Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Datum
10 oktober 2022

Ons kenmerk
4229456

nota

Nederlandse Cybersecuritystrategie (NLCS)

1. Aanleiding

De afgelopen periode is gewerkt aan de totstandkoming van de voorliggende integrale Nederlandse Cybersecuritystrategie (NLCS). De NLCS is de opvolger van de Cybersecurity Agenda (NCSA) uit 2018.[1] De NLCS beschrijft de cybersecurityaanpak voor de komende zes jaar om de Nederlandse samenleving digitaal veilig te maken.

2. Geadviseerd besluit

Via deze nota wordt u gevraagd om akkoord te gaan:

- met het aanbieden van de NLCS en het actieplan aan de Ministerraad van 7 oktober 2022, ter vaststelling;
- met verzending van de NLCS en het actieplan aan de Eerste en Tweede Kamer op 10 oktober 2022, na akkoord van de Ministerraad van 7 oktober;
- met het, vanwege de inhoudelijke samenhang, gelijktijdig aanbieden van:
    - de kabinetsreactie aan op het rapport 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix' van de Onderzoeksraad voor Veiligheid (OVV);
    - het eindrapport met de werktitel Cyclotron, van een verkenning naar de mogelijkheden van een publiek-privaat samenwerkingsplatform om sneller en gerichter gezamenlijk informatie te delen rondom (dreigende) cyberincidenten;
    - het rapport 'Samen veilig: de toekomst van mobiel online' namens de minister van Economische Zaken en Klimaat waarvan de conclusies zijn geland in diverse activiteiten in het actieplan.

Besluitvorming in de Ministerraad van 7 oktober wordt voorafgegaan door behandeling in de Commissie Defensie, Internationale, Nationale en Economische Veiligheid (CDINEV) van 23 september, waarna is besloten dat behandeling in de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV) niet noodzakelijk is.

3. Kernpunten

[1] Nederlandse Cybersecurity Agenda | Brochure | Nationaal Cyber Security Centrum (ncsc.nl)

- In de visie van het kabinet is digitale veiligheid voor iedereen een vanzelfsprekendheid. De NLCS beschrijft deze stip op de horizon en de keuzes die het kabinet maakt om daar te komen.
- De doelstellingen voor de komende zes jaar en de prioritaire acties van dit kabinet omvatten vier gelijkwaardige pijlers van het cybersecuritybeleid:
  Pijler I: Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties
  Pijler II: Veilige en innovatieve digitale producten en diensten
  Pijler III: Tegengaan van digitale dreigingen van staten en criminelen
  Pijler IV: Cybersecurity-arbeidsmarkt, onderwijs en de digitale weerbaarheid van burgers
- In het bijgevoegde actieplan staan de maatregelen waarmee deze ambities worden gerealiseerd en wie daarvoor verantwoordelijk is. Het actieplan 2022-2023 is het startpunt. Het actieplan kan jaarlijks worden geactualiseerd. De komende jaren geeft het kabinet hier samen met medeoverheden, bedrijfsleven en wetenschap uitvoering aan.

4. Toelichting

4.1 Politieke context

Per brief van 4 juli 2022 is het Cybersecuritybeeld Nederland 2022 (CSBN2022) aan de Tweede Kamer aangeboden.[2] Het CSBN2022 geeft inzicht in de strategische thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland en dient als onderliggende analyse voor de NLCS.
Het coalitieakkoord toont ambitie op het gebied van cybersecurity. Zoals toegezegd in de Kamerbrief Hoofdlijnen beleid Ministerie Justitie en Veiligheid landen deze ambities in de Nederlandse Cybersecuritystrategie en het bijbehorende actieplan.

Er is een aantal thema's in het cybersecurity veld en de politiek (meest recentelijk in de commissiedebatten Online veiligheid en cybersecurity van 7 april en 14 september 2022), waar de NLCS invulling aan geeft:

- Verbetering van de informatie-uitwisseling. Hierbij hoort bijvoorbeeld ook de integratie tussen Nationaal Cyber Security Centrum (NCSC), Digital Trust Center (DTC) en Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) (uitgewerkt in pijler I).
- Meer samenhang en efficiëntie in het cybersecurity-stelsel en meer regie op de doorontwikkeling ervan (uitgewerkt in pijler I).
- Het belang van Europese en internationale samenwerking voor de ontwikkeling van veilige en innovatieve digitale producten en diensten (uitgewerkt in pijler II) en het tegengaan van digitale dreigingen van staten en criminelen (uitgewerkt in pijler III).
- Er zijn (meer) investeringen nodig op het gebied van cybersecurity. In de NLCS wordt toegelicht welke structurele middelen aanvullend beschikbaar zijn gemaakt voor het verhogen van de digitale weerbaarheid voor de departementen, inclusief de uitvoeringsorganisaties (uitgewerkt in de financiële appendix, te bezien in relatie tot het eigenaarschap in het actieplan).

