiligheidsdiensten, Nationaal Cybersecurity Centrum (NCSC), politie en Openbaar Ministerie (OM) samen aan een digitaal veilig Nederland.

Uitgangspunt in ons stelsel is dat alle organisaties primair zelf verantwoordelijk zijn voor digitale weerbaarheid. De overheid treedt op waar nodig, onder meer door opsporing, vervolging en attributie. Bovendien zorgt de overheid voor informatievoorziening over dreigingen en kwetsbaarheden. Specifieke doelgroepen als de vitale infrastructuur en de rijksoverheid kunnen rekenen op bijstand in het geval van een incident. Uitval van systemen bij deze organisaties kan immers al snel gevolgen hebben voor alle burgers en bedrijven in ons land. In deze brief wordt daarom in beide hoofdstukken (respons en weerbaarheid) steeds onderscheid gemaakt tussen:
A) Alle bedrijven en organisaties in Nederland, om vervolgens in te gaan op de specifieke aanpak voor:
B) De als vitaal aangewezen organisaties (vitale aanbieders) en
C) De (rijks)overheidsorganisaties

Geleerde lessen Citrix-problematiek

Digitale incidenten bij organisaties zoals universiteiten en ziekenhuizen hebben ons laten zien dat kwetsbaarheden een grote impact kunnen hebben. Begin dit jaar heeft de Citrix-problematiek ons in de praktijk laten zien hoe groot de noodzaak is om aanvullende maatregelen te nemen. Daarom is de evaluatie naar aanleiding van de Citrix-problematiek betrokken bij deze kabinetsreactie.[2] Bijgevoegd vindt u de bevindingen van deze evaluatie.[3]

Aanpak van incidenten of crises met digitale elementen: Respons (I) en Preventie (II)

I - Respons bij incidenten en crises met digitale elementen

De WRR stelt dat het bestaande instrumentarium tijdens een crisis met digitale elementen moet worden aangepast en dat de overheid onvoldoende bevoegdheden heeft om in te grijpen. De WRR doet de aanbe-

[2] Kamerstuk 26 643, nrs. 658 en 660
[3] Deze evaluatie is verricht door COT: Instituut voor veiligheids- en crisismanagement. Raadpleegbaar via **www.tweedekamer.nl**

veling om een helder afgebakende wettelijke bevoegdheid voor digitale hulptroepen te creëren en de noodzaak van een aparte regeling voor overheidshandelen gericht op tegengaan van escalatie te onderzoeken.

Voor situaties waarin de nationale veiligheid in het geding is of kan zijn, en dus vitale belangen van de samenleving zodanig bedreigd worden dat er sprake is van (potentiële) maatschappelijke ontwrichting, kan de nationale crisisstructuur in werking treden. Deze is door het kabinet vastgelegd in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbesluitvorming. Het Nationaal Crisisplan Digitaal (NCP-Digitaal)[4] dat in februari van dit jaar aan uw Kamer is aangeboden, is een specifieke uitwerking voor de aanpak van een crisis met digitale elementen. Dit plan is een leidraad om inzicht en overzicht te creëren voor organisaties en actoren, die een rol spelen bij de beheersing van de maatschappelijke gevolgen en effecten van een ICT-incident. Het plan beschrijft de crisisaanpak op rijksniveau en de samenwerking en aansluiting met betrokken publieke en private partners en netwerken op internationaal en regionaal niveau. Centraal staat de gezamenlijke opgave om in het geval van een grootschalig incident of crisis de maatschappelijke ontwrichting te voorkomen of de effecten te beperken. Zoals aan uw Kamer gemeld, wordt het NCP-Digitaal al dit najaar geactualiseerd. Daarbij zullen de leerpunten uit de evaluatie van de aanpak van de Citrix-problematiek worden verwerkt, alsook de relevante punten uit deze kabinetsreactie, het Cybersecuritybeeld Nederland 2020 en de lessen van oefening ISIDOOR 2020. Verder zal het kabinet vanwege de snelle ontwikkelingen in het digitale domein in overleg met de betrokken partijen jaarlijks bezien of het crisisplan moet worden aangepast of geactualiseerd.

A) Respons – Alle bedrijven en organisaties

De WRR beschrijft dat incidenten met digitale componenten zich snel kunnen verspreiden en dat de impact groot kan zijn. Dit geldt ook voor organisaties die niet als vitaal zijn aangemerkt. De Citrix-problematiek maakte nogmaals duidelijk dat incidenten bij organisaties die niet als vitaal zijn aangemerkt tot overlast of onrust kunnen leiden.

Effectievere informatie-uitwisseling landelijk dekkend stelsel

Alle bedrijven en organisaties in Nederland moeten hun verantwoordelijkheid op het gebied van cybersecurity kennen en nemen. Dit betekent dat zij zelf moeten investeren in hun digitale veiligheid, maar ook dat ze moeten kunnen rekenen op informatie en advies wanneer er sprake is van een ernstige dreiging. Het NCSC is het expertisecentrum voor cybersecurity in Nederland en stelt- mede gebaseerd op dreigingsinformatie van de inlichtingen- en veiligheidsdiensten actuele beveiligingsadviezen op. Hierbij geldt het uitgangspunt dat het NCSC informatie zoveel als mogelijk deelt met partijen binnen het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden (LDS). Dit stelsel is volop in ontwikkeling. De verdere opbouw en uitbreiding ervan zijn van groot belang. Het NCSC deelt daarnaast bepaalde vertrouwelijke informatie (persoonsgegevens, bedrijfsvertrouwelijke gegevens) met aangewezen[5] computercrisisteams

[4] Nationaal Crisisplan Digitaal, bijlage bij Kamerstuk 30 821, nr. 102

[5] Aanwijzing van Computer Emergency Response Teams (CERTs) en OKTTs vindt plaats op grond van artikel 3, lid 2 van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Bij CERTs kan aanwijzing ook op grond van artikel 16, lid 3 onder b en artikel 20, tweede lid, onder b Wbni plaatsvinden. Zo zijn bijvoorbeeld SurfCERT, ZorgCERT, de Informatiebeveiligingsdienst en CERT-WM aangewezen.

of koepelorganisaties[6], deze sectorale cybersecurity-organisaties verspreiden de informatie onder hun doelgroepen. Organisaties kunnen daarbij ook gebruik maken van beschikbare diensten in de markt.

