Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

Ministerie van Volksgezondheid, Welzijn en Sport
(10)(2e) (10)(2e)
Postbus 20350
2500 EJ Den Haag

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

Ons kenmerk
(10)(2b)
Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 16 april 2020
Onderwerp Apps voor bron- en contactonderzoek COVID-19 en nationale-veiligheidsaspecten

Geachte (10)(2e)

Het OMT adviseert zo snel mogelijk de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken. Het OMT acht dit noodzakelijk voor de toekomstige fase in aanvulling op reguliere bron- en contactopsporing door de GGD'en. Het OMT heeft een voorkeur voor een populatiegebaseerde aanpak gebruikmakend van technieken die de privacy van eindgebruikers waarborgen conform de privacywetgeving (AVG, enz.), zie bijvoorbeeld het recente PEPP-PT-initiatief. Naast het waarborgen van privacy is ook het waarborgen van de nationale veiligheid essentieel. In dit stuk wordt ingegaan op de voorwaarden vanuit het perspectief van de nationale veiligheid.

Met deze brief informeer ik u, mede namens de wnd. directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst en de directeur van het Nationaal Cyber Security Centrum, over risico's voor de nationale veiligheid bij ontwikkeling en inzet van apps voor ondersteuning van bron- en contactopsporing en over randvoorwaarden en aanbevelingen om deze risico's te verminderen.

Om de in dit document beschreven risico's zoveel mogelijk te mitigeren is het noodzakelijk om de randvoorwaarden en aanbevelingen mee te nemen aan de voorkant van het traject, waaronder in ieder geval bij het opstellen van criteria en bij selectie, met gebruik van gewogen risicoanalyses. NCTV, NCSC en AIVD blijven VWS graag adviseren op het gebied van nationale veiligheid en cybersecurity.

Risico's voor de nationale veiligheid

Om toegevoegde waarde te behalen uit het gebruik van de apps is maatschappelijk draagvlak essentieel. Tegelijkertijd kan de inzet van apps voor contactonderzoek leiden tot onrust en gevoelens van wantrouwen naar de overheid en/of private bedrijven. In zijn algemeenheid geldt dat het vertrouwen in de gehele systematiek essentieel is voor het realiseren van een bijdrage aan de nationale veiligheid.

Door aan de voorkant rekening te houden met de risico's rondom de nationale veiligheid wordt bijgedragen aan het creëren van het noodzakelijke draagvlak. Op

langere termijn kunnen de apps bijdragen aan een sneller herstel van de Nederlandse samenleving en daarmee ook aan de nationale veiligheid.

Er bestaat een gekende dreiging vanuit statelijke actoren ten aanzien van onder meer het vergaren van persoonsgegevens en bulkdata. Concreet betekent dit dat de gegevens uit verschillende apps, de apps zelf en de bijbehorende infrastructuur een zeer aantrekkelijk doelwit zijn voor met name spionage of prepositionering (voor latere spionage of verstoring) door statelijke actoren. Statelijke actoren zullen deze gegevens nu én in de toekomst proberen te misbruiken om, ten koste van Nederlandse belangen, hun eigen belangen te dienen. Daarnaast kunnen statelijke actoren misbruik maken om het vertrouwen in de overheid te ondermijnen, bijvoorbeeld desinformatie over de apps verspreiden of valse ziekmeldingen genereren.

De omvang van de risico's voor de nationale veiligheid zijn zeer sterk afhankelijk van de wijze waarop apps opgezet en ingezet worden. Met name keuzes over (al dan niet) gebruik van locatiegegevens, (direct) herleidbare koppeling aan personen en met wie zij contact hebben, wijze van ziekmelden, gecentraliseerde verwerking en/of dataopslag ten behoeve van de apps, en de leverancierskeuze hebben een sterke invloed op deze risico's.

Het vertrouwen in de inzet van apps voor contactonderzoek kan aangetast worden door bijvoorbeeld misbruik van de app door criminelen en andere actoren. Er bestaat een dreiging vanuit criminelen ten aanzien van diefstal en misbruik van (persoons)gegevens of misbruik van de apps als springplank vanwege het zeer brede gebruik. Het is tevens voorstelbaar dat criminelen proberen malafide gelijkende apps te laten installeren middels phishing e.d.

Ook is voorstelbaar dat activistische opportunisten en complotdenkers misbruik zouden kunnen maken van de apps waardoor de effectiviteit van de apps (sterk) daalt, bijvoorbeeld door het doen van valse ziekmeldingen of doelgericht de apps in diskrediet proberen te brengen door het verspreiden van valse informatie en eenzijdige getuigenissen.

