Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 738 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 februari 2021

Langs deze weg informeer ik uw Kamer over verschillende trajecten en toezeggingen die betrekking hebben op het thema digitale weerbaarheid. Dit zal gaan langs de volgende onderwerpen, die ik hier beneden nader toelicht:

1. Cybersecuritystelsel en governance
2. Informatiedeling vanuit de overheid
3. Interventiemogelijkheden van de rijksoverheid ten aanzien van vitale aanbieders en niet vitale organisaties in geval van digitale dreigingen en incidenten.
4. Ransomware

Aanleiding

Met deze brief geef ik een beleidsreactie op twee onderzoeken die in opdracht van het WODC zijn uitgevoerd, en waarvan ik de rapporten reeds aan uw Kamer heb aangeboden. Op 17 december 2020 heb ik u toegezegd een beleidsreactie te geven op het in opdracht van het WODC uitgevoerde onderzoek naar cybersecurity governance en vitale sectoren[1]. Hier zal ik op ingaan in hoofdstuk 1 van deze brief. Op 17 november 2020 heb ik u toegezegd een beleidsreactie te geven op het in opdracht van het WODC uitgevoerde onderzoek naar het Landelijk Dekkend Stelsel (LDS)[2]. Hier zal ik op in gaan in hoofdstuk 2 van deze brief. Hiermee kom ik tevens tegemoet aan de toezegging aan de Kamer uit het AO van 9 december 2020, om u te informeren over de voortgang van het LDS.

Daarnaast heb ik in de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» van 20 maart 2020[3] en de beleidsreactie CSBN

[1] Kamerstuk 26 643, nr. 732.
[2] Kamerstuk 26 643, nr. 717.
[3] Kamerstukken 26 643 en 30 821, nr. 673.

kst-26643-738
ISSN 0921 - 7371
's-Gravenhage 2021

2020[4] uw Kamer toegezegd in samenspraak met andere betrokken ministers, de huidige wettelijke taken en bevoegdheden van de overheid in kaart te brengen die het mogelijk maken informatie te delen met of in het uiterste geval in te grijpen op de digitale weerbaarheid bij rijksoverheid, vitale aanbieders en niet-vitale organisaties, en te bezien of aanvullingen hierop nodig zijn. Hier zal ik op in gaan in hoofdstukken 2 en 3 van deze brief. In dezelfde kabinetsreactie is tevens aangegeven dat de Staatssecretaris van Binnenlandse Zaken zal verkennen welke kaders en afspraken nodig zijn voor samenwerking tussen alle overheidsorganisaties, waaronder gemeenten, veiligheidsregio's, waterschappen en provincies. U zult in een afzonderlijke brief door de Staatssecretaris van BZK over de uitkomsten daarvan worden geïnformeerd. Tot slot zal ik in hoofdstuk 4 kort ingaan op de toezegging uit datzelfde AO rondom ransomware, en de toezegging over inzicht in systemen.

Inleiding

Het kabinet heeft cybersecurity als een prioriteit benoemd en heeft met het Regeerakkoord ingezet op een stevige aanpak hiervan. De kabinetsbrede aanpak van cybersecurity is vastgelegd in de Nederlandse Cyber Security Agenda (NCSA)[5]. De uitvoering van de maatregelen binnen deze agenda wordt ondersteund met investeringen die oplopen tot 95 miljoen euro op jaarbasis. Binnen de NCSA zijn deze kabinetsperiode substantiële stappen gezet om te werken aan de digitale weerbaarheid van Nederland. Hierover informeer ik uw Kamer via de jaarlijkse voortgangsrapportages, waarvan de meest recente in juni 2020 met uw Kamer is gedeeld[6].

Tegelijkertijd laat het Cybersecuritybeeld Nederland 2020 (CSBN 2020) zien de digitale dreiging permanent is, en dat allerlei actoren, inclusief statelijke actoren, het digitale domein misbruiken voor cyberaanvallen die onze maatschappij gedurende korte of langere tijd kunnen verlammen. Dat statelijke actoren deze intenties hebben blijkt ook uit het Dreigingsbeeld Statelijke Actoren[7]. Door de gevolgen van de COVID-19-pandemie is onze afhankelijkheid van digitale middelen verder toegenomen. Verhoging van de digitale weerbaarheid blijft de belangrijkste maatregel om deze risico's te beheersen. Ook in de toekomst zal een stevige inzet op digitale weerbaarheid noodzakelijk blijven.

De uitgevoerde verkenningen en WODC-onderzoeken dragen bij aan het vormgeven van die inzet. Ik zal hieronder verder ingaan op de verschillende verkenningen en onderzoeken langs de lijnen governance, informatie delen, en interventiemogelijkheden. De werkwijzen en methodiek zoals gevolgd voor de verkenning van wettelijke taken en bevoegdheden is toegelicht in de bijlage met de uitkomsten.