Uit de Citrix-evaluatie bleek dat de beveiligingsadviezen niet in alle gevallen de organisaties buiten de primaire doelgroepen van het NCSC bereikten en dat men niet altijd wist wat de verschillende verantwoordelijkheden binnen het stelsel zijn. Voor alle sectoren moet duidelijk zijn welke basismaatregelen zij minimaal moeten nemen en bij welke sectorale cybersecurity-organisatie zij terecht kunnen voor actuele informatie in geval van incidenten. Dit vraagt om een actievere houding van alle betrokken organisaties en een sterker bewustzijn van de verschillende rollen en verantwoordelijkheden binnen het stelsel. De komende periode wordt daarom een handreiking LDS opgesteld, hierin wordt ingegaan op de verschillende rollen binnen het stelsel en de verantwoordelijkheid van het NCSC en de sectorale cybersecurityorganisaties bij het doorgeleiden van beveiligingsadviezen. Hierbij wordt ook ingegaan op de aanbeveling van het COT om na te denken over «taal en impact» van het advies. Daarnaast geldt voor krachtens de Wet beveiliging Netwerk- en informatiesystemen (Wbni) aangewezen organisaties dat zij bepaalde vertrouwelijke informatie ook doorgeleiden aan doelgroeporganisaties. Tussen krachtens de Wbni aangewezen cybersecurity-organisaties en het NCSC worden hierover aanvullende afspraken gemaakt.

Certificering van cybersecurity dienstverleners

Aangezien bedrijven en organisaties primair voor hun eigen veiligheid en continuïteit verantwoordelijk zijn, is het van belang dat zij toegang hebben tot betrouwbare en kwalitatief goede private cybersecuritydienstverlening bij incidenten zodat zij kunnen handelen n.a.v. een beveiligingsadvies van het NCSC door geschikte en betrouwbare expertise in te huren. Daarom heb ik samen met de Staatssecretaris van Economische Zaken en Klimaat een subsidie aan het Centrum voor Criminaliteitspreventie en Veiligheid verstrekt om te komen tot een risicomodel en een kwaliteitsregeling voor leveranciers van cybersecuritydiensten. Hiermee wordt een basisniveau van betrouwbaarheid en kwaliteit gegarandeerd. Naar verwachting zullen het risicomodel en de kwaliteitsregeling medio dit jaar opgeleverd worden. In de tweede helft van 2020 vinden pilots plaats en worden de gewenste verbeteringen doorgevoerd. Begin 2021 vindt definitieve vaststelling en publicatie plaats.

B) Respons bij vitale aanbieders

De WRR wijst met betrekking tot crisisrespons op de afhankelijkheid van de overheid van private vitale aanbieders tijdens een crisis. Private vitale aanbieders hebben volgens de WRR niet altijd dezelfde belangen en zouden geen toegang tot systemen kunnen of willen verlenen aan de overheid. Volgens de WRR ontbreekt het aan instrumenten om private partijen te dwingen om mee te werken.

Eigen verantwoordelijkheid

Vitale aanbieders kunnen rekenen op ondersteuning van het NCSC bij incidentrespons. De incidentrespons bij vitale organisaties moet gezien de complexiteit en dynamiek echter altijd in nauwe samenwerking met de vitale aanbieders zelf gebeuren. Organisaties blijven zelf verantwoordelijk

[6] Organisaties die *objectief kenbaar tot taak* hebben organisaties of het publiek te informeren over digitale kwetsbaarheden en dreigingen (OKTT), zoals digitale koepelorganisaties.

en hebben zelf baat bij continuïteit van de door hen geleverde dienst, onder meer door het gevaar voor financiële of reputatieschade. Daarbij zijn zij zich bewust van hun maatschappelijke taak en hebben ze ook laten zien zich hiervoor in te willen zetten. Bovendien zijn de netwerk- en informatiesystemen dusdanig complex, gelaagd en uitgebreid dat gedetailleerde kennis nodig is om ook daadwerkelijk bijstand te kunnen verlenen. Hierbij is het ook wat betreft herstel de vitale aanbieder zelf die het vitale proces moet herstellen, aangezien deze aanbieder beschikt over de specifieke kennis en het noodzakelijke specialistisch personeel met kennis van de systemen.

«Pas toe of leg uit» afspraken met vitaal

Het NCSC informeert vitale aanbieders krachtens de Wbni actief over actuele dreigingen en adviseert over in verband daarmee te nemen beveiligingsmaatregelen. Verschillende van deze aanbieders hebben een meldplicht voor incidenten met aanzienlijke gevolgen voor hun dienstverlening bij het NCSC en bij de sectorale toezichthouder én de verplichting om passende beveiligingsmaatregelen te nemen ten aanzien van hun systemen (zorgplicht). In een ontwerpwijziging van het Besluit beveiliging netwerk en informatiesystemen (Bbni), die momenteel in procedure is, is ter nadere invulling van die zorgplicht opgenomen dat deze aanbieders voor wat betreft beveiligingsadviezen van relevante instanties, zoals het NCSC, moeten beoordelen of aanvullende beveiligingsmaatregelen nodig zijn om de risico's te reduceren. Dit zal hierdoor ook onderwerp zijn van de periodieke audits en controles die toezichthouders uitvoeren op de naleving van genoemde zorgplicht door deze aanbieders.
Daarbij zullen onder mijn coördinatie binnen het bestaande stelsel de komende periode samen met vakdepartementen, toezichthouders en vitale aanbieders werkafspraken gemaakt worden over *pas toe of leg uit* (comply or explain). Dit betekent dat vitale aanbieders in ernstige gevallen, zoals bij een *high-high* [7] beveiligingsadvies van het NCSC, in het geval zij geen opvolging geven aan een advies, uitleg geven aan een door de verantwoordelijke Minister gemandateerde organisatie. Deze gemandateerde organisatie kan een toezichthouder zijn of een andere geschikte aangewezen partij.

