Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 614 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 juni 2019

Hierbij bied ik uw Kamer het Cybersecuritybeeld Nederland 2019 (CSBN2019)[1] en mijn reactie hierop aan en informeer ik u over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA).[2]

Het CSBN2019 schetst een zorgwekkend beeld. Er is sprake van een toenemende digitale dreiging. De dreiging die uitgaat van statelijke actoren groeit. Landen als China, Rusland en Iran hebben offensieve cyberprogramma's gericht tegen onder meer Nederland. Statelijke actoren zetten digitale middelen in voor spionage, verstoring en sabotage. Bovendien behoeft de blijvende dreiging die uitgaat van criminele actoren onverminderd onze aandacht. Laagdrempelige toegankelijkheid van digitale aanvalscapaciteit en de makkelijke schaalbaarheid zorgen voor een verhoging van de dreiging die uitgaat van beroepscriminelen, terwijl de opsporing en vervolging van daders complex is.[3] Daarbij zijn vrijwel alle vitale processen en diensten afhankelijk van ICT. Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen groot geworden. De digitale weerbaarheid dreigt bij deze ontwikkelingen achter te lopen.

[1] Raadpleegbaar via www.tweedekamer.nl

[2] Nederlandse Cybersecurity Agenda (Kamerstuk 26 643, nr. 536). Hiermee wordt tevens tegemoet gekomen aan het verzoek van het lid Laan-Geselschap in de RvW van 16 mei 2019 (Handelingen II 2018/19, nr. 83, item 7), raadpleegbaar via www.tweedekamer.nl.

[3] Over de voortgang van de Integrale Aanpak Cybercrime wordt u separaat en gelijktijdig geïnformeerd.

kst-26643-614
ISSN 0921 - 7371
's-Gravenhage 2019

Het CSBN2019 en andere rapporten[4] laten een beeld zien dat om actie vraagt. Cybersecurity is een complex grensoverschrijdend vraagstuk en dus is een kabinetsbrede inzet nodig. Met de implementatie van de eerste NCSA-maatregelen is een goede start gemaakt. Vanaf begin dit jaar is gestart met het aanwenden van de structurele aanvullende middelen van 95 miljoen euro voor cybersecurity die dit kabinet bij het Regeerakkoord (bijlage bij Kamerstuk 34 700, nr. 34) beschikbaar heeft gesteld. Bovendien heeft het kabinet eind 2018 incidenteel 30 miljoen euro extra vrijgemaakt, waarvan 10 miljoen voor cybersecurity en 20 miljoen voor de aanpak van digitale criminaliteit met speciale aandacht voor cybercrime en ondermijning. Door het nemen van maatregelen ontstaat steeds beter zicht op de aard en omvang van de dreiging. Dit bevestigt dat de voortzetting van de aanpak zoals aangekondigd in de NCSA en extra inspanning hard nodig zijn. Daarom wordt gezamenlijk met de betrokken vakdepartementen en onder mijn regie voor alle vitale sectoren ingezet op structurele en adaptieve risicobeheersing. Hiermee wordt verder invulling gegeven aan ambitie 7 van de NCSA om de regie op de kabinetsbrede aanpak te versterken. Concreet betekent dit:

1. Awareness – bewustwording van de risico's en het noodzakelijke niveau van de digitale weerbaarheid worden vergroot;
2. Beheersmaatregelen en toezicht – de digitale weerbaarheid wordt structureel verhoogd en het toezicht wordt versterkt;
3. Oefenen en testen – inzicht in de effectiviteit van genomen maatregelen;
4. Regie en interventie – partijen nemen hun verantwoordelijkheid en waar nodig wordt ingegrepen.

Om dit te realiseren werken de vakdepartementen en mijn ministerie (NCTV en NCSC)[5] intensief samen met de vitale aanbieders, toezichthouders en de inlichtingen- en veiligheidsdiensten. Hierbij hebben overheid en bedrijfsleven een gedeeld belang vanuit de continuïteit van de dienstverlening.

