Voortgang Nederlandse Cybersecurity Agenda

Met de NCSA heeft het kabinet de koers voor de aanpak van cybersecurity in de komende jaren uitgezet. De eerste structureel aanvullende middelen die dit kabinet beschikbaar stelt zijn inmiddels vrijgekomen, waardoor er over de gehele linie gestart is met de implementatie van maatregelen. 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. De NCSA bevat zeven ambities om Nederland digitaal veilig te houden. Per ambitie worden op hoofdlijnen de voortgang sinds april 2018 en de maatregelen die het kabinet de komende periode neemt geschetst.

1. Digitale slagkracht op orde

Om digitale aanvallen op tijd te kunnen signaleren en een halt toe te kunnen roepen is van cruciaal belang dat de detectie- en responscapaciteit op orde is. Het kabinet investeert sinds dit jaar daarom extra in capaciteit en expertise bij het NCSC, inlichtingen- en veiligheidsdiensten, opsporingsdiensten en Defensie om de digitale slagkracht verder te vergroten. Het gaat daarbij onder meer om een significante uitbreiding van het aantal cybersecurityprofessionals en om investeringen in materiaal. Concreet is ten behoeve van het Nationaal Detectie Netwerk (NDN) de capaciteit uitgebreid. Doordat er het afgelopen jaar tientallen nieuwe partijen op het NDN zijn aangesloten, is het zicht op dreigingen ten aanzien van netwerken van de (rijks)overheid en vitale partijen verbeterd. Naast het verkrijgen van een beeld over de digitale dreiging zetten de inlichtingen- en veiligheidsdiensten in op het verstoren van cyberoperaties gericht op Nederland.

De verwevenheid van digitale processen en onderlinge afhankelijkheden maakt het noodzakelijk om zoveel mogelijk partijen continu te voorzien van de meest actuele dreigingsinformatie en handelingsperspectief. Het kabinet werkt toe naar een Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. Daarom zijn het afgelopen jaar stappen gezet om het bestaande stelsel van samenwerkingsverbanden te versterken en uit te breiden. Mede om aan de grotere behoefte voor informatie-uitwisseling binnen dit stelsel te kunnen voldoen, is ook de positie van het NCSC, zijnde het computercrisisteam en informatieknooppunt voor Rijk en vitaal, versterkt met een vergroting van de capaciteit. Verder is met de oprichting van het Digital Trust Center (DTC) begin 2018 een informatieknooppunt ingericht voor het niet als vitaal aangemerkte deel van het bedrijfsleven. Het DTC en het NCSC werken nauw samen om ter verhoging van de cyberweerbaarheid van de onderscheidenlijke doelgroepen zo veel als mogelijk informatie te kunnen ontsluiten. Het DTC helpt daarnaast bij de oprichting van cybersecurity samenwerkingsverbanden tussen bedrijven, zoals het cyberweerbaarheidscentrum Noord-Nederland (met name op het MKB gericht) en het cyberweerbaarheidscentrum Brainport Eindhoven (hightechindustrie). Bovendien is sinds 1 januari jl. het CSIRT[1] voor digitale dienstverleners operationeel, waarmee dienstverleners aanspraak kunnen maken op bijstand bij cyberincidenten.

Vooruitblik

De komende periode wordt de capaciteit van de inlichtingen- en veiligheidsdiensten verder vergroot en worden nog meer concrete acties genomen om de digitale slagkracht te verhogen. De investeringen in personeel en expertise bij betrokken organisaties worden voortgezet met de werving van meer deskundigen. Spionage via onder andere digitale middelen (op het Nederlands bedrijfsleven en andere instellingen door statelijke actoren) vraagt om een verkenning naar de strafbaarstelling van spionage waaronder in het digitale domein.
Daarnaast wordt met het oog op een toekomstbestendig systeem voor veilige communicatie momenteel onder leiding van de AIVD in interdepartementaal verband gewerkt aan de 'Nationale Cryptostrategie'.

[1] Computer Security Incident Response Team

2. Internationale vrede en veiligheid in het digitale domein

De grootste digitale dreiging voor Nederland gaat uit van statelijke actoren. Verschillende landen gebruiken digitale middelen om geopolitieke en economische doelstellingen te bereiken ten koste van Nederlandse belangen. Het kabinet zet daarom in op versterking van de internationale vrede en veiligheid en het bestendigen van de internationale rechtsorde in het digitale domein.