Interveniëren wanneer nodig

Onder bestaande wettelijke kaders kan worden ingegrepen wanneer dit toch nodig is. Vakdepartementen hebben hierin bevoegdheden om in te grijpen op basis van sectorale wetgeving en de Wbni, al dan niet gemandateerd aan sectorale toezichthouders, en kunnen van die bevoegdheden bijvoorbeeld gebruik maken als, in geval van crisis, een daartoe strekkend besluit door bijvoorbeeld via de Ministeriële Commissie Crisisbesluitvorming (MCCb) is genomen. Daarnaast geldt dat wanneer vanuit mijn ministerie vitale aanbieders geadviseerd worden om cybersecurity maatregelen te nemen en geconstateerd wordt dat onvoldoende of geen opvolging aan wordt gegeven en daardoor risico op maatschappelijke ontwrichting blijft bestaan, ik op basis van de Wbni de voor de betrokken sector verantwoordelijke Minister of bevoegde autoriteit informeer. Vakdepartementen kunnen zo op grond van hun wettelijke bevoegdheden, in het uiterste geval – na overleg – partijen door middel van een bindende aanwijzing alsnog maatregelen laten nemen. Tenslotte kan als uiterste middel noodwetgeving worden ingezet.

[7] Hoge kans op misbruik van een kwetsbaarheid en hoge schade door misbruik van een kwetsbaarheid

Verkenning wettelijke bevoegdheden overheid bij digitale crisissituaties

De hierboven genoemde bevoegdheden van het kabinet zijn vastgelegd in meerdere wetten. Met de betrokken departementen zal ik deze bevoegdheden in kaart brengen zodat het gehele instrumentarium voor ingrijpen bij crises met digitale elementen inzichtelijk wordt en zodat kan worden bezien waar eventuele aanvullingen nodig zijn. Hierbij worden onder meer de Coördinatiewet uitzonderingstoestanden en de Wet buitengewone bevoegdheden burgerlijk gezag betrokken. Inzet is dat over de volle maatschappelijke breedte voor alle sectoren en domeinen geborgd is dat er in crisissituaties voldoende bevoegdheden en interventiemogelijkheden zijn voor de rijksoverheid om in te kunnen grijpen waar dat in uiterste gevallen nodig is.

Respons bij de rijksoverheid

De rijksoverheid heeft een voorbeeldfunctie en belangrijke verantwoordelijkheden als het gaat om digitale veiligheid. Hoewel er de afgelopen periode flinke stappen zijn gezet, laten kwetsbaarheden in software zoals Pulse-VPN en Citrix zien dat verdere verbetering op het gebied van inzicht, handelingsperspectief en risico-bewustzijn noodzakelijk is.

Rollen en verantwoordelijkheden

Voor (dreigende) incidenten of crisis bij de rijksoverheid, is het NCP-digitaal leidend. Hierin staan de rollen en verantwoordelijkheden van alle partijen waaronder NCTV, NCSC, politie, inlichtingen- en veiligheidsdiensten, CIO-Rijk, CIO-beraad, vakdepartementen en de publieke-private ICT Response Board en het Nationaal Response Netwerk (NRN). Het NRN is een samenwerkingsverband tussen verschillende partijen onder coördinatie van het NCSC. Door de krachten van verschillende responscapaciteiten te bundelen worden bestaande capaciteiten versterkt en kan er effectiever worden gehandeld bij ICT-incidenten. Bij grootschalige ontwrichting beschikt het Defensie Cyber Security Centre over de expertise en middelen om aanvullende Cyber Incident Response uit te voeren.

Pas toe of leg uit bij de rijksoverheid

De komende periode gaat de rijksoverheid naast de al bestaande richtlijnen en kaders bindende afspraken maken op bestuurlijk en politiek niveau over *pas toe of leg uit.* Organisaties binnen de rijksoverheid moeten dan bij dringende adviezen van het NCSC aan de CIO-Rijk uitleg geven wanneer zij beveiligingsadviezen van het NCSC niet opvolgen. Bij eventuele conflicterende inzichten zal de CIO-Rijk escaleren naar de Minister van BZK. Net als voor bedrijven en andere organisaties geldt voor de rijksoverheidsorganisaties dat er in crisissituaties in uiterste gevallen voldoende mogelijkheden moeten zijn om in te grijpen. De mogelijkheden hiertoe worden betrokken bij de eerdergenoemde brede inventarisatie van wettelijke bevoegdheden voor de overheid bij digitale crisissituaties. Bij de Citrix-problematiek is voor het eerst met deze methodiek gewerkt en dit droeg in belangrijke mate bij aan een beter beeld van de opvolging van het beveiligingsadvies.[8]

[8] Daar waar de Wbni geldt of zal gelden voor vitale aanbieders binnen de rijksoverheid heeft de Wbni voorrang.

Optreden tegen kwaadwillende actoren en operationele paraatheid

Bovenstaande is voornamelijk gericht op respons met als doel de continuïteit van de samenleving zo goed als mogelijk te borgen. Indien er bij een incident of crisis sprake is van kwaadwillend handelen van een statelijke of criminele actor zullen de organisaties uit de nationale veiligheidsketen en waar nodig ook het Ministerie van Buitenlandse Zaken (BZ) betrokken zijn bij de respons. Hierbij moet rekening gehouden worden met de mogelijke spanning tussen de verschillende belangen zoals het opsporings- en inlichtingenbelang en het belang van de continuïteit van de geleverde diensten.

Nationale respons

Welke inzet aan de orde is, hangt af van de specifieke situatie en de verschillende belangen en afwegingen. Daarom wordt een geïntegreerd nationaal responskader opgesteld. Hierin maken de inlichtingen- en veiligheidsdiensten, politie, Defensie, BZ, OM, NCSC, betrokken vakdepartementen, veiligheidsregio's en de NCTV gezamenlijke werkafspraken over de respons bij een incident met digitale componenten. Dit responskader wordt de komende periode uitgewerkt en zal naar verwachting bij de eerstvolgende actualisering van het NCP-Digitaal operationeel zijn. Ook wordt verkend of het nodig is om vertrouwelijke informatiekanalen tussen overheidsdiensten en vitale aanbieders te verbeteren zodat deze zoveel als mogelijk in staat worden gesteld om tijdig de juiste maatregelen te kunnen nemen.

Om een landelijk situationeel beeld van dreigingen en kwetsbaarheden te verkrijgen en daarmee handelingsperspectief aan belanghebbende organisaties en bedrijven te bieden, is het van belang dat de relevante overheidsorganisaties robuuste informatiekanalen inrichten om gevoelige informatie te kunnen delen. Naar verwachting zal nog dit jaar een nieuw samenwerkingsplatform operationeel worden waar op dezelfde fysieke locatie samengewerkt wordt door politie, OM, NCSC, de AIVD en de MIVD met als doel informatie over cyberdreigingen en- incidenten bijeen te brengen en gezamenlijke analyses te verrichten.

