Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1216

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 september 2024

Via deze brief bied ik u het evaluatierapport aan van de cyberoefening ISIDOOR 2023. Het evaluatierapport is door het Instituut voor Veiligheids- en Crisismanagement (COT) opgesteld, in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC).

ISIDOOR 2023

De ISIDOOR oefening is een nationale crisisoefening waarin een cybercrisis wordt gesimuleerd en de gezamenlijke respons wordt beoefend. Eerdere edities van ISIDOOR (2015, 2017 en 2021) hebben de meerwaarde van gezamenlijk oefenen aangetoond. In de Nederlandse Cybersecurity Strategie (NLCS) en het onderliggende actieplan worden expliciet aandacht besteed aan oefenen en het belang van effectieve voorbereiding op digitale crises. ISIDOOR draagt hieraan bij.

Tijdens ISIDOOR komen de thema's cybersecurity en crisisbeheersing samen. Samenwerking, informatie-uitwisseling en coördinatie tussen de deelnemers staan tijdens de oefening centraal. Deelnemers interacteren in het verloop van de oefening volgens de structuren en afspraken die zijn vastgelegd in het Landelijk Crisisplan Digitaal (LCP Digitaal).

ISIDOOR is een publiek-private oefening. ISIDOOR IV telde 120 deelnemende organisaties en meer dan 3000 individuele deelnemers. De hoofdoefening vond plaats tussen 13 en 15 november. Op 27 november is in de Interdepartementale Commissie Crisisbeheersing de ministeriële crisisbesluitvorming voorbereid. Vanwege de Tweede Kamerverkiezingen in November 2023 was het niet mogelijk om de bewindspersonen van de verschillende ministeries mee te laten oefenen.

kst-26643-1216
ISSN 0921 - 7371
's-Gravenhage 2024

Oefenelementen

ISIDOOR IV telde drie hoofddoelen: (1) het beoefenen van informatie-uitwisseling en samenwerking ten tijde van een cybercrisis, (2) het beoefenen van de nationale opschalingsstructuur tijdens een cybercrisis, tot en met het niveau van een Interdepartementale Commissie Crisisbeheersing, en (3) het versterken van de onderlinge samenwerking tussen vitale en rijksoverheidsorganisaties.

De kern van de oefening betrof een wijdverspreide software kwetsbaarheid die misbruikt werd door een statelijke actor, met als gevolg verstoring van processen bij verschillende organisaties binnen en buiten de vitale sectoren. Verspreid over de oefendagen zijn verschillende dynamieken aan bod gekomen. Technische analyse van de kwetsbaarheid, signalering van (fysieke) gevolgeffecten in de buitenwereld, nationale opschaling en coördinatie, publiekscommunicatie, en attributie- en respons. Met in dit laatste onderdeel een prominente rol voor het Ministerie van Buitenlandse Zaken, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

Opvolging evaluatie

ISIDOOR IV was een succesvolle oefening. Het evaluatierapport bevat veel concrete en nuttige aanbevelingen en constateringen, de opvolging waarvan zal bijdragen aan het versterken van onze digitale weerbaarheid en de voorbereiding op een digitale crisis.

Ik neem het rapport mee in gesprek met mijn collega bewindspersonen om de acties te identificeren die nodig zijn voor een goede opvolging van de evaluatie. Ik verwacht dat uw Kamer geïnformeerd wordt over de opvolging van aanbevelingen in de jaarlijkse voortgangsrapportage van de Nederlandse Cyber Security Strategie en in de voortgangsrapportage van de Landelijke Agenda Crisisbeheersing.

De Minister van Justitie en Veiligheid,
D.M. van Weel