Awareness: bewustwording van risico's en weerbaarheid

De Nationale Veiligheid Strategie (NVS), waarover uw Kamer op 7 juni 2019 is geïnformeerd, laat zien dat digitale dreigingen alle nationale veiligheidsbelangen raken, omdat we vrijwel geheel afhankelijk geworden zijn van digitale middelen. Dreigingen in de digitale ruimte hebben ook een impact op de fysieke wereld. De toenemende digitale dreiging, onderlinge afhankelijkheden en de opkomst van nieuwe technologieën vereisen een risicogestuurde benadering van wat beschermd moet worden. De NCTV gaat vanuit mijn ministerie samen met de vakdepartementen opnieuw beoordelen welke belangen in de digitale ruimte het meest van invloed zijn op de nationale veiligheid en onderzoeken of organisaties voldoende bewust zijn van de kwetsbaarheden. Bovendien zal deze beoordeling periodiek plaatsvinden en waar nodig leiden tot aanpassing van of aanvulling op de NCSA of de NVS, waaronder bij de voorziene evaluatie van de NCSA in 2021.

---

[4] Algemene Rekenkamer «Digitale dijkverzwaring: cybersecurity en vitale waterwerken», Algemene Rekenkamer «Zicht op revolverende Fondsen van het Rijk» (Kamerstuk 31 865, nr. 133), brief Verstoring Russische cyberoperatie in Den Haag (Kamerstuk 33 694, nr. 21), brief Statelijke dreigingen (Kamerstuk 30 821, nr. 72), de Nationale Veiligheid Strategie 2019 (Kamerstuk 30 821, nr. 81), Jaarverantwoording politie 2018, *self-assessment* TNO vertegenwoordigers uit alle processen in de vitale infrastructuur 2018 (zie daarvoor ook de bijlage van deze brief).

[5] De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC)

Beheersmaatregelen en toezicht: verhoging veiligheidsniveau

Het veiligheidsniveau van vitale processen moet op orde zijn. Voor deze processen worden op basis van het meest actuele dreigingsbeeld beveiligingsdoelen opgesteld door de departementen, toezichthouders, inlichtingen- en veiligheidsdiensten en het NCSC in samenwerking met de vitale sectoren. Voor alle vitale processen wordt een basisniveau van fysieke en digitale beveiligingsdoelen vastgesteld en periodiek beoordeeld. Daarnaast werken alle sectorale toezichthouders vanuit de eigen expertise samen met het NCSC aan sectorspecifieke beveiligingsdoelen. Uitgangspunt hierbij is het meest actuele beeld van dreigingen en risico's van de NCTV, waarbij informatie van een groot aantal partners waaronder de opsporings-, inlichtingen- en veiligheidsdiensten gebruikt wordt. Hiermee ontstaat een dynamische werkwijze waarbij de beveiliging van vitale processen en daarmee de nationale veiligheid voorop staan. Voor de telecomsector zijn hiervoor in het 5G-traject van de Taskforce Economische Veiligheid reeds stappen gezet met betrokkenheid van telecombedrijven. Deze vorm van samenwerking kan als uitgangspunt dienen voor andere sectoren. Over het 5G-traject van de Taskforce Economische Veiligheid wordt uw Kamer apart geïnformeerd. Met deze werkwijze worden vitale partijen onder meer in staat gesteld om nadere invulling te geven aan de zorgplicht die uit onder andere de Wet beveiliging netwerken informatiesystemen (Wbni) volgt. Zo wordt geborgd dat vitale aanbieders, zowel publiek als privaat, hun verantwoordelijkheid kunnen nemen om de digitale weerbaarheid van Nederland naar een substantieel hoger niveau te brengen. Om ervoor te zorgen dat organisaties ook daadwerkelijk hun verantwoordelijkheid nemen en passende maatregelen treffen is effectief toezicht op digitale veiligheid noodzakelijk. Toezicht vormt een krachtig impuls voor vitale aanbieders om blijvend te werken aan een hoog niveau van digitale weerbaarheid en continuïteit. Toezichthouders moeten in staat gesteld worden om hun rol optimaal te kunnen vervullen. Vanuit mijn stelselverantwoordelijkheid, zal ik er samen met mijn collega ministers zorg voor dragen dat het geheel aan beveiligingsdoelen optimaal bijdraagt aan de nationale veiligheid. De NCTV heeft vanuit mijn ministerie daarin een adviserende rol. De Inspectie Justitie en Veiligheid draagt samen met andere Rijksinspecties zorg voor een samenhangend inspectiebeeld en onderlinge kennis en expertise tussen inspecties.