De politie en het OM hebben verschillende wettelijke mogelijkheden om op te treden bij strafbare feiten en om verdere escalatie te voorkomen, dit geldt in het fysieke en het digitale domein[9]. Zij handelen op basis van publieksaangifte, ambtsbericht van inlichtingen – en veiligheidsdiensten of andere bronnen. Het OM en de politie kunnen ingrijpen wanneer er zich strafbare feiten voordoen. Daarnaast zal ik met de eerder aangekondigde inventarisatie van wettelijke bevoegdheden voor de overheid bij (digitale) crisissituaties in kaart brengen wat er nog meer mogelijk is om in te grijpen bij een incident met digitale elementen.

Daarbij zal ik onder andere ook naar aanleiding van de geleerde lessen van de Citrix-kwetsbaarheid bezien of we voldoende in staat zijn om te reageren op incidenten op het snijvlak van cybersecurity en cybercrime zoals misbruik door middel van ransomware.

[9] Voor meer informatie over de aanpak van cybercrime verwijs ik u naar eerder brieven over de integrale aanpak cybercrime en in het bijzonder naar voortgangsbrief aan uw kamer daarover – Kamerstuk 28 684, nr. 564

Internationale respons

Met het oog op de toenemende dreiging vanuit statelijke actoren en het mondiale karakter van het internet is samenwerking met internationale partners cruciaal. Buitenlandse Zaken coördineert diplomatieke en politieke respons in EU-, OVSE-, NAVO-verband en ad-hoc coalities. Het kabinet zet in op een versterking van de capaciteit om diplomatiek en politiek te kunnen reageren op ondermijnende cyberoperaties. Bij het bepalen van responsopties staat een zorgvuldige en integrale afweging van de Nederlandse belangen centraal.

Om de internationale samenwerking ook in Europees verband verder te structuren, is op Nederlands initiatief een «EU cyberdiplomatie toolbox» tot stand gekomen. Hiermee worden verschillende instrumenten van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid aangewend om actoren die ondermijnende cyberactiviteiten ontplooien ter verantwoording te roepen. Als onderdeel daarvan is op Nederlands initiatief 17 mei 2019 een EU cyber sanctieregime ingesteld waarmee het mogelijk wordt om tegoeden te bevriezen en inreisverboden op te leggen. Ook maakt het kabinet zich in het NAVO-bondgenootschap sterk voor het belang van verweer tegen het volledige spectrum aan vijandige cyberoperaties. Dit betreft niet alleen cyberoperaties die beschouwd kunnen worden als een gewapende aanval, maar ook operaties die onderdeel zijn van een hybride campagne onder de drempel van een gewapend conflict. Mede in navolging op de gewijzigde motie van de leden Verhoeven en Koopmans[10] zet Nederland zich in internationaal verband in voor versterking van coördinatie op het gebied van politieke attributie van cyberaanvallen. Een actief politiek attributiebeleid draagt bij aan het afschrikkend vermogen en het minder aantrekkelijk maken van Nederland als doelwit voor cyberaanvallen. Een actueel voorbeeld is de attributie door Nederland en gelijkgezinde landen van de cyberaanvallen op Georgië 28 oktober jl. aan de militaire geheime dienst van Rusland. Het kabinet wil daders van cyberaanvallen zoveel mogelijk publiekelijk aanspreken op hun gedrag.

II. Voorkomen van incidenten en verhogen van de weerbaarheid

De WRR zegt dat we ons moeten voorbereiden op digitale incidenten die kunnen leiden tot maatschappelijke ontwrichting. Dit houdt in dat we snel en effectief moeten kunnen reageren wanneer nodig, maar ook dat we ons in preventieve zin zo goed mogelijk moeten beschermen tegen digitale dreigingen.

A) Bescherming van alle bedrijven en organisaties

Ten behoeve van bedrijven en organisaties die geen deel uitmaken van de doelgroep van het NCSC (Rijk, vitaal) voorziet het NCSC, met inachtneming van de wettelijke kaders, andere computercrisisteams en cybersecurity samenwerkingsverbanden in het LDS zo veel als mogelijk van voor hun doelgroepen relevante dreigingsinformatie. De inzet van het kabinet is om dit stelsel verder uit te breiden en te versterken. Een belangrijk voorbeeld hiervan is de oprichting van het Digital Trust Center (DTC) van het Ministerie van EZK. Bij het DTC kan het (niet als vitaal aangemerkt) bedrijfsleven terecht voor informatie en advies. Het DTC werkt hierbij samen met samenwerkingsverbanden van bedrijven op het gebied van cybersecurity. Momenteel zijn dit er twintig en het streven is eind van dit jaar dertig samenwerkingsverbanden aangesloten te hebben bij het DTC. De Staatssecretaris van Economische Zaken en Klimaat heeft

[10] Kamerstuk 33 694, nr. 56

uw Kamer 18 februari 2020 geïnformeerd over positieve resultaten en structurele inrichting van het DTC[11]. Daarnaast kunnen ook organisaties uit andere sectoren terecht bij een computercrisisteam of samenwerkingsverband. Zo is er het Z-CERT voor de zorg, SURF-CERT voor universiteiten en hogescholen en de Informatie Beveiligingsdienst voor gemeenten. Voorts vervult het Ministerie van EZK krachtens de Wbni de taak van Computer Security Incident Response Team (CSIRT) voor digitale dienstverleners. Deze organisaties hebben als taak hun doelgroepen te informeren en adviseren over en te ondersteunen bij incidenten en in dat kader bijvoorbeeld algemene beveiligingsadviezen van het NCSC onder hun eigen doelgroepen te verspreiden.

Versterken landelijk dekkend stelsel

Het afgelopen jaar heeft dit kabinet al verschillende stappen gezet om de informatiepositie van organisaties binnen het LDS te versterken, onder meer door het krachtens de Wbni aanwijzen van verschillende van deze organisaties als computercrisisteams en andere koepelorganisaties met een cybersecurity-taak[12]. Dit maakt het mogelijk dat het NCSC bepaalde vertrouwelijke informatie over dreigingen, incidenten en kwetsbaarheden met deze organisaties kan delen. Tijdens de Citrix-problematiek werd duidelijk dat er nog veel sectoren zijn die niet over een eigen computercrisisteam of samenwerkingsverband beschikken. Uiteindelijk moet elk bedrijf en organisatie ergens terecht kunnen voor informatie en advies. Deze moeten in beginsel worden opgericht door de sectoren zelf, de verantwoordelijke vakministers spelen een belangrijke rol bij het aanjagen en faciliteren hiervan. Bovendien wordt het aantal organisaties dat wordt aangewezen als computercrisisteam of koepelorganisatie om andere organisaties of het publiek over dreigingen te informeren verder uitgebreid. Hierdoor kan het NCSC bepaalde vertrouwelijke informatie aan die aangewezen organisaties verstrekken.

