Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1025

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 mei 2023

Op 10 oktober 2022 is de kabinetsbrede Nederlandse Cybersecuritystrategie (NLCS) aangeboden aan uw Kamer (Kamerstuk 26 643, nr. 925). Hierin is aangegeven dat begin 2023 een model wordt ingericht om integraal te kunnen sturen op een voortvarende implementatie van de strategie in nauwe samenwerking tussen publieke, wetenschappelijke en private partijen. In het debat van 15 december 2022 met de Commissie voor Digitale Zaken van uw Kamer heb ik toegezegd uw Kamer te informeren over dit sturingsmodel.[1] Met deze brief voldoe ik aan deze toezegging.

Cybersecurity is een belangrijke randvoorwaarde voor een veilige, veerkrachtige en steeds verder digitaliserende en innoverende maatschappij. In de NLCS staan de doelstellingen van het kabinet om te komen tot een digitaal veilig Nederland en de acties die nodig zijn om deze te bereiken. Vrijwel alle bewindspersonen hebben een verantwoordelijkheid om bij te dragen aan de realisatie van de NLCS en zijn (mede)eigenaar van acties om dit te bereiken. Zij zijn ook verantwoordelijk om dit samen te doen met (mede)overheden, wetenschap, burgers en private partijen, daar waar dit kan bijdragen aan de realisatie van de NLCS.

Sturingsmodel en regie

Digitale veiligheid behoeft prioriteit op het hoogste niveau. Leiderschap, regie en eigenaarschap zijn daarbij cruciaal. De sturing op de implementatie van de NLCS is daarom belegd in de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV) als onderraad van de ministerraad. Cybersecurity is daar een vast thema dat in samenhang besproken wordt met andere veiligheidsvraagstukken en strategische thema's zoals open strategische autonomie en digitalisering. De voorbereiding van deze sturing en bespreking op ministerieel niveau wordt

[1] Kamerstuk 26 643, nr. 961.

kst-26643-1025
ISSN 0921 - 7371
's-Gravenhage 2023

gedaan in de ambtelijke Commissie Defensie, Internationale, Nationale en Economische Veiligheid (CDINEV).

Als coördinerend bewindspersoon op cybersecurity ben ik verantwoordelijk voor een optimale werking van het cybersecuritystelsel en voer ik regie op de implementatie van de strategie door te faciliteren, te ondersteunen en te stimuleren. Ik treed daarbij vanzelfsprekend niet de in verantwoordelijkheid van andere bewindspersonen. U kunt van mij verwachten dat ik over grenzen heen verbinding legen de samenhang bewaak tussen de verschillende thema's en verantwoordelijkheden. Ik heb onder voorzitterschap van de NCTV een ambtelijke sturing ingericht, met mede eigenaren van de acties. Deze stuurgroep zet zich gezamenlijk in, vanuit structureel inzicht in de voortgang, voor een voortvarende implementatie van de strategie en effectieve samenwerking tussen publieke, wetenschappelijke en private partijen.

Jaarlijkse bijstelling en rapportage over de voortgang

Om in te kunnen spelen op trends, actuele dreigingen en risico's, worden de acties uit de NLCS in de loop van de tijd uitgewerkt, aangepast of versterkt. Het actieplan kan daarom jaarlijks op punten worden geactualiseerd, waardoor adequaat ingespeeld kan worden op de snelle ontwikkelingen in relatie tot digitale veiligheid en bijgestuurd kan worden als daar aanleiding toe is.

Mogelijke aanleidingen kunnen gesignaleerd worden door het jaarlijkse Cybersecuritybeeld Nederland (CSBN) wat een actueel beeld geeft van de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en digitale risico's. Daarnaast kunnen inzichten van publieke, private- en wetenschapspartijen ook reden zijn voor bijsturing. Zij worden jaarlijks betrokken bij een toets of zij ontwikkelingen zien die aanleiding kunnen vormen voor bijstelling. Dit kan daarnaast verwoord zijn in nationale dan wel internationale rapporten of adviezen die gedurende de looptijd van de NLCS worden uitgebracht. Tot slot wordt de Cyber Security Raad (CSR) jaarlijks om advies gevraagd over strategische ontwikkelingen die volgens hen meegewogen moeten worden.

Uw Kamer wordt jaarlijks geïnformeerd over de eventuele bijstelling van de NLCS en de voortgang. De eerste voorgangsrapportage ontvangt u in het najaar van 2023. Uw Kamer wordt jaarlijks geïnformeerd over de eventuele bijstelling van de NLCS en de voortgang. De eerste voorgangsrapportage ontvangt u in het najaar van 2023. Ik ben voornemens in deze eerste voortgangsrapportage de acties waar nodig en mogelijk meer uit te werken, te verbinden aan een concreter tijdpad en/of de meetbare realisatie van de doelstellingen.