Oefenen en testen: inzicht in de effectiviteit van maatregelen

Dit kabinet stelt een breed, publiek-privaat, oefen- en testprogramma op. Door gezamenlijk te oefenen en te testen zorgen we ervoor dat onze digitale weerbaarheid structureel van voldoende niveau is. Met dit programma wordt inzichtelijk gemaakt welke best-practices relevant zijn voor andere sectoren. Hiermee kan maximaal leereffect bereikt worden. Door te oefenen en testen wordt duidelijk of de genomen maatregelen ook in de praktijk volstaan. Dat dit een effectief middel is om de sectorale weerbaarheid te verhogen bewijst bijvoorbeeld het Threat Intelligence Based Ethical Red Teaming (TIBER) project van De Nederlandsche Bank. Met het TIBER-testraamwerk worden geavanceerde hacktests gedaan met realistische scenario's op basis van actuele dreigingsinformatie. Daarnaast zorgt het programma ervoor dat organisaties en mensen in staat zijn om bij een daadwerkelijk incident snel en adequaat te kunnen handelen. De weerbarstigheid van cybersecurity maakt namelijk dat risico's nooit volledig kunnen worden weggenomen. Door goed voorbereid te zijn kan de impact van een incident echter worden beperkt. Zo wordt dit jaar voor de derde keer de grootschalige cyberoefening ISIDOOR met publieke en private partijen georganiseerd. Hiermee wordt het Nationaal Crisisplan ICT (NCP-ICT) in de praktijk getest. Het NCP-ICT wordt geactualiseerd en

aangepast aan de hand van de huidige inzichten en dreigingen. Het NCSC draagt vanuit zijn expertise bij aan de kwaliteit van het oefen- en testprogramma.

Regie en interventie: duidelijke verantwoordelijkheden en ingrijpen waar nodig

Het maatschappelijke belang van cybersecurity is voor zowel overheid als bedrijfsleven zo groot dat er op moet worden toegezien dat vitale organisaties hun verantwoordelijkheid nemen. Met het oog op de nationale veiligheid wordt onder regie van de NCTV de integraliteit van de genomen maatregelen bewaakt. De beoordeling hiervan dient samen met het actuele dreigingsbeeld als input voor de risicobeoordeling. Hierdoor kunnen nieuwe beheersmaatregelen worden getroffen daar waar ze het meest nodig zijn. Als stelselverantwoordelijke zal ik er samen met mijn collega bewindspersonen zorg voor dragen dat de betrokken partijen hier adequate opvolging aan geven. Indien dit onvoldoende gebeurt kan interventie nodig zijn. Wanneer vanuit mijn ministerie vitale partijen geadviseerd zijn maatregelen te nemen en geconstateerd wordt dat er onvoldoende of geen opvolging aan wordt gegeven en daardoor risico's op maatschappelijke ontwrichting aanwezig blijven, informeer ik op basis van de Wbni de voor de betrokken sector verantwoordelijke Minister of toezichthouder. Dit stelt vakdepartementen in staat om in het uiterste geval – na overleg – partijen op grond van hun wettelijke bevoegdheden via bijvoorbeeld een bindende aanwijzing alsnog maatregelen te laten nemen. Bij de evaluatie van de Wbni zal de effectiviteit van deze werkwijze worden bezien.

Nederlandse Cybersecurity Agenda

Met de implementatie van de eerste NCSA-maatregelen is een goede start gemaakt. Zoals ook aangekondigd in de «Geïntegreerde Buitenland- en Veiligheidsstrategie» wordt op Europees en internationaal niveau actief samengewerkt om de dreiging te verminderen, waar nodig met offensieve middelen.[6] Ook is op Nederlands initiatief een EU sanctieregime opgesteld.[7] Om de weerbaarheid verder te verhogen zet het kabinet in op extra inspanning voor de realisatie van de in de NCSA aangekondigde maatregelen en zal het bezien welke aanvullende maatregelen eventueel nodig zijn. Hieronder is uiteengezet hoe langs de ambities van de NCSA wordt gewerkt aan het structureel verhogen van de digitale weerbaarheid. In de bijlage bij deze brief is een rapportage op hoofdlijnen opgenomen over de voortgang van de NCSA sinds april 2018.