Daarnaast wordt het bredere publiek over digitale risico's geïnformeerd door educatie, campagnes en structurele voorlichting door initiatieven als Veiliginternetten.nl en Alert Online. Naast bredere bewustwording over cybersecurity moet worden opgemerkt dat cybercrime en slachtofferschap daarvan centraal staan in de integrale aanpak cybercrime[13] waarover ik uw Kamer periodiek informeer.

Compensatie

De WRR beschrijft compensatie van slachtoffers als een belangrijk onderdeel van herstel na een ontwrichtend incident en doet daarom de aanbeveling om onderzoek te stimuleren naar de haalbaarheid van een cyberpool om financiële dekking mogelijk te maken voor schade als gevolg van digitale ontwrichting.
Het kabinet herkent deels de problemen die de WRR schetst. Het is belangrijk dat partijen met schade zo snel mogelijk in staat worden gesteld om de draad weer op te pakken. Verzekeringen kunnen hierbij een belangrijke rol spelen. Compensatieregelingen voor schade naar aanleiding van een cyberincident zijn vaak complex, omdat de oorzaak en eventuele dader van een incident lastig te achterhalen zijn. Wel ziet het

[11] Kamerstuk 26 643, nr. 668, Evaluatie Digital Trust Center
[12] Aanwijzing van CERTs en OKTTs vindt plaats op grond van artikel 3, lid 2 onder c van de Wbni. Bij CERTs kan aanwijzing ook op grond van artikel 16, lid 3 onder b en artikel 20, tweede lid, onder b Wbni plaatsvinden.
[13] Voor meer informatie over de aanpak van cybercrime verwijs ik u naar eerder brieven over de integrale aanpak cybercrime en in het bijzonder naar voortgangsbrief aan uw kamer daarover – Kamerstuk 28 684, nr. 564

kabinet dat op het gebied van verzekeringen schade na cyberincidenten steeds vaker onder normale bedrijfspolissen vallen[14] en dat er ook steeds meer cyberpolissen worden aangeboden. Op dit moment ziet het kabinet daarom geen aanleiding voor aanvullende maatregelen, maar blijft het de situatie monitoren. Als er in de toekomst problemen ontstaan zal worden bezien of ingrijpen alsnog nodig is.

B) Bescherming van de vitale infrastructuur

Om maatschappelijke ontwrichting te voorkomen is het waarborgen van de continuïteit van de vitale processen van belang. Bepaalde processen zoals drinkwater en energie zijn dusdanig essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting kan leiden en daarmee een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Binnen deze processen worden organisaties die belangrijk zijn voor de continuïteit van deze processen aangewezen als vitale aanbieder.

Vakdepartementen

De primaire verantwoordelijkheid voor de continuïteit en weerbaarheid van hun dienstverlening binnen vitale processen ligt bij de vitale aanbieders zelf. Daarbij hoort het verkrijgen van inzicht in dreigingen en kwetsbaarheden, risico's en het ontwikkelen en onderhouden van capaciteiten waarmee de weerbaarheid van vitale processen wordt verhoogd en geborgd. Het verantwoordelijke vakdepartement stelt – vanuit zijn systeemverantwoordelijkheid – sectorspecifieke kaders vast voor de vitale processen (in beleid of in wet- en regelgeving). In samenwerking met de vitale aanbieders en toezichthouders zorgen de vakdepartementen voor wettelijke borging van en controle op de vitale infrastructuur. Daarnaast heeft het bestuur van de veiligheidsregio een rol bij de vitale infrastructuur. Het Bestuurlijk Routeboek Digitale Ontwrichting van het Veiligheidsberaad brengt verantwoordelijkheden en bevoegdheden op regionaal niveau in kaart.

Wijziging Wet beveiliging netwerk- en informatiesystemen (Wbni)

In de Wbni is voor de meeste vitale aanbieders een plicht voor het treffen van passende beveiligingsmaatregelen opgenomen (zorgplicht). Daarnaast geldt een meldplicht voor incidenten met aanzienlijke gevolgen voor hun dienstverlening aan zowel de toezichthouder als het NCSC. Deze zorg- en meldplicht zijn erop gericht de gevolgen van cyberincidenten te beperken en maatschappelijke ontwrichting te voorkomen. Bovenstaande geldt echter niet voor alle vitale aanbieders, voor een deel van hen geldt slechts een meldplicht van incidenten met aanzienlijke gevolgen bij het NCSC en geen zorgplicht of toezicht daarop. Door ook andere vitale aanbieders onder het volledige regime van de Wbni te brengen, moeten zij aan de zorgplicht en daarmee aan een algemeen basisniveau van beveiligingsdoelen voldoen. Daartoe wil ik een wetswijzigingstraject starten zodat voor alle vitale aanbieders het volledige regime van de Wbni van toepassing wordt, voor zover sectorale wetgeving niet reeds dezelfde of strengere eisen stelt[15].

---

[14] «Silent» of «non-affirmative» cyber»: Deze term wordt gebruikt voor de claims n.a.v. cyberincidenten die worden uitbetaald vanuit een normale bedrijfspolis.

[15] Dit geldt bijvoorbeeld voor de financiële- en telecomsector

Zicht op afhankelijkheden

De WRR stelt dat in het digitale tijdperk beter inzicht nodig is in de verbindingen tussen digitale en fysieke sectoren en in de ketens en netwerken waarbinnen organisaties functioneren. Ook beveelt de WRR aan een cyberafhankelijkheidsbeeld op te stellen. Het kabinet ziet in dit kader een rol voor de sectorale toezichthouders. De verschillende vitale aanbieders zijn zelf verantwoordelijk voor het structureel uitvoeren van risicoanalyses en het treffen van maatregelen om de risico's voor de continuïteit van het vitale proces te beheersen. Onderdeel hiervan is zicht houden op afhankelijkheden. Tenslotte wordt beter inzicht in afhankelijkheden ook meegenomen in de versterkte aanpak bescherming vitale infrastructuur. Belangrijk hierbij is dat breder wordt gekeken dan alleen cybersecurity. Kwaadwillende actoren bedienen zich steeds meer van een hybride aanvalsmethode. Normen en beveiligingsadviezen ter bevordering van de weerbaarheid tegen (statelijke) actoren moeten dus integraal bekeken worden.