De hierboven geschetste versterking maakt onderdeel uit van de aanpak Statelijke Dreigingen, waarover uw Kamer in april jl. is geïnformeerd,[2] en van de 'Geïntegreerde Buitenland- en Veiligheid Strategie'. U zult separaat door de minister van Buitenlandse Zaken worden geïnformeerd over de toepassing van het bestaande internationaal recht op het digitale domein.[3]

In de internationale aanpak wordt nauw samengewerkt tussen verschillende overheidsorganisaties. Dat komt onder andere tot uiting in het ontwikkelde diplomatieke responskader bij cyberincidenten om Nederland minder aantrekkelijk te maken als doelwit van digitale aanvallen. Nederland werkt daarbij nauw samen met gelijkgezinde landen. De gecoördineerde respons na de verstoorde inlichtingenoperatie bij de OPCW is hier een voorbeeld van. Daarnaast is Europese samenwerking op dit terrein van groot belang, zoals het verder bestendigen van de *EU Cyber Diplomacy Toolbox*. Nederland blijft zich inzetten om ook via de EU de ambities uit de NCSA te realiseren. Gelet op de grote stappen die de EU recentelijk heeft gezet (onder andere *Cyber Security Act* en *EU Competence Centre*), richt de inzet zich komende periode op de implementatie, integratie en consolidatie van deze wet- en regelgeving.

Om de samenwerking met partnerlanden en de Nederlandse internationale positie verder te verstevigen, is er geïnvesteerd in het cyberdiplomatennetwerk. De eerste cyberdiplomaten zijn reeds actief. Ook blijft Nederland internationale uitwisseling van kennis en expertise met betrekking tot het digitale domein actief bevorderen, onder meer via het *Global Forum on Cyber Expertise*. De internationale aanpak ziet behalve op veiligheid ook op het beschermen van mensenrechten online, zoals via de *Freedom Online Coalition*.

De krijgsmacht vervult een belangrijke rol ten behoeve van de handhaving en bevordering van de internationale rechtsorde door deel te nemen aan militaire missies en operaties in bondgenootschappelijk verband. Het digitale domein zal in toekomstige conflicten een steeds belangrijkere rol spelen. Voor een effectieve uitvoering van de tweede hoofdtaak van de krijgsmacht in het digitale domein investeert Defensie de komende jaren verder in haar militaire cybercapaciteiten.

Vooruitblik

Doordat de cyberdreiging die uitgaat van statelijke actoren groeit, is het kabinet genoodzaakt om stevig in te zetten op internationale vrede en veiligheid in het digitale domein. De minister van Buitenlandse Zaken zal uw Kamer voor het zomerreces een brief sturen over internationale vrede en veiligheid en het bestendigen van de internationale rechtsorde in het digitale domein.

De nieuwe Defensienota, die gepland staat voor 2020, presenteert een visie en strategie die laat zien welke rol Defensie in de toekomst moet kunnen vervullen in onder andere het digitale domein.

3. Digitaal veilige hard- en software

Het is belangrijk dat iedereen kan vertrouwen op veilige ICT-producten en diensten. De opmars van *Internet of Things* (IoT)-apparaten brengt een versnelling aan in de digitalisering van onze samenleving en economie. Om de veiligheid van hard- en software en IoT te bevorderen is de 'Roadmap Digitaal Veilige Hard- en Software'[4] opgesteld. De afgelopen periode zijn belangrijke

[2] Kamerstuk 30 821, nr. 72

[3] Motie Verhoeven – Bruins Slot, Kamerstuk 33 694, nr. 35

[4] Kamerstuk 26 643, nr. 535

stappen gezet. Momenteel wordt er in EU-verband gekeken naar de mogelijkheden die de *Radio Equipment Directive* biedt om minimum digitale veiligheidseisen te stellen aan IoT-apparaten.

Met de *Cyber Security Act*, die in 2018 werd aangenomen binnen de EU, wordt een raamwerk gecreëerd voor de certificering van ICT-producten, -diensten en –processen. Nederland zet in op de voortvarende ontwikkeling en implementatie van cybersecurity certificeringschema's.

In opdracht van het ministerie van Justitie en Veiligheid (JenV) en het ministerie van Economische Zaken en Klimaat (EZK) en in samenwerking met diverse private partijen ontwikkelt het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een cybersecurity risicomodel voor bedrijven gekoppeld aan beschermingsmaatregelen. Daarnaast ontwikkelt het CCV een certificeringsschema voor cybersecurity diensten met een lijst van eisen die bedrijven kunnen stellen aan dienstverleners.

