Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Programma
Nederland Digitaal
Veilig

Contactpersoon
(10)(2e)
Beleidsmedewerker

T (10)(2e)
(10)(2e)@
nctv.minvenj.nl

Datum
12 mei 2020

agenda

Interdepartementaal Overleg Cybersecurity

Vergaderdatum en -tijd	12 mei 2020, 13.30 - 15.00 uur
Vergaderplaats	Conference call: Inbelnummer: (10)(2e) Toegangscode: (10)(2e) #

1. 13.30 – 13.35 Opening, vaststellen agenda en verslag

- (10)(2e) geeft aan in de verslaglegging van het vorig IOCS overleg niet terug te lezen dat VWS de ICOS leden heeft bijgepraat over hackaanval op de medische centrum Leeuwarden.
    - Actie NCTV: NCTV neemt in de verslaglegging van het vorig overleg dat VWS de ICOS leden heeft geïnformeerd over de hackaanval bij MCL en de daarop volgende Kamervragen.

2. 13.35 – 13.50 Actualiteiten en mededelingen

- (10)(2e) heeft de groepsleden bijgepraat over de spoedwet die momenteel in de maak is om farmaceuten en medische labs ism met het NCSC cyberhulp te bieden.
- Over the one confrence van JenV is nog niet besloten of het doorgaat of niet irt corona. Mocht de confrence worden afgeblazen dan zal dat in het IOCS worden gecommuniceerd.
- Is VWS aangehaakt bij de cybersecurity maand in oktober van de rijksoverheid? Gaan we activiteiten organiseren?
    - **Actie** (10)(2e): Checken intern met (10)(2e)
- (10)(2e) geeft aan dat Z-CERT cyberconferentie 2020 niet doorgaat vanwege COVID-19 ontwikkelingen en de daarmee opgevoerde drukte op Z-CERT en de zorgsector. Z-CERT wilt in eerste helft 2021 de conferentie organiseren.

3. 13.50 – 14.10 Brief CSBN 2020 en voortgang NCSA

- (10)(2e) geeft een reactie op PM punten voor VWS inzake stavaza vitaal herbeoordeling en risicogestuurde aanpak.

4. 14.10 – 14.35 Implementatieplan WRR

- Deadline alle departementen: Reageren binnen twee weken.
  - **Actie** (10)(2e) Met (10)(2e) schakelen over input/commentaar op het WRR-implementatieplan. Excelbestand met (10)(2e) delen.
  - Met name over het punt verplichten dat cybersecurity onderdeel worden van «In-Control-verklaring» rijksoverheidsorganisaties.

5. 14:35 – 14:55 VNAC en vervolg richting formatie

- Digitale dienstverlening in de nieuwe 1,5 meter samenleving door corona staat onder druk en dient beter georganiseerd te worden. Hiervoor is geld nodig. Niet alleen de digitale uitrusting om op afstand veilig en betrouwbaar te werken maar ook het gedrag van mensen om op afstand op een veilig manier om te gaan met informatie is een punt van aandacht voor alle depramtenten.
- Alle vakdepartementen willen zoals in 2017 bij de vorming van het nieuwe kabinet VNAC middelen beschikbaar komen als investering in cybersecurity en het verhogen van de weerbaarheid. Hiervoor is het nodig om te weten:
  - Hoeveel financiering heeft het departement nodig?
  - Wat gaat het departement concreet ermee doen om bij te dragen aan maatschappelijk doel (bijv NL digitaal veilig maken)?
  - Hiervoor dient het departement een claim/plan in te dienen bij JenV
  - JenV bundelt alle plannen en legt het voor aan de formatietafel voor het komend kabinet.
- Over het VNAC traject zal JenV nog nader communiceren om departementen in de gelegenheid stellen om een claim op VNAC middelen in te dienen.
- CSR komt eind dit jaar met een advies welke investeringen er nodig zijn om cybersecurity in NL te verhogen. Goed om in het plan van het departement daarop aan te sluiten.
- (10)(2e) geeft aan dat cyberbeleid van VWS onderhevig is aan ontwikkeling en staat in grote politieke en maatschappelijke belangstelling. VWS heeft nodige stappen gezet op cybergebied maar zal in de komende periode meer aandacht geven aan cybersecurity in de zorgsector en zal meer geïnvesteerd moeten worden om de weerbaarheid van de sector te verhogen. Op dit moment wordt cyberbeleid vanuit VWS budget gefinancierd. Om de weerbaarheid in de zorgsector te verhogen heeft VWS meer budget nodig. VNAC middelen kunnen hierin voorzien.

6. 14.55 – 15.00 W.v.t.t.k.

Geen punten