Nationaal Coördinator
Terrorismebestrijding en Veiligheid
*Ministerie van Justitie en Veiligheid*

**Dep. VERTROUWELIJK**
Ministerie van Volksgezondheid, Welzijn & Sport

Programma Nederland Digitaal Veilig
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

**Datum**
8 juli 2020

**Projectnaam**
.

**Ons kenmerk**
2966502

# nota

**Tussenadvies nationale veiligheid inzake digitale contactalarmering app van VWS_x000d_Nationaal**

*Gezamenlijk advies NCSC, NCTV & AIVD*

## Algemeen

De afgelopen maand hebben gezamenlijke expertsessies plaatsgevonden (2, 4, 11 en 25 juni jl.) waarin NCSC, NCTV en AIVD middels expertadviezen input hebben geleverd voor een dreigings- en risicoanalyse van VWS t.a.v. digitale contactalarmering. De sessies zijn voortgekomen uit een eerdere brief en e-mail over nationale veiligheidsrisico's die gepaard gaan met de toepassing van apps voor bron-en contactonderzoek (d.d. resp. 16 april 2020 en 21 april 2020), een procesvoorstel van onze drie organisaties over hoe cybersecurity en nationale veiligheid op een gestructureerde manier geborgd kunnen worden in het ontwikkelproces van de app (d.d. 30 april 2020) en de uitnodiging voor de waarborggroep nationale veiligheid.

Het resultaat van deze gezamenlijke sessies is opgenomen in het door VWS opgestelde rapport getiteld '*Dreigings- en risicoanalyse nationale veiligheid digitale contactalarmering*'[1]. NCTV, NCSC en AIVD willen met deze nota hun waardering uitspreken voor de openheid en de ontvankelijkheid van VWS voor onze adviezen in dit proces. NCTV, NCSC en AIVD onderschrijven de inhoud van het rapport als zijnde een weergave van hetgeen besproken is in de expertsessies. Dit laat onverlet dat NCTV, NCSC en AIVD middels dit tussenadvies nog enkele aandachtspunten en overwegingen aan VWS willen meegeven rond de verdere ontwikkeling van de contactalarmeringapp en het implementeren van de adviezen uit het *Rapport*.

Dit tussenadvies is net als het *Rapport* gebaseerd op de stand van zaken van de ontwikkeling ten tijde van de sessies en op basis van de daarvoor van VWS ontvangen documentatie[2] en de toelichting die in de sessies is

[1] Hierna genaamd 'Rapport'.
[2] Programma van Eisen voor een digitale oplossing ter aanvulling op bron- en contactonderzoek [versie 0.5, 19 mei 2020]; Corona App Solution Architecture [versie 0.9, 27 mei 2020]; Corona App Crypto Raamwerk [versie 0.30, 27 mei 2020], Exposure Notificatie App Architectuur Overview [versie 0.5]; Documentatie Exposure Notification / Privacy Preservering Contact Tracing [Apple, Google].

gegeven. Het tussenadvies is gebaseerd op vier expertsessies en de daarin of in relatie tot die sessies aan ons beschikbaar gestelde informatie en inzichten. Dit advies is tevens gebaseerd op een aantal door VWS aangegeven (ontwerp)keuzes (zoals decentrale opslag van gegevens). Deze sessies zijn onder hoge tijdsdruk doorlopen. Het is daarmee een versneld *lean en mean* proces geweest waardoor niet kon worden voldaan aan alle eisen die normaliter worden toegepast bij het uitvoeren van een diepgaande en volwaardige risicoanalyse. Tegelijkertijd zijn wij van opvatting dat het rapport inzicht biedt in de belangrijkste risico's en scenario's uitgaande van de op dit moment gemaakte architecturale keuzes.

**Proces**
De ontwikkeling van de app is een dynamisch en iteratief proces waardoor dit advies nadrukkelijk een tussenadvies is, gebaseerd op de huidige inzichten en stand van zaken op dit moment. Een aantal (ontwerp)keuzes door VWS - zoals het in te richten GGD proces - die op een later moment zullen worden gemaakt of mogelijk worden aangepast, kunnen nog leiden tot aanpassing van de risicoanalyse en daarmee ook tot aanpassing van ons advies m.b.t. benodigde additionele maatregelen. Dit tussenadvies is dus niet te beschouwen als een alomvattend advies over de mogelijke cyber – en nationale veiligheidsrisico's. De uiteindelijke afweging van de te beschermen belangen en het beheersen van de risico's is een verantwoordelijkheid van het ministerie van Volksgezondheid, Welzijn en Sport.

**Adviezen**
Op basis van het hierboven geschetste, doorlopen proces worden op dit moment over de volgende aspecten onderstaande adviezen op het gebied van nationale veiligheid i.r.t. de in ontwikkeling zijnde contactalarmering app gegeven. Wanneer er meer duidelijkheid is over de inrichting van het GGD proces of andere significante keuzes worden gemaakt of veranderingen worden doorgevoerd in de architectuur zal het risicoanalyseproces opnieuw (gedeeltelijk) doorlopen moeten worden om te bezien of dreigingen anders gewaardeerd dienen te worden en additionele of andere maatregelen nodig zijn. Het komt er derhalve op neer dat over enkele elementen, zoals de (verbinding met) processen bij de GGD en het registratieproces, thans nog geen advies afgegeven kan worden.

- **Stel het risicobeeld indien nodig bij**
  Het uitvoeren van een risicoanalyse is geen eenmalige actie. Zowel aan de kant van de behoefte als die van de dreiging kunnen er zaken veranderen.