Randvoorwaarden voor beperken van nationale-veiligheidsrisico's

Om risico's voor de nationale veiligheid te beperken is hieronder een aantal randvoorwaarden gesteld. Deze randvoorwaarden zijn minimale eisen. Als niet voldaan wordt aan deze randvoorwaarden, en andere keuzes gemaakt worden, ontstaan er zeer grote risico's voor de nationale veiligheid. Door het voldoen aan de randvoorwaarden bij de ontwikkeling van apps zijn risico's voor de nationale veiligheid te verminderen.

Gebruik van contactgegevens en geen locatiegegevens

Het gebruik van zogenoemde *proximity data* (contactgegevens die niet op locatie zijn gebaseerd), waarbij vastgelegd wordt welk apparaat in de buurt van de telefoon van een gebruiker van de apps geweest is, levert de minste risico's voor de nationale veiligheid op. Locatiegegevens van personen hebben de interesse van statelijke actoren. Vanwege de grote voorziene gebruikersgroep van de apps zal dit zeker een interessante bron zijn voor statelijke actoren. Via deze weg kunnen andere landen inzicht krijgen in bewegingen van voor hen interessante personen, en kunnen zij koppelingen maken tussen locaties van verschillende personen. Het gebruik van locatiegegevens (zoals GPS) levert daarom grote

nationale-veiligheidsrisico's op, onder meer omdat metadata ervoor zorgt dat de gegevens mogelijk tot een persoon herleidbaar zijn.

Minimalisatie persoonsgegevens en contactgegevens
De apps moeten zo min mogelijk direct tot personen herleidbare gegevens (persoonsgegevens) opslaan. Herleidbaarheid van data tot personen of apparatuur moet tot een absoluut minimum beperkt worden.

Minimalisatie aanvalsoppervlak
Om risico's voor de nationale veiligheid te beperken is minimalisatie van het aanvalsoppervlak essentieel. Bijvoorbeeld contactgegevens moeten lokaal worden opgeslagen. Het centraal opslaan van contactgegevens levert een dataset op die zeer interessant is voor statelijke actoren. Er bestaat een reële dreiging dat statelijke actoren hun middelen zullen inzetten om deze dataset (of andere datasets) in handen te krijgen, zeker gezien het voorziene grote gebruik van de apps (veel gebruikers en daarmee in potentie een grote dataset). Eventuele kwetsbaarheden in de applicatiesoftware kunnen leiden tot een groot afbreukrisico, als daarmee toegang wordt verkregen tot alle centraal opgeslagen gegevens. Ook bijvoorbeeld afhankelijkheid van (meerdere) cloudleveranciers vergroot het aanvalsoppervlak.

Ontwikkeling apps door betrouwbare aanbieder
Bij de inkoop- en aanbesteding van cruciale diensten kunnen risico's voor de nationale veiligheid ontstaan. Deze risico's kunnen bijvoorbeeld bestaan wanneer vertrouwelijke of gevoelige informatie kan weglekken. Ook kan een sterke afhankelijkheid ontstaan van partijen of landen die niet dezelfde (geopolitieke) belangen delen als Nederland. Het kabinet monitort deze risico's, en heeft hiertoe eind 2018 inkoop- en aanbestedingsbeleid opgesteld. Het identificeren van mogelijke risico's voor de nationale veiligheid bij een opdracht is een verantwoordelijkheid voor de behoeftestellende partij, in dit geval de rijksoverheid. Onderdeel van het inkoop- en aanbestedingsbeleid van de rijksoverheid is het inventariseren van risico's voor de nationale veiligheid.