Inhoudelijke reactie verkenningen en rapporten

1. Cybersecuritystelsel en governance

De afgelopen jaren is een stelsel opgebouwd om de digitale weerbaarheid van Nederland te verhogen. Voordat wordt ingegaan op de gesignaleerde knelpunten en mogelijkheden tot doorontwikkeling volgt eerst een beschrijving op hoofdlijnen van dit stelsel.

---

[4] Kamerstuk 26 643, nr. 695.
[5] Kamerstuk 26 643, nr. 536
[6] Kamerstuk 26 643, nr. 695.
[7] Kamerbrief Dreigingsbeeld Statelijke Actoren, Kamerstuk 30 821, nr. 124

Beschrijving Nederlandse cybersecuritystelsel

De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity. De NCSA is opgesteld onder leiding van JenV, en wordt uitgevoerd onder coördinatie van JenV, met de vakdepartementen vanuit hun eigen specifieke verantwoordelijkheden. Ook is de Minister van JenV coördinerend bewindspersoon op het gebied van het stelsel voor crisisbeheersing, inclusief digitale crises.

Zoals in de NCSA is aangegeven, is een belangrijk uitgangspunt dat iedere private en publieke organisatie zelf primair verantwoordelijk is voor zijn eigen digitale beveiliging. Vanuit het oogpunt van nationale veiligheid zijn er echter processen en daarbinnen diensten waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Samen vormen de vitale processen de vitale infrastructuur. De aanbieders van genoemde diensten zijn daarom door de vakdepartementen aangewezen als vitale aanbieders. Voor verschillende van die vitale aanbieders geldt krachtens wetgeving (bijv. de krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni)[8] als aanbieders van een essentiële dienst (AED) aangewezen aanbieders) onder meer de verplichting om passende beveiligingsmaatregelen te nemen voor hun netwerk- en informatiesystemen (zorgplicht). Datzelfde geldt krachtens de Wbni ook voor (middel-)grote digitale dienstverleners, zoals aanbieders van cloudcomputerdiensten en online marktplaatsen. Daarnaast geldt er een meldplicht voor incidenten met (mogelijk) aanzienlijke gevolgen voor de continuïteit van de verleende dienst.

Op de naleving van de verplichtingen die voortkomen uit deze wetten (waaronder de Wbni) wordt toezicht gehouden door sectorale toezichthouders. Deze toezichthouders kunnen handhavend optreden (bijvoorbeeld door middel van een bindende aanwijzing of bestuursdwang) indien wettelijke verplichtingen niet worden nageleefd. Voor deze sectorale benadering is gekozen omdat toezichthouders beschikken over specifieke kennis en expertise over de onder hun toezicht vallende sectoren. Het toezicht op digitale veiligheid sluit daarmee aan op de al bestaande werkrelatie die toezichthouders hebben met aanbieders in hun sectoren.

Het Nationaal Cyber Security Centrum (NCSC) is het expertisecentrum voor cybersecurity in Nederland. Krachtens de Wbni heeft het NCSC primair tot taak om vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, adviseren en anderszins bijstand te verlenen. Daarnaast heeft het tot taak om dreigings- en incidentinformatie, die is verkregen in het kader van genoemde primaire taak, voor zover die relevant is voor andere aanbieders, te verstrekken aan bv. andere computercrisisteams, zodat zij organisaties in hun doelgroepen daarvan kunnen voorzien. Onder meer door het bevorderen van meldingen van organisaties uit de doelgroep van het NCSC (Rijk en vitaal) en het aangaan van samenwerkingsrelaties werkt het NCSC voortdurend aan de eigen informatiepositie en het op basis daarvan in het kader van genoemde taakuitoefening zo veel als mogelijk verstrekken van relevante informatie aan belanghebbende organisaties. Daarnaast publiceert het NCSC algemene beveiligingsadviezen op zijn website, die voor iedereen in Nederland toegankelijk is. Specifiek voor de reeds genoemde digitale dienstverleners zoals clouddiensten is er het CSIRT voor digitale dienstverleners.

[8] Met de Wbni is de Netwerk- en Informatiebeveiligings- (NIB-)richtlijn geïmplementeerd.

Ook voor organisaties die geen vitale aanbieder zijn of deel uitmaken van de rijksoverheid is digitale veiligheid van belang. Daarom heeft het kabinet sinds 2018 ingezet op de ontwikkeling van het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden, zodat ook die andere organisaties via het LDS zo goed mogelijk kunnen worden voorzien van relevante dreigingsinformatie. De ontwikkeling van dit stelsel moet leiden tot een netwerk van schakelorganisaties die kunnen adviseren en ondersteunen op het gebied van digitale veiligheid. Ik zal later in deze brief verder op het LDS en organisaties daarbinnen in gaan.