Samenwerking rondom de implementatie van de NLCS

Voor een voortvarende implementatie van specifieke acties en deelonderwerpen is het van belang dat er samengewerkt wordt met (mede)overheden, wetenschap, burgers en private partijen. Zij worden niet alleen betrokken bij de afweging of bijstelling van het actieplan aan de orde is. De samenwerking rondom de acties kent verschillende vormen en varieert in intensiteit. Zo wordt bijvoorbeeld voor het programma Cyclotron een governance board ingericht waar zowel publiek, privaat en wetenschap medeverantwoordelijk zijn voor de ontwikkeling van het informatiedelings- en samenwerkingsplatform en de uitwerking van

juridische en technische vraagstukken hieromheen.[2] Private partijen nemen deel aan de nationale oefening ISIDOOR en in aanvulling daarop aan diverse sectorale en lokale oefeningen. Een laatste belangrijk voorbeeld is dcypher. Dat is het samenwerkingsplatform voor onderzoek en innovatie op het gebied van cybersecurity in Nederland. Dcypher brengt publieke, private partijen en kennisinstellingen bij elkaar evenals middelen en expertise om effectief te kunnen inzetten op cybersecurity onderwijs, onderzoek, innovatie voor de ontwikkeling van concrete toepassingen. Per actie uit het actieplan wordt dus, daar waar relevant, gekeken naar de wijze waarop de samenwerking met de private sector en andere partijen het beste vorm gegeven kan worden.

Met de uitvoering van de voorloper van de NLCS, de Nederlandse Cybersecurity Agenda (NCSA), is binnen de Cybersecurity Alliantie (CSA) in publiek-privaat verband samengewerkt rondom cybersecurity thema's en grote en kleine organisaties zijn met diverse tools en producten ondersteund. Enkele mooie voorbeelden zijn onder andere het cybersecurity woordenboek, de oefentool en een checklist voor industriële controlesystemen die maatregelen beschrijft tegen de meest voorkomende kwetsbaarheden en adviezen geeft hoe beveiligingsproblemen kunnen worden aangepakt en voorkomen (de ICS-SCADA tool). De Cybersecurity Alliantie is afgesloten met het oog op de vernieuwde samenwerking rondom de NLCS. De positieve ervaringen en producten van de Alliantie worden hierin meegenomen en geborgd.

Met de NLCS samenhangende strategieën

Naast dat de NLCS de kabinetsdoelstellingen en de acties op dit terrein weergeeft vormt het ook een duidelijk kader aan de hand waarvan het cybersecuritybeleid zich op alle niveaus samenhangend en gestructureerd ontwikkelt. Diverse bewindspersonen hebben de NLCS vertaald naar specifiek (sectoraal) beleid ten behoeve van bijvoorbeeld het verhogen van de digitale weerbaarheid van de organisaties en processen waar zij een systeemverantwoordelijkheid voor dragen of om nadere invulling te geven aan hun specifieke verantwoordelijk op het gebied van of rakend aan cybersecurity.

Cybersecuritybeleid maakt ook soms onderdeel uit van bredere strategieën. Een aantal van deze strategieën of plannen heeft uw Kamer reeds ontvangen, zoals de Werkagenda Waardengedreven Digitaliseren van de Staatssecretaris voor Digitalisering en Koninkrijksrelaties (Kamerstuk 26 643, nr. 940) en de Strategie Digitale Economie van de Minister van Economische Zaken en Klimaat (Kamerstuk 26 643, nr. 941). Binnenkort ontvangt uw Kamer van de Minister van Buitenlandse Zaken ook de Internationale Cyberstrategie waarin de internationale component van de NLCS verder wordt uitgewerkt.

Tot slot wil ik nog kort stil staan bij de Cyber Security Raad (CSR). Het afgelopen decennium hebben de adviezen van de CSR ten gevolge van technologische, maatschappelijke en bestuurlijke ontwikkelingen een bredere scope gekregen, waardoor de advisering niet beperkt is gebleven tot de uitvoering van (eerdere) Nederlandse cybersecuritystrategieën, maar ook beleid van het Rijk en wetgeving op het terrein van cybersecurity is gaan betreffen. Hierdoor functioneert de CSR als ware het een adviescollege waarvan het instellen dient plaats te vinden met inachtneming van de Kaderwet Adviescolleges. Momenteel wordt, in samenspraak met de raad, gewerkt aan het creëren van een governance

[2] Rapport CYCLOTRON. Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband, 10 oktober 2022.

structuur ten behoeve van deze bredere scope, die recht doet aan de behoefte aan advies over de implementatie van de NLCS en het actieplan, een platform biedt voor de succesvolle tripartite samenwerking tot nu toe, en recht doet aan de vereisten conform de Kaderwet Adviescolleges.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius