Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

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

Aan de Minister van Justitie en Veiligheid

Datum
11 april 2024

Projectnaam
projectnaam

Ons kenmerk
5703757

Dossiernummer
DossiernummerC/T/A/W

Bijlagen
1

nota

Aanbieding evaluatie ISIDOOR IV aan de Tweede Kamer

1. Aanleiding
Aanbieding van het evaluatierapport ISIDOOR IV aan de Tweede Kamer. De ISIDOOR oefening is een nationale crisisoefening waarin een cybercrisis wordt gesimuleerd en de gezamenlijke respons wordt beoefend. ISIDOOR IV vond plaats op 13, 14, 15 en 27 november 2023. De evaluatie is eind april 2024 gefinaliseerd.

2. Geadviseerd besluit
Akkoord met de aanbieding van het evaluatierapport ISIDOOR IV aan de Tweede Kamer.

3. Kernpunten
De evaluatierapporten van voorgaande ISIDOOR oefeningen zijn allen verzonden aan de Tweede Kamer. De aanbieding van het evaluatierapport ISIDOOR IV is in lijn met deze werkwijze.

4.1. Politieke context
In verleden bijeenkomsten van de kamercommissie Digitale Zaken is meermaals gesproken over het belang van het oefenen van cybercrises. Daarom is in de bewindsperiode van Minister Grapperhaus ingezet op een oefen- en testprogramma. Dit initiatief is strategisch geborgd en doorontwikkeld met de publicatie van de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) en het onderliggende actieplan.

4.2. Strategie
In de Nederlandse Cybersecurity Strategie (NLCS) en het onderliggende actieplan worden expliciet aandacht besteed aan het belang van effectieve voorbereiding op digitale crises en oefenen. De ISIDOOR oefening draagt bij aan deze doelstelling. Tijdens ISIDOOR worden de structuren en afspraken die zijn vastgelegd in het Landelijk Crisisplan Digitaal (2022) beoefend.

4.3. Uitvoering
Het evaluatierapport bevat verschillende aanbevelingen:

1. Grootschalig oefenen is waardevol gebleken, maar er kleven ook nadelen aan. Zorg voor een passend vervolg op ISIDOOR IV op basis van de ontwikkelingen binnen het cyberstelsel. Overweeg daarbij om een eventuele volgende keer als voorwaarde voor deelname aan organisaties mee te geven dat zij een interne crisisorganisatie hebben waarmee zij geoefend hebben en dat er sectoraal

afspraken zijn op het gebied van informatiedeling, communicatielijnen en samenwerking die ook een keer beoefend zijn.

2. Sectoren moeten investeren in informatiedeling en zorgen dat zowel cyber gerelateerde informatie (technisch/inhoudelijk) als informatie over de impact samenkomt en aansluit op landelijke informatiestromen. Hoe de routing precies vormgegeven moet worden is ter nadere beoordeling. Uiteindelijk zal dit moeten leiden tot een beter geïnformeerde nationale crisisstructuur en actueler IAO.

3. Op rijksniveau is er een behoefte aan een scherp afwegingskader met een helder proces er omheen. Gecombineerd met een duidelijk beeld en advies vanuit de sectoren moet dit ertoe leiden dat het afwegingskader goed kan worden gevuld en benut.

4. We zien een groot verschil in de mate waarin organisaties zelf zijn voorbereid op cybercrises. Vanuit een perspectief van nationale weerbaarheid zou het goed zijn als die partijen die nu een achterstand hebben prioriteit geven aan hun eigen voorbereiding. Hiermee kan ook het beroep op, en de verwachting van, het NCSC realistischer worden.

5. Werk de rolbeschrijving en werkwijzen van sectorale CERTS, ISAC's, OKTT's, etc. beter uit zodat sprake is van een meer eenduidige rolinvulling en deze partijen vanuit een gedeeld kader opereren en een bepaalde kwaliteitsstandaard kunnen leveren.

6. Zorg dat de bestaande overlegstructuren beter worden benut en eventueel uitgebreid met relevante partners. Dit kan worden bereikt door enerzijds de bekendheid met de bestaande structuur te vergroten en anderzijds te onderzoeken waarin de bestaande structuur op dit moment niet voorziet.

7. Zorg voor meer bekendheid van de Wbni criteria en de meldingsprocedure.

Naast bovenstaande concrete aanbevelingen bevat het rapport ook constateringen die toezien op de nationale opschaling, crisiscommunicatie en de inhoud van het Landelijk Crisisplan Digitaal.

4.4. Implementatie
In gesprek tussen de departementen worden acties geformuleerd die opvolging geven aan de aanbevelingen en constateringen in het evaluatierapport. De Tweede Kamer wordt geïnformeerd over de opvolging van de cybersecurity specifieke aanbevelingen in de jaarlijkse voortgangsrapportage van de Nederlandse Cyber Security Strategie. In de voortgangsrapportage van de Landelijke Agenda Crisisbeheersing wordt de Tweede Kamer geïnformeerd over de opvolging van aanbevelingen die zich richten op algemene crisiswerkwijzen.

4.5. Communicatie
Het evaluatierapport is reeds vertrouwelijk gedeeld met alle deelnemers aan de oefening ISIDOOR IV. Met de aanbieding aan de Tweede Kamer zal het rapport openbaar worden.

5. Informatie die niet openbaar gemaakt kan worden
De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.