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
14 augustus 2020

Ons kenmerk
3002061

nota

Aanvullend nationaal veiligheidsadvies inzake CoronaMelder

Algemeen

Voor u ligt een aanvullend advies betreffende nationale veiligheidsrisico's en mogelijk te treffen maatregelen om deze risico's te beperken. Dit advies is aanvullend op het tussenadvies van 8 juli 2020[1] over hetzelfde onderwerp. Beide adviezen zijn gebaseerd op de gezamenlijke expertsessies, waarvan de meest recente heeft plaatsgevonden op 28 juli 2020 en heeft geresulteerd in een door VWS bijgewerkte dreigingsanalyse[2]. Deze laatste expertsessie en deze bijgewerkte dreigingsanalyse vormen de aanleiding voor dit aanvullend advies.

Dit aanvullend advies is net als het vorige tussenadvies gebaseerd op de stand van zaken van de ontwikkeling ten tijde van de sessies en op basis van de daarvoor van VWS ontvangen documentatie[3] en de toelichting die VWS in de sessies heeft gegeven. Tijdens de expertsessie van 28 juli 2020 is gebleken dat door NCTV, NCSC en AIVD ontvangen documentatie op veel punten niet meer actueel was. Het verdient daarom de aanbeveling dat documentatie tijdig bijgewerkt wordt. Dat de eerder gegeven adviezen niet worden herhaald in dit aanvullend advies, maakt deze adviezen vanzelfsprekend niet achterhaald of niet van belang.

Proces

De ontwikkeling van de app is een dynamisch en iteratief proces. Op het moment van schrijven van dit aanvullend advies zijn er nog onderdelen waarop geen zicht is, zoals de in de toekomst voorziene integratie van de app met het GGD-proces in HPZone ("Bouwsteen 2"). Het advies is derhalve gebaseerd op de huidige inzichten en stand van zaken. Dit nationaal veiligheidsadvies kan geen uitsluitsel geven over alle mogelijke digitale en nationale veiligheidsrisico's die in de toekomst de kop

[1] Tussenadvies d.d. 8 juli 2020, kenmerk 2966502.
[2] Dreigings- en risicoanalyse nationale veiligheid digitale contactalarmering [versie 1.1, 10 augustus 2020).
[3] Covid-19 Exposure Notification Cryptografie raamwerk [versie 0.65, 24 juni 2020]; Integratie tussen Notificatie App en GGD Bouwsteen 1: Portaal voor gebruik tijdens uitslag gesprek [versie 0.4]; Dreigings- en risicoanalyse nationale veiligheid digitale contactalarmering [versie 1.1, 10 augustus 2020).

opsteken, mede gelet op de nog onbekende duur van het gebruik van de app en nog te maken (ontwerp)keuzes. Tenslotte is de uiteindelijke afweging van de te beschermen belangen en het beheersen van de risico's een verantwoordelijkheid van VWS. De nationale veiligheidsadviezen kunnen hierbij behulpzaam zijn.

Adviezen

Op basis van het doorlopen proces worden op dit moment onderstaande adviezen op het gebied van nationale veiligheid i.r.t. de CoronaMelder gegeven, in aanvulling op de eerder gegeven adviezen in de expertsessies en het tussenadvies. Wanneer er door VWS 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, andere risico's ontstaan en hierdoor additionele of andere maatregelen geadviseerd worden.