Om invulling te geven aan de taken en verantwoordelijkheden op het gebied van cybersecurity is er door het kabinet vanuit de NCSA geïnvesteerd in een stevige operationele basis om kennis op te bouwen bij het NCSC, de inlichtingen- en veiligheidsdiensten, de politie en andere overheidspartijen. Zo wordt verder bevorderd dat kennis over en inzicht in techniek, kwetsbaarheden, dreigingen en te beschermen belangen wordt opgedaan en gegenereerd, die ingezet kan worden voor bijvoorbeeld advisering in geval van cyberdreigingen en -incidenten. Hiervoor is een goede samenwerking tussen deze partijen van belang. Hiertoe is bijvoorbeeld de Cyber Intel/Info Cel (CIIC) ingesteld, waarbinnen verschillende overheidspartijen samenwerken om informatie over cyberincidenten en -dreigingen bijeen te brengen, te analyseren en waar aangewezen voor belanghebbende organisaties beschikbaar te maken.

Bevindingen WODC-onderzoek naar state-of-the-art cybersecurity

In opdracht van het WODC is er een onderzoek verricht naar de state-of-the-art van het cybersecuritydomein in Nederland. De onderzoekers komen tot vijf hoofdaanbevelingen aan de NCTV voor de doorontwikkeling van het Nederlandse cybersecuritystelsel. Ik zal deze aanbevelingen eerst benoemen, en er daarna puntsgewijs op ingaan.

Aanbevelingen uit het rapport:

1. De NCTV dient de rol van het onderscheid tussen vitale en niet-vitale infrastructuur binnen het Nederlandse beheersmodel nader te onderzoeken;
2. De NCTV moet verder onderzoek doen naar en investeren in proactieve en preventieve benaderingswijzen van nationale cybersecurity, die verder gaan dan het huidige, meer reactieve paradigma;
3. De NCTV zou verder onderzoek moeten doen naar de rol van minimale beveiligingsstandaarden en de mogelijke behoefte aan verdere nalevingsmechanismen;
4. De NCTV moet van de ontwikkeling van vaardigheden op het gebied van cybersecurity en engineering een hoge prioriteit maken voor de bescherming van de vitale sectoren in Nederland;
5. De NCTV moet de instrumenten ondersteunen om de risico's in verband met de supply chain van vitale infrastructuur aan te pakken.

Rol van vitaal (aanbeveling 1):

Zoals uw Kamer eerder is medegedeeld wordt er momenteel gewerkt aan een versterkte aanpak bescherming vitale infrastructuur. In de Kamerbrief over de voortgang van de aanpak Tegengaan Statelijke dreiging, die parellel aan deze brief is verzonden, zal ik u hier verder over informeren. Daarin wordt ook ingegaan op ketenafhankelijkheden.

Proactieve en preventieve aanpak cybersecurity (aanbeveling 2):

Zoals reeds hierboven aangegeven is het gezien de snelheid van technologische en maatschappelijke ontwikkelingen noodzakelijk om steeds te blijven streven naar het verbeteren van de cybersecurityaanpak, om deze zo adaptief mogelijk te maken. Hierom wordt onder andere intensiever ingezet op het nationale oefenprogramma om onze voorbereiding op ontwrichting proactief te oefenen. Dit past binnen inzet op het Nationaal Crisisplan Digitaal (NCP Digitaal). Daarnaast noemde ik eerder ook al de CIIC; met de hieraan deelnemende organisaties zal worden gekeken naar mogelijkheden om de samenwerking verder te versterken. Publieke-private samenwerking blijft een belangrijke pijler van de Nederlandse cybersecurity aanpak. Het belang van het blijven verbeteren van de cybersecurity aanpak geldt overigens niet alleen nationaal, maar ook op EU-niveau, bijvoorbeeld blijkens de recente EU voorstellen op digitaal gebied (zie ook onder kopje «Samenwerking binnen de Europese Unie»).

Minimumeisen voor cybersecurity (aanbeveling 3):

Ik onderschrijf het belang van minimumeisen op veiligheidsgebied, met name voor vitale aanbieders. Om die reden werkt het kabinet aan een aanpassing van het Besluit beveiliging netwerk- en informatiesystemen (Bbni), waarmee onder meer de zorgplicht voor AED's nader wordt ingevuld. De aanpassing van dit besluit bevind zich in een vergevorderde fase en is inmiddels in procedure gebracht. Daardoor zullen vakdepartementen ook de mogelijkheid krijgen om ministeriële regelingen op te stellen, om meer specifiek voor hun sectoren nadere regels ter invulling van genoemde zorgplicht te stellen. De Minister van IenW is bijvoorbeeld voornemens dat te gaan doen voor de sectoren luchtvaart, drinkwater en maritiem. Voor overheidsorganisaties geldt de Baseline Informatiebeveiliging Overheid (BIO). Tijdens het AO Cybersecurity op 9 december 2020 heb ik u toegezegd terug te komen op de inkoopeisen voor de overheid op het gebied van cybersecurity. Mede op basis van de eisen uit de BIO zijn voor op dit moment 11 segmenten de inkoopeisen cybersecurity (ICO) vastgesteld in een zogenoemde ICO-wizard.[9] Met behulp van de ICO-wizard kan elke overheidsorganisatie zelf bepalen welke inkoopeisen zij aan ICT-producten en -diensten moet stellen. De effectiviteit van de tool wordt momenteel in pilots getest. De pilots lopen door in 2021. Om een breed beeld te krijgen van de praktische uitwerking van de cybersecurity inkoopeisen wordt ingezet op het uitvoeren van pilots in alle overheidslagen (Rijk, provincies, gemeenten en waterschappen). De doelstelling blijft om deze cybersecurity inkoopeisen te gaan hanteren voor alle overheidslagen als een uitwerking van de Baseline Informatiebeveiliging Overheid (BIO). De tool is onderdeel van de Roadmap Digitaal Veilige Hard- en Software (DVHS) van het Ministerie van EZK en van de agenda NL DIGIbeter van het Ministerie van BZK. In de Roadmap DVHS worden verder stappen gezet op nationaal en Europees niveau om voor iedereen aantoonbaar veilige producten te stimuleren. Andere onderdelen hiervan zijn de ontwikkeling van Europese cybersecurity certificering voor ICT-producten, diensten en processen onder de *Cyber Security Act* en Europese wettelijke minimumeisen voor slimme apparaten via de *Radio Equipment Directive*. Over de voortgang van de Roadmap bent u in december door de Staatssecretaris van EZK geïnformeerd[10].

