Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 767

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 juni 2021

Hierbij bied ik uw Kamer het Cybersecuritybeeld Nederland 2021 (CSBN2021)[1] en mijn reactie hierop aan en informeer ik u over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA).

Cybersecuritybeeld Nederland 2021

In het CSBN2021 wordt opnieuw een ernstig beeld geschetst van de risico's voor de nationale veiligheid op het gebied van cybersecurity. Er zijn een aantal belangrijke nieuwe bevindingen:
- COVID-19 heeft het belang van veilige digitale processen vergroot.
- Cybercriminelen kunnen een risico vormen voor de nationale veiligheid.
- Experts signaleren grote verschillen in de weerbaarheid van organisaties. Zij vrezen dat deze weerbaarheidskloof steeds groter zal worden.
- Aanvallen schenden de veiligheid van de digitale ruimte, die kwetsbaar is voor uitval en misbruik. Het gaat hier bijvoorbeeld om het inbouwen van kwetsbaarheden in software die vervolgens via ICT-leverancierssketens wereldwijd verspreid wordt.

Het afgelopen jaar toonde wederom dat de digitale dreiging continu in ontwikkeling is. De digitalisering van onze samenleving en economie heeft met COVID-19 een vlucht genomen om op afstand te kunnen blijven werken, leren en ondernemen. Dit heeft onze afhankelijkheid van digitale processen verder vergroot. Deze ontwikkelingen bieden ook kansen voor kwaadwillenden. Zoals uit het CSBN2021 blijkt, zijn voorzieningen die gebruikt worden om op afstand met elkaar te kunnen werken en communiceren doelwit van digitale aanvallen. Zo waarschuwde het Nationaal Cyber Security Centrum (NCSC) in 2020 meerdere malen voor misbruik van kwetsbaarheden in VPN-verbindingen (vaak gebruikt voor thuiswerken) door statelijke en criminele actoren. Ook het hinderen van digitale processen, door het op slot zetten van systemen of bestanden met

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-26643-767
ISSN 0921 - 7371
's-Gravenhage 2021

gijzelsoftware, vindt plaats met soms langdurige gevolgen voor de continuïteit van processen binnen bedrijven, maatschappelijke organisaties en overheidsorganisaties. In december 2020 werd bijvoorbeeld de gemeente Hof van Twente getroffen door een ransomware-aanval, waardoor een deel van de dienstverlening van de gemeente tot stilstand kwam. Het uitvoeren van ransomware-aanvallen vormt al jaren een aantrekkelijk en solide verdienmodel voor criminelen. In het CSBN2021 wordt geconcludeerd dat cybercriminelen de nationale veiligheid kunnen raken, bijvoorbeeld wanneer zij vitale processen ontoegankelijk maken door middel van ransomware. Hoewel ze nog steeds andere intenties hebben, beschikt een aantal criminele groepen inmiddels over capaciteiten op een niveau dat niet onder doet voor het niveau van statelijke actoren. In de Kamerbrief Integrale Aanpak Cybercrime, die tegelijk met deze brief aan uw Kamer wordt aangeboden, wordt ingegaan op de aanpak van cybercriminaliteit.

Daar waar het statelijke actoren betreft is de digitale ruimte anno 2021 het speelveld van een geopolitieke krachtenstrijd. Digitalisering speelt een steeds belangrijkere rol in de verhouding tussen landen. Dit komt ook terug in het door de AIVD, MIVD en NCTV in februari 2021 gepubliceerde Dreigingsbeeld Statelijke Actoren[2]. Mede door deze geopolitieke strijd ontstaat een groeiende behoefte aan strategische autonomie. Wanneer kwaadwillenden aanvallen uitvoeren die de veiligheid van de digitale ruimte schenden heeft dit grote gevolgen voor het functioneren van alle digitale processen. Zo zijn er opnieuw geavanceerde aanvallen in de ICT-leveranciersketen met een mondiale impact aan het licht gekomen en zijn kwetsbaarheden in mondiaal gebruikte producten misbruikt. Er is vaak geen zicht op de mate van weerbaarheid van verschillende onderdelen van ICT-leveranciersketens, wat dit probleem weerbarstig maakt. Hoewel het CSBN2021 positieve ontwikkelingen in de verhoging van de weerbaarheid van Nederland signaleert, staat deze te vaak niet in verhouding tot de gesignaleerde dreiging. Er bestaan grote verschillen in weerbaarheid tussen organisaties, waardoor duurzame inzet op het verkleinen van deze verschillen van belang blijft. In het CSBN2021 wordt risicomanagement als relevant instrument gepresenteerd om de weerbaarheid van organisaties beter in kaart te brengen en aan de hand daarvan passende maatregelen te nemen.