---

[6] Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS, Kamerstuk 33 694, nr. 12), brief Statelijke dreigingen (Kamerstuk 30 821, nr. 72)

[7] Uw Kamer wordt over de inzet op internationale vrede en veiligheid en het bestendigen van de internationale rechtsorde in het digitale domein voor het zomerreces geïnformeerd door de Minister van Buitenlandse Zaken.

Schematisch overzicht Voortgang Nederlandse Cybersecurity Agenda

1 – Digitale slagkracht op orde	
Terugblik	Gestart met extra investeringen in capaciteit en expertise bij onder meer NCSC, inlichtingen- en veiligheidsdiensten, opsporingsdiensten en Defensie. De inlichtingen- en veiligheidsdiensten zetten in op het verstoren van cyberoperaties gericht op Nederland. Uitbreiding detectiecapaciteit met Nationaal Detectie Netwerk (NDN). NCSC kan als informatieknooppunt binnen Landelijk Dekkend Stelsel informatie over kwetsbaarheden en dreigingen breder delen. Digital Trust Center (DTC) operationeel als «one stop cybersecurity-shop» voor niet als vitaal aangemerkt bedrijfsleven. CSIRT voor digitale dienstverleners operationeel. Aan de hand van de in 2018 gelanceerde «Defensie Cyber Strategie» investeert Defensie in cybercapaciteiten om op te kunnen treden tegen ernstige digitale bedreigingen.
Vooruitblik	Voortzetting investeringen in en werving van personeel en expertise betrokken organisaties. Er zal een verkenning worden uitgevoerd naar strafbaarstelling van spionage, waaronder in het digitale domein. Onder leiding van de AIVD wordt in interdepartementaal verband gewerkt aan de Nationale Cryptostrategie voor veilige communicatie. Komend jaar werkt defensie aan een nieuwe Defensienota 2020 die ingaat op de rol van defensie in het digitale domein in de toekomst.
2 – Internationale vrede en veiligheid in het digitale domein	
Terugblik	Ontwikkeling Diplomatiek Responskader. Defensie investeert in militaire cybercapaciteiten. EU-Cyber Diplomacy Toolbox doorontwikkeld/bestendigd. Cyberdiplomatennetwerk NL uitgebreid. Internationale uitwisseling van kennis en expertise actief bevorderd, onder meer via het Global Forum on Cyber Expertise. Het beschermen van mensenrechten online wordt gestimuleerd, onder meer via de Freedom Online Coalition.
Vooruitblik	Inwerkingtreding Europees cybersanctieregime. Kamerbrief internationale vrede en veiligheid in het digitale domein.
3 – Digitaal veilige hard- en software	
Terugblik	De EU *Cyber Security Act* is aangenomen. Cybersecurity risicomodel ontwikkeld voor bedrijven door Centrum voor Criminaliteitspreventie en Veiligheid (CCV).
Vooruitblik	Impact assessment van de *Radio Equipment Directive* opgeleverd door Europese Commissie. De ontwikkeling van Europese certificeringschema's zal naar verwachting dit jaar starten.
4 – Weerbare digitale processen en infrastructuur	
Terugblik	Inwerkingtreding Wet beveiliging netwerk- en informatiesystemen (WBNI), met daarin onder meer een zorg- en een meldplicht voor aanbieders van essentiële diensten en digitale dienstverleners. Self-assessment vertegenwoordigers vitale processen uitgevoerd om intersectorale afhankelijkheden in beeld te brengen. Baseline Informatiebeveiliging Overheid (BIO) voor harmonisering normenkaders informatiebeveiliging voor Rijk en medeoverheden. Gestart met opstellen Cybersecurity-eisenpakket voor overheidsinkoopbeleid om de digitale veiligheid van ICT-producten te bevorderen.