Terugvalopties

De WRR benoemt het belang van het organiseren van voldoende back-up en terugvalopties. Bij de implementatie van terugvalopties kunnen verschillende belangen spelen, zoals veiligheid op locatie, of de continuïteit van de dienst of het verliezen van de initiële baten van digitalisering. Daarnaast betekent dit gezien de mogelijk grote investeringen ook het afwegen en accepteren van risico's. In eerste instantie dienen organisaties de afwegingen op het gebied van terugvalopties mee te nemen in de eigen risicoanalyse. In de Wbni is opgenomen dat van aanbieders van essentiële diensten en digitale service providers wordt verlangd dat zij passende beveiligingsmaatregelen nemen om de continuïteit van de geleverde dienstverlening zoveel mogelijk te waarborgen. In dit kader kan ook gedacht worden aan terugvalopties.

Het Ministerie van Defensie is daarnaast gestart met een onderzoek of en welke defensievoorzieningen in samenwerking met (operationele) partijen kunnen worden ingezet om kritieke processen draaiende te houden wanneer er sprake is van maatschappij-ontwrichtende ICT-uitval. Een voorbeeld hiervan is een pilot waarin wordt gekeken of en zo ja hoe het Landelijk Crisis Management Systeem van het Instituut Fysieke Veiligheid (IFV) beschikbaar kan komen via de glasvezelnetwerken van Defensie (NAFIN) en Rijkswaterstaat. Ook worden de mogelijkheden uitgewerkt om het NAFIN-netwerk van Defensie voor Rijkswaterstaat en het IFV en vice-versa beschikbaar te stellen wanneer men door een digitale verstoring geen gebruik meer kan maken van het eigen netwerk.

Oefenen

Het kabinet is evenals de WRR van mening dat oefenen een van de belangrijkste maatregelen is om ons voor te bereiden op incidenten. Het kabinet kondigde in de zomer van 2019 al aan te starten met een brede publiek-private oefenagenda[16]. Hiermee wordt onder andere invulling gegeven aan de motie over een stresstest voor vitale aanbieders en rijksoverheid[17]. Deze verzoekt de regering een structureel stresstest- en oefenprogramma op te zetten waarbij de overheid en vitale sectoren cross-sectoraal oefenen op scenario's van digitale ontwrichting om zo de

[16] Kamerstuk 26 643, nr. 614 – Brief inzake Cybersecuritybeeld Nederland 2019 en voortgangsrapportage NCSA

[17] Kamerstuk 24 095, nr. 496 – Motie van het lid Weverling over een stresstest digitale ontwrichting

weerbaarheid hiertegen te vergroten, en de Kamer jaarlijks te informeren over deze cyberoefeningen. In het kader van de oefenagenda is gestart met de voorbereiding van de nationale cyberoefening ISIDOOR die voor de derde keer georganiseerd wordt: een nationale, cross-sectorale, operationele cyberoefening primair voor rijksoverheid en vitale aanbieders.

Tegen de achtergrond hiervan wijzigt het kabinet momenteel ook het Bbni waarin zal worden opgenomen dat aanbieders van essentiële diensten hun crisismanagementbeleid periodiek moeten oefenen, waardoor oefenen een verplichtend karakter krijgt voor aanbieders van essentiële diensten. Het NCSC zal partijen hierin faciliteren en ondersteunen vanuit de brede expertise. Zo kan een hoog niveau van weerbaarheid over sectoren worden bereikt.

Bredere bescherming vitaal

Welke processen en aanbieders we moeten beschermen en hóe we deze zouden moeten beschermen is aan constante verandering onderhevig. Hierbij speelt digitalisering, zoals de WRR aangeeft, een grote rol. De WRR geeft terecht aan dat een digitale samenleving betekent dat andersoortige organisaties vitaal kunnen zijn en dat door de onderlinge afhankelijkheden en verbindingen ook breder moet worden gekeken dan individuele organisaties. Tegelijk ontstaan door digitalisering ook nieuwe aanvalsmogelijkheden waardoor systemen vatbaarder worden voor cyberaanvallen en ongewenste statelijke inmenging van buitenaf. Er moet daarom gekeken worden naar het totaal aan processen en netwerken waaruit de vitale infrastructuur bestaat, wat de afhankelijkheden hierbinnen zijn en welke veiligheidsmaatregelen genomen moeten worden.
Het kabinet heeft in de Nationale Veiligheid Strategie een versterkte aanpak van de bescherming van de vitale infrastructuur aangekondigd. Onderdeel van deze versterkte aanpak is een structuur om kennis, kunde en expertise te bundelen om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur, adequaat te adresseren, nu en in de toekomst. In deze versterkte aanpak zal ook aandacht zijn voor afhankelijkheden, keteneffecten, netwerken en toeleveranciers. Uw Kamer zal in de tweede helft van 2020 worden geïnformeerd over de voortgang.

C) rijksoverheid: «Eigen huis op orde»

Voor de rijksoverheid heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een belangrijke rol als stelselverantwoordelijke voor rijksoverheids-ICT en namens hem de CIO-Rijk. Voor organisaties binnen de rijksoverheid geldt: het eigen huis moet op orde zijn.

Cybersecurity als onderdeel van de In-Control-verklaring

Er bestaan al kaders en richtlijnen voor informatiebeveiliging van rijksoverheids-organisaties. Vorig jaar is de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, waarmee het algemeen voorgeschreven beveiligingsniveau is aangescherpt. De CIO-Rijk monitort de naleving hiervan. Daarnaast wordt nu door CIO-Rijk in overleg met de NCTV en het NCSC verkend hoe rijksoverheidsorganisaties een doorlopende kwetsbaarhedenscan[18] in kunnen richten. CIO-Rijk zal hier nog dit jaar gezamenlijk een handreiking met kaders en randvoorwaarden voor rijksoverheidsorganisaties opstellen.