Om risico's voor de nationale veiligheid te beperken, is het noodzakelijk dat het ontwerp, testen/auditen, onderhoud, beheer, monitoring en ondersteuning van de apps worden uitgevoerd door gekwalificeerde en betrouwbare aanbieders. Dat houdt in dat sprake moet zijn van het contracteren van betrouwbare aanbieders (en onderaanbieders) die aantoonbaar kunnen voldoen aan de gestelde technische beveiligingseisen en tevens voldoende vertrouwen genieten op basis van hun staat van dienst (gerenommeerd bedrijf) en risicoprofiel. Het hierboven genoemde instrumentarium helpt hierbij. Het is onwenselijk om gebruik te maken van producten, diensten of aanbieders uit landen waarvan is vastgesteld dat zij een offensief cyberprogramma gericht tegen Nederlandse belangen voeren. Hierbij geldt dat diverse landen nationale wet- en regelgeving hebben om dienstverleners te dwingen tot medewerking aan inlichtingenactiviteiten. Concreet betekent dit dat de maker bij voorkeur afkomstig is uit Nederland, om te garanderen dat de maker volledig onder Nederlandse wet- en regelgeving en toezicht valt. Indien dit niet mogelijk is, dan heeft met het oog op beperking van de risico's voor de nationale veiligheid een aanbieder uit de Europese Unie de voorkeur, zodat privacywet- en regelgeving van het land van vestiging zich op hetzelfde niveau bevindt als Nederland. Een en ander moet in overeenstemming met de eisen en procedures in de Nederlandse aanbestedingswetgeving plaatsvinden.

Onafhankelijke kwaliteitscontrole
Om te garanderen dat de ontwikkeling, maar ook het beheer en onderhoud van de apps gebeurt op een wijze die de noodzakelijke veiligheid van de toepassingen garandeert voor gebruiker en overheid, is onafhankelijke kwaliteitscontrole onontbeerlijk (door toezichthouders en externe partijen). Concreet houdt dit in dat sprake moet zijn van toetsbare architecturen (waaronder van de infrastructuur, de applicatie en de beveiligingsmaatregelen), een openbaar inzichtelijke broncode en dat deze broncode in eigendom van de rijksoverheid is. Eindgebruikers moeten de authenticiteit van de apps kunnen vaststellen, en moeten kunnen vaststellen dat de geïnstalleerde apps overeenkomen met de openbaar inzichtelijke broncode. De gecontracteerde aanbieder moet hiervan op de hoogte zijn en daar akkoord mee gaan.

Kwaliteit en integriteit gegevens
Het is gegeven de doelstelling van de apps en de basis die dit geeft voor bijvoorbeeld beleidsbeslissingen van belang dat de kwaliteit en de integriteit van de gegevens gewaarborgd zijn.

Aanbevelingen

Gegeven geschetste risico's en randvoorwaarden komen wij tot onderstaande aanbevelingen:

- Pas dataminimalisatie toe
  - Alleen gegevens opslaan en verwerken die noodzakelijk zijn voor doelstelling van de apps
  - Sla de gegevens op zo lang dit noodzakelijk is, rekening houdend met duur van de crisis en de incubatietijd van de ziekte
- Sla gegevens lokaal (decentraal) op
  - Lokale opslag gegevens en lokale controle gegevens
  - Beperk uitwisseling gegevens
  - T.b.v. het beperken van de aanvalsoppervlak
- Gebruik niet herleidbare identificerende nummers t.b.v. anonimiteit
  - Zowel herleidbaarheid naar persoon als apparaat
- Gebruik een veilige verbinding en sla gegevens veilig op
  - Volg hierbij NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)
  - Volg hierbij de NCSC ICT-beveiligingsrichtlijnen voor mobiele apps
- Neem maatregelen t.b.v. het waarborgen van de integriteit en kwaliteit van de gegevens
  - T.b.v. het voorkomen van misbruik en onbetrouwbare data
  - Door bijvoorbeeld het toepassen van logische begrenzingen
- Zorg dat de authenticiteit van de app kan worden geverifieerd
  - I.v.m. malafide apps of phishing door criminelen
- Zorg dat de authenticiteit van de (ziek)meldingen kan worden geverifieerd.
- Betrek onafhankelijke autoriteiten t.b.v. toezicht privacy en testen techniek
  - Betrek in een vroegtijdig stadium relevante toezichthouders (waaronder de Autoriteit Persoonsgegevens)
- Maak het mogelijk om fouten en kwetsbaarheden te kunnen melden en snel te kunnen verhelpen

- Richt tevens monitoring in om misbruik te kunnen detecteren en beschikbaarheid te kunnen waarborgen

- Het is onwenselijk om gebruik te maken van producten, diensten of aanbieders uit landen waarvan is vastgesteld dat zij een offensief cyberprogramma gericht tegen Nederlandse belangen voeren.
  - Hierbij geldt dat diverse landen nationale wet- en regelgeving hebben om dienstverleners te dwingen tot medewerking aan inlichtingenactiviteiten.

Datum
16 april 2020

Ons kenmerk
(10)(2b)

Met vriendelijke groet,

(10)(2e)

(10)(2e)