---

[9] De 11 inkoopsegmenten zijn: applicatieontwikkeling algemeen, clouddiensten, communicatievoorzieningen, DiGiD-applicaties, huisvesting IV, maatwerk of maatwerkpakket, middleware, mobiele applicaties, serverplatform, softwarepakketten en toegangsbeveiliging.

[10] Kamerstuk 26 643, nr. 735.

Investeer in kennisontwikkeling en de beveiliging van supply chains binnen de vitale infrastructuur (aanbevelingen 4 en 5):

In de Kamerbrief over de voortgang van de aanpak Tegengaan Statelijke dreiging wordt een toelichting gegeven op de versterkte aanpak vitaal. Investeren in kennisontwikkeling en het verbeteren van het inzicht in toeleveranciers en ketenafhankelijkheden zijn belangrijke onderdelen van deze versterkte aanpak. Daarnaast zal, in lijn met de motie van de leden Buitenweg en Yesilgöz-Zegerius[11] de komende periode in kaart worden gebracht wat er nodig is (qua mensen, middelen en expertise) om de structurele aanpak op telecom te verbreden naar andere vitale processen[12]. Hierbij gaat het enerzijds om het versterken van de sector-overstijgende expertise over risicoanalyses, strategische afhankelijkheden en informatiedeling. Daarnaast is het belangrijk om voor specifieke vitale processen in te zetten op de opbouw van diepgaande sectorale expertise. Kennis van Industrial Automation & Control Systems (IACS) moet hier inherent deel van uitmaken. Dit is zowel door RAND Europe gesignaleerd, maar bijvoorbeeld ook al door de CSR in hun advies over de digitale beveiliging van IACS binnen de vitale processen[13].

Concluderend kan worden gezegd dat de knelpunten die het rapport signaleert herkenbaar zijn en een belangrijke bijdrage leveren aan de doorontwikkeling van de cybersecurityaanpak in de komende jaren, en meer in het bijzonder taken, bevoegdheden en instrumenten op het gebied van cybersecurity van de overheid. Het huidige kabinet heeft op veel van deze terreinen reeds initiatieven ondernomen, zoals hierboven geschetst. Daarbij moet de kanttekening worden geplaatst dat veel van deze initiatieven nog relatief jong zijn en nog niet tot volledige wasdom zijn gekomen. De effectiviteit zal daarom pas op een later moment blijken. Om hier meer zicht op te krijgen werkt het WODC op dit moment ook aan een evaluatie van de NCSA (verwacht voorjaar 2021). Daarnaast heb ik de Cyber Security Raad (CSR) gevraagd om een advies uit te brengen over benodigde investeringen in cybersecurity voor een volgend kabinet (verwacht in februari 2021).

2. Informatiedeling vanuit de overheid

Voor het goed functioneren van het cybersecuritystelsel is een optimale uitwisseling van informatie over digitale dreigingen, kwetsbaarheden en incidenten tussen de overheid, vitale organisaties en niet-vitale organisaties van groot belang. Zoals eerder aangegeven, is het LDS een belangrijk instrument om die informatie-uitwisseling mogelijk te maken. Tegelijkertijd is het LDS een relatief jong onderdeel van de Nederlandse cybersecurityaanpak en is het stelsel nog steeds in opbouw. Vanwege de snelle ontwikkelingen op het digitale vlak blijft het nodig om te bezien of de ingezette koers de juiste is, en of het gerichte aanpassingen behoeft. Hiertoe is in opdracht van het WODC een onderzoek naar het LDS uitgevoerd. Ook de uitkomst van de verkenning naar wettelijke taken en bevoegdheden met betrekking tot het vanuit de overheid delen van dreigings- en incident informatie is van belang voor het LDS. Hieronder zal ik kort ingaan op de bevindingen, en geef ik een reactie op de opvolging daarvan.