Het belang van basismaatregelen

Uit het CSBN2021 blijkt opnieuw dat basismaatregelen bij veel organisaties ontbreken of nog onvoldoende zijn geïmplementeerd. Het gaat dan bijvoorbeeld om het gebruik van multifactorauthenticatie, tijdige patching en logging van netwerkverkeer. Het NCSC publiceert dit jaar gelijktijdig met het CSBN de Handreiking Cybersecuritymaatregelen, waarin belangrijke (basis)maatregelen worden beschreven die organisaties kunnen treffen. Dit biedt organisaties handvatten om hun weerbaarheid te verhogen. De handreiking wordt door het NCSC op zijn website gepubliceerd en is daarmee voor iedereen toegankelijk. De AIVD en de MIVD hebben daarnaast een brochure cyberspionage opgesteld, die ingaat op de maatregelen die genomen kunnen worden tegen spionage door statelijke actoren. Ook op de website van het Digital Trust Center (DTC) van EZK is informatie en advies beschikbaar die bedrijven helpt om beveiligingsmaatregelen te nemen.

[2] Kamerstuk 30 821, nr. 125.

De basis van de Nederlandse cybersecurityaanpak: de Nederlandse Cybersecurity Agenda

Cybersecurity is in het Regeerakkoord (Bijlage bij Kamerstuk 34 700, nr. 34) door het kabinet aangemerkt om met prioriteit te worden opgepakt. Om de digitale weerbaarheid van Nederland te verhogen en daadkrachtig te kunnen reageren op digitale dreigingen heeft het kabinet de NCSA opgesteld[3]. De NCSA geldt sinds 2018 als de basis voor de Rijksbrede inzet op het gebied van cybersecurity en is gekoppeld aan een structurele investering van 95 miljoen euro. In de NCSA werden zeven ambities gepresenteerd, met de volgende overkoepelende doelstelling: *Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.* De formulering van de zeven ambities van de NCSA laat ruimte om de agenda onderweg aan te vullen met extra maatregelen als de ontwikkeling van kennis, techniek en het dreigingsbeeld daarom vragen. Dit is dan ook op verschillende momenten gebeurd, onder andere naar aanleiding van het CSBN2019 en het WRR-rapport «Voorbereiden op digitale ontwrichting».

De afgelopen kabinetsperiode is hard gewerkt om invulling te geven aan deze ambities. U bent jaarlijks geïnformeerd over de voortgang van de uitvoering van de NCSA, maar ik licht er graag een aantal resultaten uit:

- In 2018 is de Wet beveiliging netwerk- en informatiesystemen (Wbni) in werking getreden. Hiermee is onder meer geregeld dat aanbieders van essentiële diensten (AED's) en digitale dienstverleners een plicht hebben om passende en evenredige technische en organisatorische maatregelen op het gebied van cybersecurity te nemen. Ook geldt voor hen een meldplicht voor incidenten met aanzienlijke gevolgen voor hun dienstverlening bij zowel de toezichthouder als het NCSC.
- In 2018 is bij het Ministerie van EZK het Digital Trust Center (DTC) opgericht. Met het DTC hebben bedrijven die geen vitale aanbieder zijn een aanspreekpunt op het gebied van cybersecurity. Het DTC deelt kennis en geeft advies en informatie waar bedrijven zelf mee aan de slag kunnen. Daarnaast ontwikkelt het DTC tools voor bedrijven zoals de basisscan en stimuleert het DTC samenwerkingsverbanden[4] op het terrein van cybersecurity.
- Met de Strategische I-agenda Rijksdienst 2019–2021, is ingezet op versterking van de rijksbrede informatiebeveiligingskolom[5]. Hiervoor is een nieuwe functie toegevoegd: Chief Information Security Officer Rijk (CISO Rijk). Daarnaast is met het Besluit CIO-stelsel Rijksdienst ingezet op het versterken van het CIO-stelsel[6].
- Door het opbouwen en versterken van een landelijk dekkend stelsel van cybersecurity-samenwerkingsverbanden kan informatie steeds breder, efficiënter en effectiever worden gedeeld tussen schakelorganisaties en organisaties in hun onderscheidenlijke doelgroepen. Verschillende schakelorganisaties zijn inmiddels krachtens de Wbni aangewezen als computercrisisteam of als een organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren (OKTT), waardoor zij meer informatie over dreigingen en incidenten die relevant is voor hun doelgroepen kunnen ontvangen van het NCSC. Daarnaast heeft het NCSC in enkele specifieke gevallen organisaties geïnformeerd en geadviseerd die geen deel uitmaken van de rijksoverheid of vitale infrastructuur om hen te beschermen tegen digitale dreigingen (bijv. politieke partijen gedurende de Tweede