- **Logging en responsstrategie**
  In het licht van het nu toegelichte GGD-proces en de noodzakelijke (beheerders)toegang tot de backendsystemen adviseren wij, net als in ons tussenadvies, logging op toegang en gebruik van betrokken systemen in te richten en voor te bereiden op het kunnen doen van (forensisch) onderzoek t.b.v. incident-respons in geval van misbruik of aanval. Dit geldt in het bijzonder voor de in de expertsessie van 28 juli 2020 besproken systemen waarop de uitgifte van GGD-sleutels en verwerking van de sleutels plaatsvindt. Tevens adviseren wij de processen rondom incidentrespons vast te leggen.
- **Beschikbaarheid backendservers GGD-portaal**
  In het gesprek tussen de GGD-medewerker en de positief geteste persoon wordt door de GGD-medewerker een code verstrekt (de "GGD-sleutel") waarmee het voor de gebruiker van de app mogelijk is de sleutels te laten versturen zodat andere gebruikers genotificeerd kunnen worden. Deze uitwisseling van de code vindt plaats tijdens het telefoongesprek met de testuitslag. Op het moment dat de backendservers van het GGD-portaal niet beschikbaar zijn, loopt dit gesprek en daarmee mogelijk het tijdig kunnen informeren en uitvoeren van bron- en contactonderzoek vertraging op. Wij adviseren op deze backendservers technische maatregelen tegen moedwillige en onbedoelde aanvallen, maar ook tegen verstoringen te treffen, alsmede organisatorische maatregelen om het gesprek doorgang te kunnen laten vinden bij niet-beschikbaarheid.
- **Beperken uitgifte GGD-sleutels door GGD-medewerker**
  De eerdergenoemde GGD-sleutel die tijdens het gesprek tussen de GGD-medewerker en de positief geteste persoon wordt uitgewisseld, kan oneindig worden aangemaakt door de GGD-medewerker met toegang tot dit account of het portaal. Wij adviseren hiervoor

technische en organisatorische maatregelen te treffen alsmede het toepassen van eerdergenoemde logging op deze systemen.

- **Goede afspraken met nieuwe leverancier**
  In de afgelopen periode heeft VWS de keuze gemaakt voor een andere leverancier voor de hosting van (een deel van) de backendsystemen alsmede het beheer en de ondersteuning hiervan. In eerdere expertsessies is de Belastingdienst op verzoek van VWS als beoogd beheerder aanwezig geweest voor het toetsen van de besproken maatregelen alsmede het advies hieromtrent vanuit hun expertise en ervaring. Veel besproken maatregelen pasten binnen de standaarddienstverlening van de Belastingdienst, zoals opvolging geven aan malafide apps of phishing. Nu gekozen is voor een andere leverancier wordt geadviseerd afspraken te maken over in ieder geval de dienstverlening, de implementatie van de door ons geadviseerde maatregelen en de reeds bij Belastingdienst genomen maatregelen en de hier standaard beschikbare dienstverlening, bijvoorbeeld monitoring van verdacht netwerkverkeer en het vroegtijdig detecteren van aan CoronaMelder gerelateerde phishing-pogingen. Wij adviseren deze afspraken vast te leggen.

- **Scheiding binnenkomend verkeer en verwerking gegevens**
  T.b.v. het waarborgen van de anonimiteit en het kunnen koppelen van sleutels aan identificerende gegevens als IP-adressen adviseren wij een zowel technisch als organisatorisch scheiding (rollenscheiding voor beheerders) te maken tussen het punt waar het verkeer van de app binnenkomt en het punt waar de sleutels van het toestel verder worden verwerkt. Hiertussen dient het verkeer zoveel mogelijk van identificerende gegevens 'gestript' te worden.

- **Beschikbaarheid en integriteit sleutels op het CDN**
  Via het Content Delivery Network (CDN) wordt de lijst met sleutels van positief geteste personen aangeboden aan de app. Voor een effectieve notificatie en goede werking van de app is beschikbaarheid van deze lijst belangrijk. Om deze reden heeft VWS in een vroegtijdig stadium gekozen om deze lijst op een CDN te plaatsen. Van belang is ook dat de gepubliceerde lijst correct en actueel is. Om deze laatste reden adviseren wij maatregelen te treffen om de integriteit en de actualiteit van de lijst vast te kunnen stellen. Mogelijk dat hiervoor ook maatregelen getroffen dienen te worden t.a.v. foutafhandeling aan de kant van de app.

Conclusie

In overeenstemming met het tussenadvies van 8 juli 2020 wordt er op basis van hetgeen op dit moment bekend is over de CoronaMelder en de inrichting daarvan - 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 afwegingen die

VWS zal moeten maken bij het implementeren van de CoronaMelder. Dit laat onverlet dat, zoals eerder aangegeven, dit beeld bijgesteld kan en moet worden zodra nadere keuzes door VWS m.b.t. de inrichting worden gemaakt of andere informatie beschikbaar komt en dat de dreiging en daaraan verbonden risico's gaandeweg de tijd kunnen veranderen.