Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

NCTV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
23 december 2022

Ons kenmerk
4391717

nota

Landelijk Crisisplan Digitaal

1. Aanleiding

In 2020 is bij de aanbieding van het Nationaal Crisisplan Digitaal aan de Tweede Kamer een actualisatie van het plan toegezegd. De afgelopen periode is deze actualisatie vormgegeven onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), in nauwe samenwerking met alle betrokken publieke en private crisispartners. Het Landelijk Crisisplan Digitaal (LCP-Digitaal) is het resultaat van deze inzet.

2. Geadviseerd besluit

Via deze nota wordt u gevraagd om akkoord te gaan met:

- Verzending van het LCP-Digitaal aan de Tweede Kamer.

3. Kernpunten

- Het plan is een cyber-specifieke uitwerking van de generieke crisisaanpak zoals beschreven in het recent vastgestelde Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2022 en het Nationaal Handboek Crisisbeheersing dat op 6 december 2022 aan de Kamer is aangeboden.[1] [2]
- Het LCP-Digitaal is op regionaal niveau akkoord bevonden door de voorzitters veiligheidsregio's, verenigd in het Veiligheidsberaad, en in de Ministerraad vastgesteld. Het plan weerspiegelt daarmee de gezamenlijk gevoelde verantwoordelijkheid van het Rijk en de veiligheidsregio's om als één crisisorganisatie op te treden bij digitale crises.
- Het LCP-Digitaal beschrijft de gezamenlijke aanpak tussen het Rijk, de veiligheidsregio's en andere crisispartners, waaronder vitale aanbieders, bij een digitale crisis op landelijke niveau.
- De verzending van het LCP-Digitaal sluit aan bij de visie van de Nederlandse Cybersecuritystrategie (NLCS, publicatie 10 okt jl.) en de doelstelling in het actieplan van de NLCS om het LCP-Digitaal te publiceren.
- Publicatie van het LCP-Digitaal hangt samen met de cybersecurity oefening ISIDOOR IV. Het LCP-Digitaal is de basis voor de ISIDOOR

[1] Stcrt. 2022, nr. 32675.

[2] Kamerstukken, II, 2022-2023, 29 517, nr. 225.

oefening en wordt gebruikt in de voorbereiding. Het is beoogd dat de volgende editie eind 2023 plaatsvindt.

4. Politieke context

In februari 2020 is bij de aanbieding van het Nationaal Crisisplan Digitaal een actualisatie toegezegd die zou worden uitgevoerd aan de hand van de Citrix -problematiek (december 2019), de lessen uit de landelijke cyberoefening ISIDOOR (juni 2021) en de aanbevelingen uit het rapport over digitale ontwrichting van de Wetenschappelijke Raad voor het Regeringsbeleid (9 september 2019).

Ook is - mede naar aanleiding van de lessen uit de COVID-crisis - tussen het Rijk, de Veiligheidsregio's en vitale aanbieders de afspraak tot stand gekomen om via landelijke crisisplannen gezamenlijk voor te bereiden op landelijke risico's (waaronder op het gebied van cyber).

Met deze achtergrond heeft de NCTV een schrijfgroep ingericht met betrokkenheid van de Veiligheidsregio's en het Nationaal Cyber Security Centrum (NCSC) om het proces en de redactie te verzorgen. In het schrijfproces zijn relevante publieke en private crisispartners betrokken, waaronder ook vitale aanbieders.

4.1 Krachtenveld

- De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op het gebied van cybersecurity en crisisbeheersing, en biedt het LCP-Digitaal namens het kabinet aan de Tweede Kamer aan.
- Het LCP-Digitaal is het overkoepelend en kaderstellend plan voor de individuele operationele plannen en draaiboeken van actoren en organisaties betrokken in een (potentiële) digitale crisis. Het LCP-Digitaal vervangt deze plannen niet. De operationele plannen en draaiboeken van betrokken actoren en organisaties, waaronder (vak)departementen, moeten waar relevant wel in overeenstemming worden gebracht met het LCP-Digitaal.
- Het LCP-Digitaal is tot stand gekomen met bijdragen van beleidsdepartementen, relevante uitvoeringsorganisaties, de veiligheidsregio's, de VNG en andere publieke- en private crisispartners, waaronder vitale aanbieders.
- Een stuurgroep met vertegenwoordigers van de NCTV, het NCSC en de veiligheidsregio's heeft een trekkersrol vervuld in de totstandkoming van het LCP-Digitaal.
- In het plan en het schrijfproces is nadrukkelijk aandacht besteed aan de (potentiële) gevolgeffecten van een digitale crisis in het fysieke domein en voor de openbare orde en veiligheid, en de daaraan gerelateerde koppeling tussen de functionele (digitale) en algemene crisisbeheersingsketens.

4.2 Implementatie.

- In het actieplan van de NLCS staat vermeld dat departementen zorgen voor aansluiting van departementale crisisplannen op het LCP-Digitaal. Het gebruik van het LCP-Digitaal is daarnaast drieledig:
    - Het LCP-Digitaal wordt gebruikt voor crisisvoorbereiding.
    - Het LCP-Digitaal wordt gebruikt als basis voor cybercrisisoefeningen op regionaal en nationaal niveau, zoals ISIDOOR.
    - Het LCP-Digitaal wordt gebruikt als informatiebron tijdens cybercrises.
- Het LCP-Digitaal kan alleen met gezamenlijke inzet van publieke en private partijen worden uitgevoerd en gebruikt. Gezamenlijke oefeningen, zoals ISIDOOR, en onderlinge afstemming in en communicatie over de eigen crisisplanning is noodzakelijk voor een succesvolle beheersing van een (potentiële) digitale crisis op landelijk niveau.

4.3 Communicatie

Een publieksversie van het LCP-Digitaal zal worden verzonden naar de Tweede Kamer. Ook zal de publieksversie van het LCP-Digitaal online beschikbaar worden gesteld.

Het LCP-Digitaal zal actief onder de aandacht worden gebracht bij betrokken publieke- en private crisispartners, en tevens in de voorbereiding op de cyberoefening ISIDOOR IV.

5. Informatie die niet openbaar gemaakt kan worden

5.1 Toelichting

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

Enkele onderdelen van het LCP-Digitaal zijn niet geschikt voor brede verspreiding en worden enkel gedeeld met de betrokken bestuurders en professionals.