---

[11] Motie van de leden Buitenweg en Yesilgöz-Zegerius, 35 570 VI, nr. 38.
[12] Kamerstuk 30 821, nr. 92.
[13] Cyber Security Raad, «Advies inzake de digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur van Nederland» (24 april 2020).

De schets van het LDS in het WODC-onderzoek geeft een accuraat beeld van de stand van zaken van het stelsel. Het onderzoek identificeert ook de behoeften daarbinnen en besteedt aandacht aan juridische mogelijkheden en beperkingen met betrekking tot informatiedeling binnen dit stelsel. Het formuleert ten slotte een drietal aanbevelingen.

Aanbevelingen uit het rapport

1. Creëer één loket voor alle MKB's en zzp'ers, in de vorm van het Digital Trust Center (DTC), en zet in op grootschalige marketing om de vindbaarheid van het DTC onder deze doelgroep te vergroten;
2. Zet in op het verspreiden van zogenaamde restinformatie[14] van het NCSC via het DTC naar samenwerkingsverbanden. Het DTC zou op termijn kunnen uitgroeien tot de primaire actor voor dreigingsinformatie voor niet-vitale organisaties. Hiervoor is het onder andere noodzakelijk dat het DTC een wettelijke grondslag verkrijgt op basis waarvan het persoonsgegevens kan ontvangen en verwerken;
3. Stimuleer samenwerking tussen de centrale partijen in het stelsel, met name tussen het NCSC en het DTC. Hier zouden ook andere informatieknooppunten binnen het LDS, bijvoorbeeld OKTT's en computercrisisteams zoals Z-CERT (zorg) en SURFcert (onderwijs en onderzoeksinstellingen), bij betrokken kunnen worden[15].

Vindbaarheid van het DTC (aanbeveling 1)

Voor de ondersteuning van het niet-vitale bedrijfsleven is binnen het Ministerie van EZK het Digital Trust Centre (DTC) ingericht. Het DTC kan daarmee op zich al voldoen aan de gesignaleerde informatiebehoefte. Dit jaar wordt door het Ministerie van EZK extra geïnvesteerd in communicatie om zo de vindbaarheid van het DTC en haar producten onder het MKB en zzp'ers te vergroten. Het DTC zal hierbij zowel inzetten op de eigen vindbaarheid als het benutten van de bij DTC aangesloten samenwerkingsverbanden en andere intermediaire organisaties die dicht bij de ondernemer staan. Uw Kamer is recentelijk door de Staatssecretaris van EZK geïnformeerd over de voortgang van het DTC[16]. Bij de eerstvolgende voortgangsrapportage zal ook aandacht worden besteed aan deze aanbeveling.

---

[14] Het NCSC heeft primair tot taak om informatie te verzamelen, analyseren en verstrekken in het kader van de bijstandverlening aan de doelgroep van rijksoverheid en vitaal. Daarnaast heeft het NCSC ook tot taak om «restinformatie» te verstrekken aan bijv. bij ministeriële regeling aangewezen andere computercrisisteams, indien daarmee nadelige maatschappelijke gevolgen kunnen worden voorkomen. Met «restinformatie» wordt in dit verband gedoeld op informatie over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen dan die van Rijk en vitaal, die het NCSC in het kader van zijn primaire taakuitoefening heeft verkregen.

[15] Een computercrisisteam is een gespecialiseerd team van professionals dat snel kan handelen bij beveiligingsincidenten met computers of netwerken. Een OKTT is een organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen. Als een organisatie krachtens de Wbni als computercrisisteam of OKTT is aangewezen, kan het, voor zover noodzakelijk, informatie over dreigingen en incidenten m.b.t. netwerk- en informatiesystemen van organisaties in de desbetreffende doelgroep van het NCSC ontvangen.

[16] Brief d.d. 16 december 2020

Verspreiding van restinformatie en samenwerking binnen het stelsel (aanbevelingen 2 en 3)

Het NCSC en het DTC werken vanuit hun onderscheidenlijke taken nauw samen om, met inachtneming van de hiervoor geldende wettelijke kaders, informatie te kunnen delen binnen het LDS. Ook werken ze zo veel als mogelijk samen om kennis(producten) en adviezen voor belanghebbende partijen te ontwikkelen en te delen, zoals de recent gelanceerde wegwijstool voor ondernemers. Om het niet-vitale bedrijfsleven in ruimere zin te kunnen doorzien van concrete dreigingsinformatie, wordt door het DTC momenteel een informatiedienst voor deze doelgroep ingericht en wordt door het Ministerie van EZK gewerkt aan het laten voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni als OKTT aangewezen kan worden, waaronder het versterken van de juridische basis door middel van een wetsvoorstel.