[3] Kamerstuk 26 643, nr. 536.
[4] Op dit moment zijn er 36 van dergelijke samenwerkingsverbanden.
[5] Kamerstuk 26 643, nr. 591.
[6] Kamerstuk 26 643, nr. 739.

Kamerverkiezingen; de Minister van Binnenlandse Zaken en Koninkrijkrelaties heeft u recent hierover geïnformeerd[7]).
- Door middel van de extra investeringen in de inlichtingen- en veiligheidsdiensten is een beter beeld verkregen van de intenties, capaciteiten en activiteiten van statelijke actoren. Hierdoor is het inzicht in de dreiging gegroeid. De concrete dreigingsinformatie die dit oplevert is essentieel voor het bestrijden van kwaadwillende actoren.
- In 2020 is de Cyber Info/Intel Cel (CIIC) ingesteld, waarbinnen AIVD, MIVD, NCSC, OM en Politie dreigingsinformatie bijeenbrengen en medewerkers van deze organisaties deze informatie op één fysieke locatie bij het NCSC structureel gezamenlijk beoordelen. Hierdoor kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen belanghebbende organisaties meer en sneller van handelingsperspectief worden voorzien.
- Nederland heeft een leidende rol gespeeld bij het opzetten van het EU-cybersanctieregime in 2019 en de verlenging hiervan in 2021, om zo gezamenlijk de kosten van onwenselijk gedrag in cyberspace te verhogen.
- In 2019 is de Europese *Cybersecurity Act* in werking getreden. Deze verordening creëert een Europees stelsel van cybersecurity certificering voor ICT-producten, -diensten en -processen. De eerste Europese cybersecuritycertificeringschema's zijn in ontwikkeling. Nederland draagt met de Online Trust Coalitie, onder gebruikmaking van publieke en private expertise, bij aan de ontwikkeling van het certificeringsschema voor clouddiensten. Nederland implementeert de *Cybersecurity Act* via het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening voor het inrichten van het certificeringstelsel in Nederland en wijst Agentschap Telecom aan als de nationale autoriteit en toezichthouder. Het wetsvoorstel is aan uw Kamer aangeboden.
- De Europese richtlijnen over de verkoop van goederen en over de levering van digitale inhoud en digitale diensten zijn ook in 2019 aangenomen. Voor wat betreft cybersecurity is opgenomen dat consumenten recht krijgen op (veiligheids-)updates zolang zij die redelijkerwijs mogen verwachten. De richtlijnen zijn omgezet in het wetsvoorstel «Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud» en is 16 februari 2021 (Kamerstuk 35 734, nr. 3) aan uw Kamer aangeboden.
- Via diverse impulsen is de kennisontwikkeling en innovatie op het gebied van cybersecurity versterkt. Op basis van investeringen van diverse ministeries en NWO is voor 26 miljoen euro aan calls gerealiseerd en toegekend aan onderzoeks- en innovatieprojecten. Er is ook een nieuw publiek-privaat samenwerkingsplatform voor kennis en innovatie met betrekking tot cybersecurity opgericht, DCypher, om de samenwerking in de hele valorisatieketen te versterken. In de EU is een verordening aangenomen voor het oprichten van een Europees *Competence Centre* en het bijbehorende netwerk. Als nationaal onderdeel van dit netwerk wordt in Nederland een *National Coordination Centre* opgericht, en aangesloten op het samenwerkingsplatform.
- De Ministeries van JenV en EZK hebben diverse publiekscampagnes uitgevoerd, zoals «Eerst checken dan klikken» en «Doe je updates» om burgers bewust te maken van digitale risico's en om handelingsperspectief te bieden.

In de voortgangsrapportage die als bijlage is toegevoegd aan deze brief vindt u een overzicht met de concrete resultaten die na het versturen van de voorgaande Kamerbrief over de NCSA zijn behaald[8].