Vooruitblik
De ontwikkeling van Europese certificeringschema's zal naar verwachting dit jaar starten. Nederland zet de komende periode in op de voortvarende ontwikkeling en implementatie van cybersecurity certificeringschema's. Over de voortgang van alle maatregelen in de 'Roadmap Digitaal Veilige Hard- en Software' zal uw Kamer voor de zomer worden geïnformeerd door de staatsecretaris van EZK. Daarnaast zal de Europese Commissie in 2019 een impact assessment uitvoeren van de *Radio Equipment Directive*. De Nederlandse inzet is dat de Europese Commissie daarna overgaat tot het stellen van eisen, zodat op termijn voor alle met internet verbonden apparaten minimale digitale veiligheidseisen gelden.

4. Weerbare digitale processen en infrastructuur

De continuïteit en weerbaarheid van vitale processen is van cruciaal belang voor de Nederlandse samenleving. Daarom moet vol worden ingezet op het verhogen van de weerbaarheid. Door verschillende organisaties worden doorlopend maatregelen getroffen om de weerbaarheid van digitale vitale processen te verhogen.

Op 9 november jl. is de Wet beveiliging netwerk- en informatiesystemen (Wbni) in werking getreden. Deze wet heeft tot doel om de digitale weerbaarheid van Nederland - en in het bijzonder van die van vitale aanbieders, de Rijksoverheid en digitale dienstverleners - te verhogen, onder meer door een zorg- en meldplicht voor vitale aanbieders en digitale dienstverleners.
De organisaties, genoemd in de Wbni, zoeken, met inachtneming van de wettelijke kaders, ook samenwerking met andere organisaties, dit ter bevordering van hun taakuitoefening en het daardoor verder bevorderen van de digitale weerbaarheid van de samenleving. Zo is in april 2019 begonnen met het aanwijzen van organisaties waaraan onder bepaalde voorwaarden door het NCSC informatie kan worden verstrekt om hun doelgroep te informeren over digitale kwetsbaarheden en dreigingen.

Daarnaast zijn er na de Herijking Vitaal in 2015 een aantal acties gestart om vitale aanbieders en betrokken publieke partijen handvatten te geven om bij te dragen aan een beter beschermde vitale infrastructuur. Eén van de belangrijkste acties daarin is het in kaart brengen van de intersectorale afhankelijkheden in de Nederlandse vitale infrastructuur. In samenwerking met TNO is daar een methode voor ontwikkeld. Recent is een self-assessment uitgevoerd, welke op basis van die methode voor een eerste keer is uitgevoerd door vertegenwoordigers uit alle processen in de vitale infrastructuur. De opgehaalde informatie leverde een overkoepelend beeld op van de intersectorale afhankelijkheden, hetgeen tot belangrijke nieuwe inzichten heeft geleid. Zo wordt bijvoorbeeld aangegeven dat vitale processen in hoge mate afhankelijk zijn van de elektriciteitsvoorziening en datacommunicatie.[5]

[5] De gedetailleerde informatie van het *self-assessment* bevat bedrijfsgevoelige informatie en geeft een beeld van sterktes en zwaktes. Er zijn afspraken gemaakt met de betrokken departementen en aanbieders vanwege de vertrouwelijkheid en gevoeligheid van de informatie. Het is daarom niet mogelijk dit stuk openbaar te maken.

Om de weerbaarheid bij de overheid verder op peil te brengen heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) met het Rijk, provincies, gemeenten en waterschappen gewerkt aan het uniformeren en harmoniseren van normenkaders op informatiebeveiliging. Deze uniformering heeft zich geuit in de 'Baseline Informatiebeveiliging Overheid' (BIO). De BIO is eind 2018 vastgesteld en momenteel wordt deze geïmplementeerd bij verschillende overheidslagen.

Eveneens is begin dit jaar een start gemaakt met de uitwerking van eisen op het terrein van cybersecurity die relevant zijn voor het inkoopbeleid. De overheid wenst daarmee de digitale veiligheid van ICT-producten te bevorderen. Eerste concrete product dat voor de zomer van 2019 wordt opgeleverd betreft de uitwerking van het inkoopsegment softwareontwikkeling. Alle overheden (Rijk, provincies, gemeenten en waterschappen) dragen bij aan de inhoudelijke uitwerking van de betreffende inkoopsegmenten. Het gehele traject zal eind 2020 leiden tot de uitwerking van alle relevante ICT-inkoopsegmenten waarmee de digitale veiligheid van ICT-producten de juiste kant op wordt gestuwd binnen de gehele overheid.