De informatie-uitwisseling binnen het LDS is niet enkel de verantwoordelijkheid van de overheid. Het stelsel werkt alleen effectief en efficiënt als bedrijven zichzelf organiseren in samenwerkingsverbanden, die beeld hebben van wat er speelt binnen een sector en kunnen inschatten welke informatie relevant voor hen is en hoe deze informatie kan worden vertaald naar concreet handelingsperspectief. Om die reden en gelet op de bevinding uit het onderzoek die aangeeft dat er bij de gespecialiseerde en meer volwassen bedrijven behoefte is aan (additionele) dreigingsinformatie in de Nederlandse context, zoals die momenteel beschikbaar is binnen de rijksoverheid, zal onder coördinatie van JenV worden blijven ingezet op het stimuleren en bestendigen van samenwerkingsverbanden, die eventueel ook aangewezen kunnen worden als OKTT of computercrisisteam. Een voorbeeld hiervan is Cyberveilig Nederland, een brancheorganisatie van de cybersecuritysector met op dit moment 61 leden, die in december krachtens de Wbni is aangewezen als OKTT. Mede hiermee wordt steeds gewerkt aan uitbouw van het Landelijk Dekkend Stelsel, zodat meer partijen toegang krijgen tot informatie over dreigingen en incidenten waaraan zij behoefte heeft, en tevens weten waar ze terecht kunnen in geval van vragen over of problemen met cybersecurity. Over de voortgang van het LDS zult u geïnformeerd worden in de voortgangsrapportage over de NCSA.

Bevindingen en opvolging verkenning wettelijke taken en bevoegdheden met betrekking tot informatie delen

Naar aanleiding van mijn eerdergenoemde toezegging heb ik de wettelijke taken en bevoegdheden van de rijksoverheid met betrekking tot het bij digitale dreigingen of incidenten verstrekken van informatie aan vitale aanbieders, niet-vitale organisaties en rijksoverheidsorganisaties in kaart gebracht en geïnventariseerd of en in welke zin aanvullingen hierop nodig zijn. Voor een overzicht van de wettelijke taken en bevoegdheden op het gebied van informatie delen verwijs ik u naar de bijlage bij deze brief[17].

Uit deze verkenning is gebleken dat er reeds diverse wettelijke taken en bevoegdheden zijn om vanuit de overheid informatie over digitale dreigingen en incidenten te kunnen delen met rijksoverheid, vitale en niet-vitale organisaties. Het NCSC heeft bijvoorbeeld tot taak organisaties binnen haar doelgroep (rijksoverheid en vitale aanbieders) te informeren en adviseren over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen, en is daarnaast bevoegd om dreigingsinformatie met betrekking tot systemen van andere aanbieders te delen met krachtens de Wbni aangewezen schakelorganisaties.

[17] Raadpleegbaar via www.tweedekamer.nl

Mogelijke wijzigingen Wbni

Zoals gezegd is voor het goed functioneren van het cybersecuritystelsel een zo optimaal mogelijke uitwisseling van informatie noodzakelijk. In aanvulling op alle reeds bestaande mogelijkheden, zoals beschreven in evengenoemde verkenning, ben ik met uw Kamer van mening dat obstakels bij informatiedeling door het NCSC onwenselijk zijn[18].

Tegen die achtergrond bezie ik of de artikelen 3 en 20 Wbni moeten worden gewijzigd. De eventuele aanpassing van artikel 20 Wbni ziet erop dat het NCSC aan OKTT's vertrouwelijke herleidbare informatie over aanbieders kan verstrekken, zodat deze schakelorganisaties belanghebbenden in hun doelgroep van relevante dreigings- en incidentinformatie kunnen voorzien. De eventuele aanpassing van artikel 3 Wbni ziet op het in bijzondere gevallen verstrekken van informatie door het NCSC aan individuele organisaties die niet deel uitmaken van de doelgroep van Rijk en vitaal. Ook andere mogelijke obstakels die gerelateerd zijn aan bijvoorbeeld de informatie-uitwisseling tussen instanties zullen worden bezien. Ik streef ernaar, gezien de urgentie van een digitaal veilig Nederland, dit traject met voorrang op te pakken.

3. Interventiemogelijkheden van de rijksoverheid ten aanzien van vitale aanbieders en niet-vitale organisaties in het geval van een potentiele crisis met digitale elementen

Zoals eerder aangegeven is iedere organisatie, zowel vitaal als niet-vitaal, in de eerste plaats zelf primair verantwoordelijk voor de eigen digitale beveiliging. Informatiedeling vanuit de overheid kan organisaties helpen om passende beveiligingsmaatregelen te treffen, bijvoorbeeld op basis van adviezen vanuit het NCSC, het CSIRT voor digitale diensten of het DTC. Opvolging van die adviezen door organisaties is ook primair de eigen verantwoordelijkheid van die organisaties zelf. In bepaalde gevallen zijn met name bepaalde categorieën vitale aanbieders echter gebonden aan verplichtingen met betrekking tot bijvoorbeeld het treffen van passende beveiligingsmaatregelen in wet- en regelgeving én wordt op de naleving van die verplichtingen toezicht vanuit de overheid gehouden en indien nodig bij niet-naleving in geval van cyberdreigingen of -incidenten geïntervenieerd.