[18] Kamerstuk 30 821, nr. 85 – Motie van de leden Verhoeven en Laan-Geselschap over het op kwetsbaarheden scannen van overheidssystemen in de vitale infrastructuur

CIO-Rijk moet zicht hebben op de bij rijksoverheidsorganisaties in gebruik zijnde netwerk- en informatiesystemen. Van organisaties binnen de rijksoverheid wordt vanuit de BIO al verwacht dat zij een actueel en compleet overzicht hebben van informatiesystemen en componenten daarin[19]. CIO-Rijk zal in het informatiestatuut nieuwe afspraken maken over welke informatie met CIO-Rijk wordt gedeeld, zodat er een rijksbreed beeld komt van de gebruikte netwerk- en informatiesystemen.

Oefenen

Oefenen is een speerpunt van het kabinet en alle organisaties zijn hierbij gebaat. Ook rijksoverheidsorganisaties worden verplicht gesteld om periodiek crisismanagementbeleid te oefenen en om systemen te testen. Daarnaast is Nederland initiator en gastland van de Europese cyberoefening «Blue OLEx».
In zowel de Agenda Digitale Veiligheid als het Routeboek Cyber wordt ruim aandacht besteed aan de noodzaak tot oefenen op lokaal niveau. Op gemeentelijk niveau zijn daarvoor enkele oefenscenario's ontwikkeld die dit thema raken en aan kunnen sluiten op de regionale initiatieven en de hierboven beschreven landelijke oefening ISIDOOR. Een ander initiatief gericht op o.a. lokale overheden is «*De overheidsbrede cyberoefening: Wat zou jij doen*?», welke onder verantwoordelijkheid van de Minister van BZK plaatsvond in het najaar van 2019 en ook dit jaar weer wordt georganiseerd.

Medeoverheden

Het is van belang om duidelijke afspraken te maken met alle overheidsorganisaties die niet onder de rijksoverheid vallen, waaronder gemeenten, veiligheidsregio's, waterschappen en provincies. Immers daar leidt onderbreking van de dienstverlening al snel tot hinder voor burgers. De Citrix-problematiek liet dit ook zien. De BIO is sinds vorig jaar van kracht en is bedoeld voor de vier Nederlandse overheidslagen. De Minister van BZK gaat in overleg met onder meer de Vereniging van Nederlandse Gemeenten en mijn ministerie verder verkennen welke kaders en afspraken in dit verband noodzakelijk zijn. Hierbij wordt op gemeentelijk niveau gewerkt aan de Agenda Digitale Veiligheid Gemeenten waarin op lokaal niveau handelingsperspectief wordt geschetst bij diverse aspecten van digitale veiligheid. Ook in sectoraal verband worden afspraken gemaakt. Zo zijn in het Bestuursakkoord Water bijvoorbeeld aanvullende afspraken gemaakt over de versterking van cybersecurity in samenwerking tussen waterschappen, gemeenten, provincies, drinkwaterbedrijven en Rijkswaterstaat.

Toezicht, verantwoording en rapporteren

Een cruciaal element in een volwassen cybersecuritystelsel is toezicht en verantwoording op alle niveaus. Inzet van het kabinet is om cybersecurity een centraal onderdeel te maken van het brede toezichtsbeleid.

Inspecties en toezichthouders in het algemeen

Alle rijksinspecties en toezichthouders hebben een belangrijke signalerende en agenderende rol om cybersecurity binnen hun domein naar een hoger niveau van volwassenheid te brengen. Over de volle breedte moet

[19] BIO 8.1.1 1 Inventariseren van bedrijfsmiddelen «Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden

er meer cybersecuritybewustzijn komen bij de inspecties en toezichthouders. Samenwerking en afstemming is daarbij van groot belang. De Inspectieraad zal ik daarom vragen om met een voorstel te komen hoe die brede samenwerking en afstemming tussen de rijksinspecties en toezichthouders het beste tot stand kan worden gebracht. Hierbij zal ik ook vragen hoe een gedegen rapportagestructuur ingericht kan worden. Hier kan een voorstel uit volgen dat cybersecurity deel gaat uitmaken van het inspectie- of toezichtkader voor alle domeinen.

Toezichthouders vitale aanbieders

Voor bijna alle toezichthouders binnen het vitale domein geldt al dat cybersecurity een belangrijk onderdeel van hun werk is. Dit zal de komende jaren alleen maar toenemen en ook hier zullen meer investeringen nodig zijn. Met als doel de inzet van de verschillende toezichthouders op cybersecurity in kaart te brengen is dit jaar onder coördinatie van de Inspectie Justitie en Veiligheid voor het eerst een vertrouwelijk beeld opgesteld over het toezicht op cybersecurity bij vitale aanbieders. Dit is een belangrijke stap en vormt een gezamenlijk vertrekpunt voor een samenhangend periodiek inspectiebeeld cybersecurity dat bijdraagt aan inzicht in de effectiviteit van de maatregelen en algehele weerbaarheid van de vitale infrastructuur.

Rijksoverheid in control

Voor de rijksoverheid geldt dat er meer zicht moet komen op de staat van de weerbaarheid. De CIO-Rijk maakt bindende afspraken over welke informatie door rijksorganisaties met CIO-Rijk wordt gedeeld, zodat de CIO-Rijk een rijksbreed beeld ten aanzien van informatieveiligheid kan opleveren. Er worden afspraken gemaakt over het periodiek verstrekken van risicorapportages door departementale Chief Information Security Officers aan CIO-Rijk. Deze worden onderdeel van de *In-Control-verklaring*. Indien daartoe aanleiding is worden onderdelen daarvan geagendeerd in interdepartementale overleggen op hoog-ambtelijk niveau en waar nodig politiek.

Evalueren

Het kabinet deelt de conclusie van de WRR dat een incident waardevolle lessen kan bieden en bijdraagt aan beter beeld van de dreigingen en mogelijke verbetermaatregelen. In dit kader is dan ook meteen een evaluatie van Citrix-problematiek uitgevoerd. Het NCSC deelt daarnaast de beschikbare kennis die wordt verkregen naar aanleiding van incidenten en oefeningen op uiteenlopende wijze zoals berichten aan doelgroepen, producten (bijvoorbeeld het cyber kompas en het e-magazine) en conferenties.

Conclusie

Ik wil de WRR danken voor zijn bijdrage aan het debat over cybersecurity. Dit kabinet maakt werk van een groot deel van de adviezen van de WRR en neemt hierin ook de geleerde lessen van de Citrix-problematiek mee. De WRR wijst ons op belangrijke vraagstukken over digitalisering, de veiligheid van onze samenleving en de rol van de overheid hierin. Door versnelling van de ontwikkelingen op het gebied van dreigingen, technologie en afhankelijkheden worden deze vraagstukken de komende jaren alleen maar urgenter. Zoals ik ook in de inleiding van deze brief aangaf: cybersecurity kan niet gezien worden als een losstaand fenomeen. Het is integraal onderdeel van al onze maatschappelijke structuren en processen.