---

[7] Kamerstuk 35 165, nr. 40.

[8] Raadpleegbaar via www.tweedekamer.nl.

Resultaten evaluatie NCSA

De hierboven geschetste resultaten zijn erop gericht om de weerbaarheid van Nederland tegen cyberdreigingen te verhogen. Ontwikkelingen in het cyberdomein gaan echter snel en het is zaak om kritisch te blijven kijken naar wat we doen in het licht van de dynamische ontwikkelingen in het cyberdomein en aan de hand van nieuwe (wetenschappelijke) inzichten. Dat geldt ook voor de cybersecurityaanpak van dit kabinet in zijn geheel, zoals vastgelegd in de NCSA. Daarom heb ik het WODC gevraagd een evaluatie uit te voeren van de NCSA, zoals ook eerder aan uw Kamer is toegezegd[9]. Dit rapport van het WODC heb ik recent met uw Kamer gedeeld[10].

Het uitgevoerde evaluatieonderzoek bestaat uit een kritische reflectie op de beleidstheorie achter de NCSA en een verkenning naar de mogelijkheden voor een effectevaluatie. Hoewel in het rapport wordt geconcludeerd dat de opbouw van de NCSA via doelstellingen, ambities en maatregelen in algemene zin logisch is, constateert het rapport ook een aantal tekortkomingen in de beleidstheorie. Aan de hand van deze observaties worden er in het rapport verschillende aanbevelingen gedaan om de opbouw van een toekomstige cybersecuritystrategie beter in te richten.

De aanbevelingen uit deze evaluatie vormen belangrijke leerpunten voor het opstellen van nieuwe cybersecuritystrategieën in de toekomst. Hierbij is het zaak om in de voorbereidende fase op een nieuwe cybersecurityaanpak expliciet stil te staan bij de meetbaarheid van de (verwachte) effecten van de strategie, zodat er bij een toekomstige evaluatie meer zicht kan worden verkregen op de effectiviteit van cybersecuritybeleid. Een besluit over de opvolging van de NCSA zal moeten worden genomen door het volgende kabinet.

Inspectiebeeld

Naar aanleiding van het CSBN2019 heeft de Inspectie Justitie en Veiligheid aangegeven de oplevering van een jaarlijks onafhankelijk inspectiebeeld te coördineren. In dit beeld worden bevindingen van de verschillende toezichthouders en inspecties die toezicht houden op de naleving door vitale aanbieders van wettelijke verplichtingen op het terrein van cyber security bijeengebracht. Dit geeft inzicht in de staat van het toezicht en de weerbaarheid van vitale processen. De betrokken inspecties hebben het eerste openbare inspectiebeeld afgerond. Dit zal met uw Kamer gedeeld worden.

Vooruitblik

Het huidige CSBN en voorgaande beelden laten zien dat de dreiging zich continu blijft ontwikkelen. Door de adaptieve opzet van de NCSA heeft het kabinet in de afgelopen kabinetsperiode kunnen inspelen op deze veranderingen in het dreigingsbeeld en op technologische, maatschappelijke en geopolitieke ontwikkelingen. Hoewel belangrijke stappen zijn gezet om de digitale weerbaarheid te verhogen laat het CSBN2021 zien dat de weerbaarheid nog steeds achterblijft bij de digitale dreiging. Het kabinet blijft zich daarom inzetten om de Nederlandse digitale weerbaarheid te versterken. Daarbij schets ik voor de nabije toekomst een aantal belangrijke ontwikkelingen:

---

[9] Kamerstuk 26 643, nr. 536.
[10] Kamerstuk 26 643, nr. 763.