[2] Tweede Kamer, vergaderjaar 2021-2022, kamerstuk 26 643, nr. 891.

Als bijlage bij deze beslisnota is een overzicht toegevoegd van politieke toezeggingen en hoe deze zijn geland in de NLCS of het actieplan.
De Tweede Kamer wordt jaarlijks geïnformeerd over de voortgang van de cybersecuritystrategie en ontvangt jaarlijks het CSBN.

4.2 Financiële overwegingen

- Dit kabinet investeert 111 miljoen euro structureel in cybersecurity. Dit is onderdeel van een bredere structurele investering waar onder andere de inlichtingen- en veiligheidsdiensten mee worden versterkt en investeringen worden gedaan op het gebied van economische veiligheid en de vitale infrastructuur.
- Deze structurele investering van 111 miljoen euro draagt bij aan het uitvoeren van de verschillende acties die de departementen ondernemen ten behoeve van de realisatie van de doelen uit de cybersecuritystrategie.
- Daarnaast dragen ook andere investeringen die dit kabinet in brede zin doet in digitalisering bij, zoals de versterking van de eigen ICT-infrastructuur of investeringen op specifieke beleidsterreinen voor verhoging van de digitale weerbaarheid.
- Waar geen additionele investeringen mogelijk zijn en toch een opgave ligt zal herprioritering binnen de eigen begrotingen plaatsvinden en/of worden de mogelijkheden onderzocht om aanvullende activiteiten te financieren via Europese digitaliseringsfondsen. Daarnaast kunnen generieke nationale fondsen zoals het Nationaal Groeifonds ook ingezet worden voor digitale weerbaarheid.

4.3. Probleemanalyse, doelstellingen, inzet beleidsinstrumenten, monitoring en evaluatie.

- De cybersecuritystrategie biedt een antwoord op de huidige en toekomstige uitdagingen op het gebied van cybersecurity zoals beschreven in het CSBN2022. Het CSBN is aangevuld met een aantal additionele inzichten die in de strategie zijn meegenomen na consultatie van ministeries, publieke en private stakeholders en/of na aanleiding van eerder uitgebrachte beleids- en adviesrapporten. Deze probleemanalyse staat in het eerste hoofdstuk van de NLCS.
- In de visie van het kabinet streeft naar een digitaal veilig Nederland waarin burgers en bedrijven ten volle kunnen profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico’s. De NLCS beschrijft deze stip op de horizon en de keuzes die het kabinet maakt om daar te komen in het tweede hoofdstuk.
- Rondom vier thematische pijlers staan hoofd- en subdoelstellingen geformuleerd. Deze vier hoofdthema’s zijn in acht werksessies met stakeholders geïnventariseerd en aangescherpt onder begeleiding van een externe partij en met betrokkenheid van de verantwoordelijke departementen. De realisatie van de subdoelen zijn (tussen)stappen voor de realisatie van de hoofddoelstellingen.
- Achter elke pijler staan enkele lang lopende en overkoepelende acties benoemd, die worden uitgewerkt en aangevuld in het actieplan. In het actieplan staat:
    - wanneer de actie start en eindigt;
    - wie het eerste aanspreekpunt is in het kabinet voor realisatie van de actie;
    - welke partijen nog meer betrokken zijn.

- In het vijfde hoofdstuk staat beschreven hoe de evaluatie en monitoring wordt uitgevoerd.

4.3 Juridische overwegingen

De NLCS kondigt geen concrete nieuwe wetgeving aan. Wel wordt er verwezen naar lopende wetgevingstrajecten, zoals de lopende wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) én het opstellen van nationale implementatie- of uitvoeringswetgeving met betrekking tot Europese richtlijnen en verordeningen zoals de herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB2-richtlijn) en de Cyber Resilience Act (CRA). Een deel van het in de NLCS opgenomen beleid volgt op de bovenbedoelde nieuwe (nationale, Europese) wetgeving.

Daarnaast worden er verschillende initiatieven en onderzoeken aangekondigd in de NLCS die op termijn mogelijk wetswijzigingen nodig zullen maken. Het gaat onder meer om de oprichting van een publiek- privaat samenwerkingsplatform, de integratie van het DTC en NCSC en het onderzoek naar verdere vormgeving van doelwit- en slachtoffernotificatie. In deze initiatieven wordt nader onderzocht of en in hoeverre nieuwe wetgeving of wetswijzigingen in de komende jaren in relatie tot bovengenoemde initiatieven nodig zijn.