Cybersecurity is dan ook een prioriteit van dit kabinet en er zijn al veel belangrijke maatregelen in gang gezet bij de overheid, (vitale) bedrijven en andere organisaties. Naast op preventie moeten we ons richten op onze respons bij ernstige incidenten en crises. Onze fysieke en economische veiligheid zijn dermate afhankelijk van onze digitale veiligheid dat we ons hier geen vrijblijvendheid bij kunnen permitteren. Voor alle sectoren moet gekeken worden naar wet- en regelgeving om uitvoering, toezicht, verantwoording en evaluatie op cybersecurity mogelijk te maken. Dit geldt in het bijzonder voor als vitaal aangemerkte- en rijksoverheidsorganisaties. Uitval van systemen bij deze organisaties heeft immers al snel gevolgen voor alle burgers en bedrijven in ons land. In situaties waarbij er sprake is van een dreiging voor de nationale veiligheid moet de overheid bovendien in een uiterste geval in kunnen grijpen. De mogelijkheden hiertoe moeten duidelijk en toereikend zijn. Om onze digitale weerbaarheid te borgen zal de komende periode over de hele breedte meer geïnvesteerd moeten worden om de ontwikkelingen bij te kunnen houden. We zullen bovendien steeds kritisch moeten bekijken of het huidige instrumentarium en stelsel voldoende zijn.

Tot slot zal de Cyber Security Raad de komende periode een brede evaluatie van de aanpak van cybersecurity verrichten en onder meer aan de hand daarvan een advies geven over waar meer investeringen nodig zijn[20]. Hierover blijf ik uw Kamer informeren en blijf ik graag met uw Kamer in gesprek.

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

[20] Hiermee geef ik invulling aan de toezegging tijdens het AO-Cybersecurity 30 oktober 2019 (op verzoek van Kamerlid Verhoeven D66) om te bezien waar in de toekomst meer investeringen nodig zijn. Kamerstukken 26 643 en 30 821, nr. 650

Tabel Versterking Cybersecuritystelsel: Respons en Weerbaarheid

1. Slagvaardig handelen tijdens een crisis met digitale componenten
JenV/NCTV **inventariseert met betrokken departementen de wettelijke bevoegdheden voor de overheid bij digitale crisissituaties** (waaronder noodwetgeving), maakt het volledig instrumentarium inzichtelijk en beoordeelt of en waar eventuele aanvullingen nodig zijn.
De inlichtingen- en veiligheidsdiensten, politie, Defensie, BZ, OM, NCSC, betrokken vakdepartementen, veiligheidsregio's en de NCTV richten gezamenlijk een **geïntegreerd nationaal responskader** in met werkafspraken over handelwijze bij incidenten met digitale componenten.
De NCTV beziet jaarlijks of actualisatie van het **Nationaal Crisisplan Digitaal** nodig is.
Werkafspraken worden gemaakt over *pas toe of leg uit*-methodiek (Comply or Explain aan de verantwoordelijke Minister) **voor vitale aanbieders** bij dringende beveiligingsadviezen van het NCSC.
Voor Rijksoverheidsorganisaties komt er een *pas toe of leg uit*-**plicht** aan de CIO-Rijk bij dringende beveiligingsadviezen van het NCSC.
Er komt een risicomodel en een kwaliteitsregeling voor leveranciers van cybersecuritydiensten.

2. Effectief informatie uitwisselen over dreigingen en maatregelen
NCTV, NCSC, AIVD, MIVD, NP en OM richten gezamenlijk **operationeel samenwerkingsplatform in voor analyse van cyberincidenten- en dreigingen.**
Vakministers inventariseren waar blinde vlekken zitten binnen het Landelijk Dekkend Stelsel en stimuleren waar nodig **het oprichten van sectorale cybersecurityorganisaties**.
Een **handreiking LDS** wordt opgesteld waarin wordt ingegaan op de verschillende rollen binnen het stelsel en verantwoordelijkheden bij het doorgeleiden van beveiligingsadviezen.
Uitbreiding van krachtens de Wbni aangewezen sectorale cybersecurityorganisaties met als doel bredere informatiedeling vanuit het NCSC.
Inventarisatie **benodigde kaders en afspraken voor cybersecurity van decentrale overheden** (gemeenten, provincies en waterschappen).
Een handreiking met kaders en randvoorwaarden om alle rijksoverheidsorganisaties om doorlopend te scannen op kwetsbaarheden.

3. Toezicht en grip op de digitale weerbaarheid
De Inspectieraad wordt gevraagd om met een voorstel te komen hoe brede **samenwerking en afstemming tussen de rijksinspectie en toezichthouders op cybersecurity** het beste tot stand kan worden gebracht.
Cybersecurity afspraken worden onderdeel van «In-Control-verklaring» rijksoverheidsorganisaties.
De Inspectie JenV realiseert met alle betrokken toezichthouders een **periodiek inspectiebeeld cybersecurity vitaal.**
Deze zomer treedt de eerste wijziging van het Bbni inwerking, met daarin de nadere invulling van de zorgplicht in de Wbni voor aanbieders van essentiële diensten. Hiermee wordt **de zorgplicht aangescherpt** voor aanbieders van essentiële diensten.
Heel vitaal komt onder vol regime Wbni, hiermee geldt de zorg- en meldplicht voor elke vitale aanbieder. Uitzondering zijn hierbij gevallen waar de sectorale wetgeving strengere eisen stelt zoals in de telecom- en financiële sector.
Binnen **de versterkte aanpak bescherming vitale infrastructuur** zal aandacht zijn voor afhankelijkheden, keteneffecten, netwerken en toeleveranciers.

4. Oefenen
Cyberoefening ISIDOOR2020 met publieke en private partijen georganiseerd en voor het eerst in kabinetsverband – onder coördinatie van de NCTV. Nederland is initiator en gastland *Blue Olex*
EU-cyberoefening op bestuurlijk en strategisch niveau.
Aanbieders van essentiële diensten worden onder het Bbni **verplicht om hun crisismanagementbeleid** periodiek te oefenen.
Rijksoverheidsorganisaties worden verplicht om periodiek crisismanagementbeleid te oefenen en systemen te testen.