Vooruitblik
Het komende jaar wordt het toezicht op de digitale weerbaarheid van vitale processen onder meer versterkt door nadere invulling van de zorgplicht uit de Wbni. Om ook goed voorbereid te zijn op grootschalige incidenten met onderlinge afhankelijkheden wordt komend najaar het vernieuwd 'Nationaal Crisisplan ICT' opgeleverd. Het in de bovenliggende brief genoemde gezamenlijke oefen- en testprogramma sluit hier op aan. Het crisisplan zal in samenwerking met private partijen in de praktijk getest worden tijdens de cyberoefening ISIDOOR III.

In oktober zal het ministerie van BZK bovendien een overheidsbrede cyberoefening organiseren voor de overheidslagen Rijk, provincies, gemeenten en waterschappen. Doelstelling is om te oefenen met cyberincidenten en de doelgroepen bestuurders, ambtelijke top, middenmanagement, (ICT)-professionals te voorzien van handelingsperspectief. Daarnaast wordt, onder coördinatie van het ministerie van BZK, een gezamenlijke faciliteit voor *vulnerability scanning* ontwikkeld en ingericht in samenwerking met CIO Rijk. Dat wil zeggen: het controleren van alle systemen van de Rijksdienst die met het internet zijn verbonden op bekende kwetsbaarheden.

Met de 'Nationale Veiligheid Strategie' ontwikkelt het kabinet bovendien een versterkte aanpak voor de bescherming van vitale infrastructuur. Onderdeel hiervan is een structuur om kennis, kunde en expertise te bundelen om tijdig in te kunnen spelen op actuele dreigingen. Risico's voor de nationale veiligheid ten behoeve van de vitale infrastructuur kunnen hierdoor ook in de toekomst adequaat worden geadresseerd.

Het ministerie van Infrastructuur en Waterstaat (IenW) (her)beziet of de sectoren transport over spoor en transport over de weg als vitaal aangemerkt zouden moeten worden. De resultaten van deze vitaliteitsbeoordelingen worden in de tweede helft van 2019 verwacht. Verder worden door IenW vanuit de samenwerking van het addendum van het 'Bestuursakkoord Water' instrumenten en technieken ontwikkelt om de watersector als geheel weerbaarder te maken tegen cyberdreigingen. Daarnaast zet Rijkswaterstaat zich, in samenwerking met de waterschappen, in om een 'Baseline Informatiebeveiliging voor procesautomatisering' te realiseren.

5. Barrières tegen cybercrime
Cybercriminelen, al dan niet in samenwerking met statelijke actoren, krijgen steeds makkelijker toegang tot geavanceerde aanvalsmiddelen. Het CSBN2019 laat zien dat de opkomst van "cybercrime as a service" doorzet. Door het gebruik van cybercrime as a service hebben kwaadwillende geen hoog kennisniveau nodig om een aanval uit te voeren. Andere dreigingen die worden genoemd in het CSBN zijn bijvoorbeeld phishing en ransomware-aanvallen. De noodzaak voor de aanpak van cybercrime blijft onverminderd hoog. Onderdeel van de aanpak is het opwerpen van barrières tegen cybercrime om te voorkomen dat mensen of bedrijven slachtoffer

worden. De maatregelen uit de NCSA spelen hierbij een belangrijke rol. Wanneer bijvoorbeeld hard- en software beter wordt beveiligd, zoals genoemd in ambitie 3, is de kans kleiner dat gebruik wordt gemaakt van producten om cybercriminaliteit te plegen. Daarnaast is kennisontwikkeling, zoals verwoord in ambitie 6, van groot belang om de maatschappij weerbaarder te maken in het digitale domein. In het versterken van de preventie zijn het verbeteren van cybersecurity en de aanpak van cybercrime het sterkst verweven. Een concreet voorbeeld van preventie is de bewustwordingscampagne tegen phishing die eind mei is gelanceerd. Deze campagne zal verder toegelicht worden in de voortgangsbrief integrale aanpak cybercrime. De voortgangsbrief van de integrale aanpak cybercrime wordt gelijktijdig met de bovenliggende brief verstuurd en zal, naast het voorkomen van strafbare feiten, ingaan op het opsporen, vervolgen en verstoren, internationale samenwerking en het beperken van slachtofferschap, daderschap en recidive.