4.4 Krachtenveld

- De minister van Justitie en Veiligheid is de coördinerend bewindspersoon op het gebied van cybersecurity en biedt de NLCS namens het kabinet aan de Tweede Kamer aan.
- Ook is er een nauwe samenhang met de inzet van het kabinet op digitalisering, onder regie van de staatssecretaris voor Koninkrijksrelaties en Digitalisering, zoals uiteengezet in de hoofdlijnenbrief digitalisering van 8 maart 2022.
- In de Tweede Kamer zijn er sinds december 2021 verschillende debatten geweest met betrekking tot online veiligheid en cybersecurity. De wensen die Kamerleden hebben geuit in deze debatten zijn ook meegenomen in de strategie.
- De NLCS is tot stand gekomen met bijdragen van beleidsdepartementen, andere overheidspartijen, wetenschap en maatschappelijke organisaties die een rol spelen op het gebied van cybersecurity.
- Een stuurgroep met vertegenwoordigers van de ministeries van JenV, BZK, EZK, BZ en DEF heeft een trekkersrol vervuld voor de totstandkoming van de NLCS.
- In verschillende werksessies en bestuurlijke tafels is door publieke en private belanghebbenden bijgedragen aan het formuleren van de visie, de doelstellingen en de acties.
- Gezien de omvang van het cybersecurity domein en de beschikbare tijd voor de totstandkoming van de NLCS is er vanzelfsprekend een selectie gemaakt in het aantal partners dat betrokken is. Waar mogelijk en relevant is de input zo veel als mogelijk meegenomen ten behoeve van de integraliteit en het draagvlak van de NLCS. Ook zijn (externe) belanghebbenden betrokken bij het formuleren van de maatregelen in het actieplan.
- De Cyber Security Raad (CSR) is gedurende de totstandkoming van de NLCS op meerdere momenten geconsulteerd. Dit heeft zowel in plenaire

vergaderingen als in subcommissievergaderingen en een-op-op consultaties plaatsgevonden.

4.7 Implementatie

- In het actieplan staat vermeld wie het eerste aanspreekpunt is en verantwoordelijk is voor de realisatie van de actie(s).
- Onder de CDINEV wordt begin 2023 een integraal sturingsmodel ingericht. In dit model wordt op deelonderwerpen de gezamenlijke inzet van publieke en private partijen gericht en geïntensiveerd met het oog op het behalen van de doelstellingen. De inzet is om aan te sluiten bij bestaande overleggen en positieve ervaringen met publiek-private samenwerking.
- De NLCS kan alleen met gezamenlijke inzet van publieke en private partijen worden geïmplementeerd en de (bestaande) publiek private samenwerking wordt geïntensiveerd waar dat bijdraagt aan de realisatie van de NLCS, bijvoorbeeld rondom de doelstellingen gericht op versterking van de arbeidsmarkt, het intensiveren van innovatie of het efficiënter en effectiever inrichten van het cybersecurity-stelsel.

4.8 Communicatie

De NLCS wordt 10 oktober 2022 gepubliceerd met een persbericht. Oktober is cybersecurity-maand en er vinden verschillende activiteiten plaats waar (tevens) aandacht is voor de NLCS, zoals tijdens de jaarlijkse ONE Conference.

4.9 Ontwikkelingen hiervoor

Om voortvarend aan de slag te kunnen met het formuleren van acties en maatregelen om de doelstellingen te kunnen realiseren is het eerste deel van de NLCS bekrachtigd in de CDINEV op 22 juni 2022 en de RDINEV op 5 juli 2022. Het eerste deel bestond uit de probleemanalyse, visie en doelen van de NLCS.

Als startpunt voor de probleemanalyse is gebruik gemaakt van het CSBN2022. De basis vanuit het CSBN2022 is vervolgens aangevuld doormiddel van een analyse op al bestaande rapporten en adviezen, een tweetal werksessies met stakeholders en een schriftelijke enquête aan een brede groep stakeholders, gevolgd door een inloopsessie om de uitkomsten van de enquête met elkaar aan te scherpen.

Vervolgens zijn er vier hoofdthema's opgesteld (pijlers) waaromheen doelstellingen zijn geformuleerd. Deze zijn in acht werksessies met stakeholders (twee sessies per thema) geïnventariseerd en aangescherpt met betrokkenheid van de verantwoordelijke departementen. Per pijler zijn twee tot vier hoofddoelstellingen geformuleerd, met daarbij een aantal subdoelen.
Om de visie en de leidende principes te formuleren zijn een aantal bestuurlijke tafels georganiseerd. Tijdens deze sessies is gesproken over de visie op het cybersecuritybeleid in Nederland en de gezamenlijke richting vooruit.

5. Informatie die zich niet leent voor openbaarmaking

5.1 Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.