In zijn rapport «Voorbereiden op digitale ontwrichting» wijst de WRR erop dat bij een incident met mogelijk digitale ontwrichting tot gevolg, de overheid in de respons afhankelijk is van de medewerking van private partijen. In een dergelijk geval zou de overheid adequate bevoegdheden moeten hebben om private partijen indien noodzakelijk te dwingen om mee te werken om maatschappelijke ontwrichting te voorkomen. In de kabinetsreactie op dit rapport heb ik daarom aangegeven om deze interventiemogelijkheden in kaart te brengen. In de bijlage vindt u de uitkomsten van deze verkenning.

Bevindingen en opvolging verkenning wettelijke taken en bevoegdheden met betrekking tot interventiemogelijkheden

De uitkomsten van de wettelijke verkenning laten zien dat er met name met betrekking tot vitale aanbieders een breed juridisch instrumentarium is om indien noodzakelijk te kunnen interveniëren. Specifiek als het gaat om crisissituaties verwijs ik u ook naar het Nationaal Crisisplan Digitaal[19].

[18] Aanhangsel Handelingen II 2020/21, nr. 955

[19] Dit plan is in februari met uw Kamer gedeeld als bijlage bij de Voortgangsbrief Agenda Risico en Crisisbeheersing (Kamerstuk 30 821, nr. 102).

Hierin is onder andere een beknopt overzicht opgenomen van de meest relevante wet- en regelgeving ten tijde van een crisissituatie, veroorzaakt in het digitale domein.

Ten aanzien van vitale aanbieders is er op basis van de verkenning geen reden om te concluderen dat er in de Wbni dan wel in sectorale wetgeving interventiebevoegdheden ontbreken. Toezichthouders kunnen op basis van deze wetgeving op zich op adequate wijze handhavend optreden, indien deze aanbieders niet voldoen aan de voor hen krachtens die wetgeving geldende verplichtingen, zoals de verplichting om passende beveiligingsmaatregelen te nemen.

Er wordt steeds gewerkt aan het verder verbeteren van het inzicht van toezichthouders in hun vitale sectoren binnen het huidige wettelijke stelsel. Zoals aangegeven in de kabinetsreactie op het WRR-rapport werkt het kabinet aan de uitwerking van «pas toe of leg uit». Dit betekent dat vitale aanbieders in ernstige gevallen, zoals bij bepaalde beveiligingsadvies van het NCSC[20], in het geval zij geen opvolging geven aan een advies, zij om uitleg gevraagd worden waarom zij dit niet doen. Over de precieze invulling hiervan informeer ik uw Kamer in de voortgangsbrief NCSA.

Uit de verkenning is ook gebleken dat de overheid ook mogelijkheden heeft om in te grijpen in buitengewone omstandigheden bij aanbieders die niet als vitaal zijn aangemerkt. Hiertoe dient noodwetgeving te worden toegepast, zoals onder meer geregeld in de Coördinatiewet uitzonderingstoestanden. Dit biedt vergaande mogelijkheden om te kunnen interveniëren door de rijksoverheid, zoals ten tijde van een noodtoestand. Het uitroepen van de noodtoestand, en daarmee de eventuele toepassing van vergaande bevoegdheden, is echter zeer ingrijpend.

Mede hierom is het nodig om steeds zorgvuldig te blijven kijken naar het bepalen van onze vitale processen en strategische belangen in relatie tot risico's die kunnen leiden tot maatschappelijke ontwrichting. Voor vitale aanbieders geldt immers, vanwege het vitale belang van de continuïteit van hun dienstverlening voor de samenleving, dat op basis van reguliere wetgeving kan worden geïntervenieerd ten behoeve van de digitale weerbaarheid als dit noodzakelijk is.

Samenwerking binnen de Europese Unie

Nederland is niet het enige land dat zich geplaatst ziet voor vraagstukken rondom digitale veiligheid. Ook op EU-niveau wordt er samengewerkt op dit onderwerp. In december heeft de Europese Commissie een nieuwe EU Cybersecurity Strategie gepresenteerd, inclusief een voorstel tot herziening van de NIB-richtlijn[21]. Dit voorstel zal gevolgen hebben voor nationaal cybersecuritybeleid en regelgeving. Over de inhoud van het voorstel en het kabinetsstandpunt ten aanzien van het voorstel wordt u verder geïnformeerd via een BNC-fiche.

4. Ransomware

In het AO Cybersecurity op 9 december jl. heb ik u toegezegd om na te gaan wat de omvang van incidenten met ransomware in Nederland is, en daarbij in kaart te brengen hoe vaak er sprake is van het betalen van losgeld.

---

[20] Classificatie *high/high* betekent dat de kans op misbruik groot is en de schade bij misbruik hoog wordt geacht.

[21] EU Cybersecurity Strategy, JOIN (2020) 18.