6. Cybersecurity kennisontwikkeling

De cyberdreiging vraagt van de samenleving dat burgers in voldoende mate om kunnen gaan met de verregaande digitalisering. Dat brengt een intensivering op de thema's onderwijs, kennisontwikkeling en awareness met zich mee. Naast aandacht voor digitale vaardigheden in den brede is er een groeiende behoefte aan cybersecurityprofessionals.

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft op 21 maart jl. de digitaliseringsagenda voor het primair en voortgezet onderwijs gelanceerd met onder meer als doel leerlingen van jongs af aan digitaal vaardig te maken.

Uw Kamer wordt door de staatssecretaris van EZK op korte termijn geïnformeerd over de eerste bevindingen uit de verkenning die is gestart naar cybersecurity kennisontwikkeling. Via deze verkenning wordt onderzocht hoe zowel fundamenteel als toegepast cybersecurity onderzoek versterkt kan worden. Daarop vooruitlopend zijn er inmiddels al investeringen gedaan om cybersecurity onderzoek te stimuleren. Zo is via de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO) een brede nationale cybersecurity onderzoeksoproep gepubliceerd van 5,5 miljoen euro.

Door het ministerie van JenV wordt in samenwerking met het ministerie van EZK eveneens ingezet op het creëren van meer bewustwording over veilig digitaal gedrag bij een breed publiek, bijvoorbeeld middels de recent gestarte campagne over phishing. Doordat JenV en EZK hun campagnes in samenhang ontwikkelen wordt het gewenste effect vergroot. Ook het bestaande platform Alert Online, waarvan het aantal partners afgelopen jaar is toegenomen, draagt bij aan bewustwording. In oktober zal de jaarlijkse campagne Alert Online plaatsvinden. Komende periode wordt bezien in welke vorm Alert Online na 2019 het meest effectief wordt voortgezet.

Vooruitblik

Door teams van leraren en schoolleiders wordt onder de naam *Curriculum.nu* gewerkt aan een curriculumherziening in het onderwijs. In het leergebied 'digitale geletterdheid' hebben mediawijsheid en cybersecurity een duidelijke plaats. Het streven is om in 2021 een voorstel voor nieuwe kerndoelen aan uw Kamer te verzenden.

Via de NWO wordt komende periode een oproep van 5,15 miljoen euro uitgewerkt in het kader van de Nationale Wetenschapsagenda (NWA). Daarnaast zal cybersecurity stevig worden verankerd binnen het missiegedreven innovatiebeleid. Daarmee wil het kabinet de innovatiekracht van de topsectoren gebruiken om onder andere cyberuitdagingen aan te pakken én de concurrentiekracht van ons land te versterken.

Defensie voert samen met een aantal andere partijen een studie uit naar de opzet, vorm en organisatie van een in 2019 op te richten *Cyber Innovation Hub*, waarin departementen, onderzoeksinstellingen en bedrijven samenwerken aan gezamenlijke en geprioriteerde veiligheidsvraagstukken op het gebied van cyber. Het doel van de *Cyber Innovation Hub* is

cyberkennis en -kunde in Nederland te versterken, innovaties en experimenten te faciliteren en een ecosysteem van partners te bouwen, om zo bij te dragen aan het reduceren van cyberdreigingen.

7. Integrale, publiek-private aanpak van cybersecurity
De bovengenoemde ambities vragen om samenwerking en regie. Zowel in het brede publieke domein als tussen private en publieke partijen, nationaal en internationaal, wordt op verschillende manieren intensief gewerkt om de doelstellingen van de NCSA te bereiken. Deze samenwerking wordt onder andere vormgegeven door de publiek-private Cybersecurity Alliantie, waarmee eind 2018 is gestart. Daarin wordt gewerkt aan kortlopende concrete projecten. Een voorbeeld hiervan is het project dat de bredere toepassing van het eerder genoemde TIBER-raamwerk onderzoekt.

Daarnaast wordt – zoals geschetst in de bovenliggende Kamerbrief – onder mijn regie door dit kabinet ingezet op structurele en adaptieve risicobeheersing. Hiermee wordt de integrale publiek-private aanpak van cybersecurity voor nationale veiligheidsbelangen versterkt en ingezet op een structurele verhoging van de digitale weerbaarheid.