  Wanneer er wijzingen worden doorgevoerd in 1. de applicatie of de IT-architectuur, 2. de dreiging verandert of 3. er meer duidelijkheid is over de inrichting van het GGD-proces zal het proces m.b.t. de risicoanalyse opnieuw (gedeeltelijk) doorlopen moeten worden om te bezien of de maatregelen hier op aangepast moeten worden. Wees

hierbij ook bewust van de mogelijk lange tijd waarin de app gebruikt kan worden en de hiervoor veranderende en ontwikkelende dreiging. Andere dreigingen kunnen echter in de loop der tijd minder groot worden.

Om voldoende zicht op veranderingen te houden is het noodzakelijk om publicaties op gebied van de gebruikte technologieën op de voet te volgen. Dit is onder andere noodzakelijk, omdat de beveiliging voor een deel afhankelijk is van de implementaties van Google en Apple. Daarnaast is het van belang experts op gebied van informatiebeveiliging en cryptografie vanuit universiteiten of de overheid bij de ontwikkeling te (blijven) betrekken.

- **Zorg voor integere besmettingsgegevens**
  De werking van de app is in sterke mate afhankelijk van de integriteit van besmettingsgegevens die aan de app beschikbaar worden gesteld via de backend. Een goede en integere opslag en verwerking van deze gegevens is van groot belang voor het goed kunnen laten functioneren van de app. Hoe deze verwerking zal plaatsvinden was nog niet bekend ten tijde van de sessies. Het maken van een risicoanalyse en het op basis daarvan treffen van maatregelen op dit terrein is cruciaal voor het goed functioneren van de app. Denk hierbij aan het proces van vaststellen van een besmetting, het invoeren van een besmetting door GGD en het opslaan en vervolgens verzenden van deze gegevens aan de app.
- **Zorg voor een op risico's gebaseerde security architectuur**
  Bij gebrek aan detailinformatie is er tijdens de workshops slechts beperkt gesproken over de technisch-inhoudelijke risico's van bepaalde IT-componenten. Daarom willen wij VWS in het algemeen adviseren om naast het volgen van algemene best practices op gebied van beveiliging zowel preventieve als detectiemaatregelen te treffen t.a.v. de meest voorstelbare risicoscenario's (*naast algemene maatregelen ook maatwerkbeveiliging te treffen*). Wanneer VWS een hoge mate van zekerheid wil ten aanzien van specifieke systeemcomponenten, kan VWS overwegen gebruik te maken van gespecialiseerde labs. Bepaal per risicoscenario welke maatregelen de businesscase van de aanvaller het meest negatief beïnvloeden of de kans op detectie vergroten.
- **Bepaal een strategie in geval van een mogelijke compromittering**
  Ondanks de getroffen beveiligingsmaatregelen is de verwachting dat er kwetsbaarheden gevonden zullen worden; er zullen incidenten en storingen optreden. Richt hiervoor een goed incidentresponsproces in om incidenten adequaat en snel af te kunnen handelen, en dat bekend is wie welke rol heeft bij de afhandeling. Dit houdt in dat wanneer er onverhoopt een compromittering van het systeem plaatsvindt, VWS en haar partners hierop voorbereid zijn en daarmee

in staat zijn de negatieve effecten van de compromittering te beperken. Deze voorbereiding zou betrekking moeten hebben op zowel technische als niet-technische aspecten. Denk hierbij aan het offline halen van het systeem en het kunnen faciliteren van digitaal forensisch onderzoek (bijv. door het voorhanden hebben van logging) maar ook escalatiepaden, communicatielijnen of een -plan en mandaten.

- **Voer op frequente basis een redteamingoefening uit**
  Het uitvoeren van pentests geeft een waardevol, maar tegelijkertijd selectief beeld van de actuele beveiliging omdat pentests zich primair richten op het vinden van technische kwetsbaarheden. Middels een redteamingoefening worden naast deze technische kwetsbaarheden ook ander beveiligingselementen zoals het detecteren van aanvallen, awareness van mensen en het incidentresponseproces, getest. Het inrichten van een proces waarbij redteamingoefeningen elkaar frequent opvolgen waarbij keer op keer nieuwe aanvalsscenario's worden getoetst, geeft een beter beeld van het actuele beveiligingsniveau. De tijdens de risicoanalyse geïdentificeerde risicoscenario's kunnen een eerste vertrekpunt zijn voor een redteamingoefening.

- **Handel n.a.v. bevindingen over veiligheid**
  De diverse penetratietests en andere tests zullen naar verwachting bevindingen opleveren. Aan de hand daarvan en de risicoanalyse wordt geadviseerd de bevindingen te verhelpen en te mitigeren.

**Conclusie**
Geconstateerd wordt dat de zorgen die in de adviezen van 16 en 21 april geuit zijn, zijn geadresseerd en meegenomen zijn in het maken van keuzes m.b.t. de inrichting van de contactalarmeringapp.

Op basis van hetgeen op dit moment bekend is over de contactalarmeringapp en de inrichting daarvan, wordt er, als de gegeven adviezen worden geïmplementeerd, weerbaarheid georganiseerd tegen potentiële risico's op het gebied van nationale veiligheid. De geïnventariseerde risico's en mogelijke maatregelen kunnen daarom meegenomen worden in de afweging die VWS zal moeten maken m.b.t. het implementeren van de contactalarmeringapp. Dit laat onverlet dat, zoals eerder aangegeven, dit beeld bijgesteld kan en moet worden zodra nadere keuzes m.b.t. de inrichting worden gemaakt of andere, nieuwe informatie beschikbaar komt.