Uit een analyse van de politie blijkt dat in de jaren 2018, 2019 en 2020 (tot half december) er respectievelijk 180, 188 en 186 meldingen en aangiften van ransomware-aanvallen bij de politie zijn gedaan. Hierbij moet worden vermeld dat de meldings- of aangiftebereidheid van ransomware laag is. De politie registreert niet of er losgeld is betaald. In 2020 is in opdracht van EZK het Veilig Online onderzoek uitgevoerd. Hieruit blijkt dat van de bevraagde medewerkers en IT-verantwoordelijken bij bedrijven (zowel vitaal als niet-vitaal) tussen de 2% en 12% in het voorafgaande jaar te maken heeft gehad met ransomware[22]. Daarnaast is de bereidheid om te betalen bij ransomware-aanvallen bij bevraagde medewerkers en IT-verantwoordelijken groot. Om het inzicht in de prevalentie van ransomware onder burgers te vergroten wordt met het CBS gewerkt aan de aanpassing van de Veiligheidsmonitor[23]. Met betrekking tot ransomware-aanvallen bij publieke instellingen verwijs ik u naar de beantwoording van de schriftelijke vragen van het lid Van Raak[24].

Het kabinet zet zich actief in op preventie via het verhogen van de bewustwording en weerbaarheid van bedrijven en burgers. Zo biedt het Digital Trust Center (DTC) van het Ministerie van EZK verschillende kennisproducten aan met adviezen voor ondernemers om een besmetting met ransomware te voorkomen en adequaat te reageren als het toch gebeurt. Daarnaast biedt het DTC mogelijkheden om de cyberweerbaarheid van een bedrijf te testen middels een basisscan.

Conclusie en vooruitblik

Het kabinet heeft onder mijn coördinatie de afgelopen jaren belangrijke stappen gezet voor het verhogen van de digitale weerbaarheid via de NCSA. Dit heeft onder andere geleid tot de oprichting en uitbreiding van het Landelijk Dekkend Stelsel, het versterken van de kennispositie van en samenwerking tussen overheidsdiensten (via bijvoorbeeld CIIC), het in wetgeving vastleggen van regels over de beveiliging van netwerk- en informatiesystemen van vitale aanbieders, en de herijking van het NCP Digitaal om een stevige basis te creëren voor het bestrijden van digitale crises.

In al deze trajecten ben ik, maar ook de buitenwereld, steeds kritisch blijven kijken of we het goede doen, en wat beter kan en moet. We weten immers dat we afhankelijk zijn van digitale middelen voor alle aspecten van onze maatschappij en economie. We weten ook dat de digitale dreiging permanent is en de komende jaren zal blijven groeien. Stilzitten is daarom geen optie; we moeten onszelf scherp houden en ons instrumentarium blijven aanscherpen op basis van voortschrijdend inzicht. De verkenning naar wettelijke bevoegdheden en de rapporten waar deze brief op in gaat helpen hierbij. Tegelijkertijd leveren deze onderzoeken ook specifieke aandachtspunten op voor de toekomst, die ik hieronder zal benoemen. Deze bevindingen zouden meegewogen moeten worden in de verdere doorontwikkeling van het cybersecuritylandschap onder een nieuw kabinet.

De eerste is de digitale beveiliging van vitale processen. De komende periode wordt in kaart gebracht wat er nodig is om de structurele aanpak op telecom te verbreden naar andere vitale processen. De digitale

---

[22] https://www.rijksoverheid.nl/documenten/rapporten/2020/10/14/veilig-online-2020---medewerkers-bedrijfsleven

[23] De Veiligheidsmonitor is een periodiek bevolkingsonderzoek naar veiligheid en slachtofferschap van criminaliteit.

[24] Aanhangsel Handelingen II 2020/21, nr. 1383

beveiliging van de vitale processen zal hier naar verwachting een belangrijk onderdeel van zijn.

De tweede is de informatie-uitwisseling met niet-vitale organisaties. We zullen kritisch moeten blijven kijken naar datgene wat vitaal moet zijn, zodat vitale aanbieders bijvoorbeeld de benodigde informatie kunnen verkrijgen. Tegelijkertijd weten we ook dat niet alles vitaal verklaard kan worden. Daarom zullen we ook moeten blijven inzetten op de verdere ontwikkeling van het Landelijk Dekkend Stelsel, bijvoorbeeld via versterking van het DTC. Daarnaast moeten we blijven werken aan de verbetering van informatiedeling binnen het LDS. Daarbij hoort ook dat we telkens de daarop betrekking hebbende wetgeving blijven beoordelen.

Als derde is versterking van de operationele capaciteiten en samenwerking tussen operationele partijen noodzakelijk, inclusief het versterken van de informatie-uitwisseling met private partijen. Voor samenwerking tussen overheidspartijen is met de CIIC bijvoorbeeld reeds een belangrijke stap gezet. Hiermee kan de relevante informatie en kennis beter bij elkaar gebracht en verwerkt worden om vitaal en niet-vitaal van de benodigde informatie en advisering te kunnen voorzien.

De komende periode werk ik binnen de kaders van de NCSA verder aan de digitale weerbaarheid van Nederland. Ook in de toekomst zal het zaak zijn kritisch te blijven kijken naar de vraag of we de juiste dingen doen en of het bestaande instrumentarium daarvoor toereikend is.

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