Vooruitblik	Nadere invulling zorgplicht Wbni. Vernieuwd Nationaal Crisisplan ICT wordt opgeleverd. Grootschalige oefening ISIDOOR III met private partijen om het Nationaal Crisisplan ICT in de praktijk te testen. In oktober organiseert BZK een cyberoefening voor de overheidslagen Rijk, provincies, gemeenten en waterschappen. Ontwikkeling en inrichting van een gezamenlijke faciliteit voor vulnerability scanning in samenwerking met CIO Rijk. Met als doel het controleren van alle systemen van de Rijksdienst die met het internet zijn verbonden op bekende kwetsbaarheden (onder coördinatie BZK). Uitwerking van eisen op het terrein van cybersecurity die relevant zijn voor het inkoopbeleid van alle overheidslagen. Versterkte bescherming vitale infrastructuur onder Nationale Veiligheid Strategie kabinet (NVS). IenW (her)beziet of sectoren transport over spoor en transport over weg als vitaal aangemerkt zouden moeten worden. In de tweede helft van 2019 worden de resultaten van deze vitaliteitsbeoordelingen verwacht. Vanuit de samenwerking van het addendum van het Bestuursakkoord Water worden instrumenten en technieken ontwikkeld om de watersector als geheel weerbaarder te maken tegen cyberdreigingen. Rijkswaterstaat ontwikkelt in samenwerking met de waterschappen een Baseline Informatiebeveiliging voor procesautomatisering.
5 – Barrières tegen cybercrime	
Terugblik	Met de inwerkingtreding van de wet Computercriminaliteit III zijn de opsporingsmogelijkheden van politie en justitie van cybercriminaliteit of dreigingen uitgebreid. In het versterken van de preventie zijn het verbeteren van cybersecurity en de aanpak van cybercrime het sterkst verweven. Bewustwordingscampagnes zoals Alert Online dragen hier aan bij (zie ook ambitie 6). Als onderdeel van de integrale aanpak cybercrime is in mei een bewustwordingscampagne over phishing gelanceerd.
Vooruitblik	In het najaar zal een vervolg aan deze campagne worden gegeven, waarbij de focus op digitale veilige hard- en software zal liggen. Een van de ambities van de NCSA is om succesvol barrières op te werpen tegen cybercrime. Met een voortvarende inzet op bovenstaande maatregelen worden deze barrières meer betekenisvol.
6 – Cybersecurity kennisontwikkeling	
Terugblik	Lancering Digitaliseringsagenda Primair en Voortgezet Onderwijs (OCW). Publicatie brede nationale cybersecurity onderzoeksoproep van 5,5 miljoen door Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) (oktober 2018). Bewustwordingscampagne Alert Online om veilig digitaal gedrag bij een breed publiek te stimuleren.
Vooruitblik	Curriculumherziening in het onderwijs onder de naam *Curriculum.nu* (streven 2021 gereed). Defensie voert samen met andere partijen een studie uit naar de opzet, vorm en organisatie van een in 2019 op te richten Cyber Innovation Hub.
7 – Integrale, publiek-private aanpak van cybersecurity	
Terugblik	Cybersecurity Alliantie gestart met concrete publiek private projecten (oktober 2018).
Vooruitblik	Herbeoordeling van welke belangen in (onder meer) de digitale ruimte het meest van invloed zijn op nationale veiligheid (onder coördinatie JenV/NCTV). Basislaag van fysieke en digitale beveiligingsdoelen wordt opgesteld voor de als vitaal aangemerkte belangen ten behoeve van sectoraal toezicht en de advisering van het NCSC. Het kabinet stelt een breed, publiek-privaat, oefen- en testprogramma op.

Conclusie

Het CSBN2019 schetst een zorgwekkend beeld. Cybersecurity is een complex grensoverschrijdend vraagstuk dat vraagt om een gezamenlijke aanpak door publieke en private partijen. De inzet van het kabinet is erop gericht dat Nederland op een veilige wijze de economische en maatschappelijke kansen van digitalisering verzilvert en de nationale veiligheid in het digitale domein beschermt. Door de eerste maatregelen van de NCSA ontstaat meer zicht op de aard en omvang van de dreiging en op het weerbaarheidsniveau. Het kabinet blijft met de NCSA werken aan een integrale aanpak van cybersecurity, zowel nationaal als internationaal. Vanuit mijn coördinerende rol voor nationale veiligheid en als stelselverantwoordelijke voor cybersecurity ga ik als onderdeel van de NCSA met een aanvullend pakket maatregelen regie voeren op het verhogen van de weerbaarheid en op verdere intensivering van de cybersecurity aanpak.

De ontwikkelingen van de afgelopen periode en het dreigingsbeeld laten zien dat dit hard nodig is. Over de voortgang blijf ik u periodiek informeren.

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