– Zoals vermeld in mijn antwoorden op vragen van het lid Yesilgöz-Zegerius van 29 maart 2021[11] werk ik aan een wetsvoorstel tot wijziging van de Wbni. Dit wetsvoorstel zorgt ervoor dat het NCSC meer dreigings- en incidentinformatie met betrekking tot de netwerk- en informatiesystemen van aanbieders (niet zijnde vitale aanbieders of aanbieders die deel uitmaken van de rijksoverheid) bij deze aanbieders terecht kan laten komen. Dit voorstel regelt dat het NCSC in bijzondere gevallen de hiervoor bedoelde informatie kan verstrekken aan deze aanbieders. Daarnaast regelt dit voorstel dat het NCSC ook aan OKTT's vertrouwelijke herleidbare informatie over aanbieders kan verstrekken, zodat deze schakelorganisaties aanbieders in hun doelgroepen van deze informatie kunnen voorzien. Ik streef ernaar dit wetsvoorstel rond de zomer in consultatie te brengen.
– Door het Ministerie van EZK wordt gewerkt aan het laten voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni als OKTT kan worden aangewezen, onder meer door het versterken van de juridische basis met een wetsvoorstel. Na aanwijzing zal het DTC gaan beschikken over meer dreigings- en incidentinformatie die met het niet-vitale bedrijfsleven kan worden gedeeld.
– Eind vorig jaar heeft de Europese Commissie de *EU Cyber Strategy* gepubliceerd, waarin onder andere een voorstel wordt gedaan voor een herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB, in Nederland geïmplementeerd in de Wbni). Daaraan gerelateerd heeft de Commissie ook een voorstel gedaan voor een nieuwe richtlijn voor de veerkracht van kritieke entiteiten *(Critical Entities Resilience Directive*; CER). Gezamenlijk richten deze voorstellen zich op het beschermen van voornamelijk vitale aanbieders tegen zowel digitale als fysieke dreigingen. Ook heeft de Commissie een voorstel gedaan om de cyber diplomatie toolbox verder te ontwikkelen. Dit voorstel richt zich op het aanpakken van onwenselijk gedrag in cyberspace dat grote gevolgen heeft voor de samenleving. U bent over deze voorstellen geïnformeerd via BNC-fiches.[12] In de komende periode zullen de lidstaten, het Europees Parlement en de Commissie deze voorstellen verder uitwerken.
– Zoals eerder gemeld[13] heeft het kabinet besloten voor de telecomsector een structureel proces in te richten waarin doorlopend nieuwe dreigingsinformatie kan worden gedeeld en op risico's worden beoordeeld door overheidsorganisaties en telecomaanbieders. Hierdoor kunnen snel en effectief maatregelen worden genomen als veranderingen in het dreigingsbeeld of technologische ontwikkelingen daarom vragen. Daarnaast zien we dat vanuit deze kennis en ervaring ook de sectoroverstijgende expertise kan worden versterkt, bijvoorbeeld op het gebied van risicoanalyses, strategische afhankelijkheden en informatiedeling. De komende periode wordt in kaart gebracht wat er nodig is (qua mensen, middelen en expertise) om deze vorm van structurele samenwerking op telecom te verbreden naar andere vitale processen, zoals landelijk transport, distributie en productie van elektriciteit (dat sterke intersectorale afhankelijkheden kent) en digitale overheid.

In het CSBN2021 komen daarnaast een aantal onderwerpen aan bod die in de komende periode aandacht zullen vragen. Het gaat dan onder meer om het vervagen van het onderscheid tussen de capaciteiten van een aantal groepen cybercriminelen en die van statelijke actoren, risico's die voortvloeien uit kwetsbaarheden met betrekking tot ICT-leveranciersketens, het vergroten van het inzicht in de digitale

[11] Aanhangsel Handelingen II 2020/21, nr. 2173.
[12] Kamerstuk 22 112, nr. 3053.
[13] Kamerstuk 30 821, nr. 92.

weerbaarheid van organisaties, het feit dat de digitale ruimte onderwerp is geworden van een geopolitieke krachtenstrijd en de bijbehorende roep om digitale soevereiniteit[14]. Gelet op deze ontwikkelingen, de permanente digitale dreiging en de toenemende afhankelijkheid van digitale middelen zal stevige inzet op het blijven versterken van de Nederlandse digitale veiligheid onder een nieuw kabinet noodzakelijk zijn. Dat wordt ook benadrukt in het rapport van de Cyber Security Raad «Integrale aanpak cyberweerbaarheid»[15], waarin een advies wordt gegeven over benodigde investeringen in cybersecurity aan het volgend kabinet.

Tot de beëdiging van een nieuw kabinet zullen wij onze acties blijven uitvoeren op basis van de NCSA en de latere aanvullingen daarop, waar uw Kamer over geïnformeerd is.

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

[14] Zie ook het advies van de Cyber Security Raad van 18 februari 2021: «Nederlandse Digitale Autonomie en Cybersecurity», https://www.cybersecurityraad.nl/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie.

[15] Zie CSR Adviesrapport «Integrale aanpak cyberweerbaarheid» | Rapport | Cyber Security Raad en Kamerstuk 26 643, nr. 752.