Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

CIO VWS, CISO VWS

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

Afzender
NCTV
NCSC
AIVD

T 512e

Datum
11 april 2020

memo

Covid-19-apps voor contactonderzoek en nationale veiligheidsaspecten

Het OMT adviseert zo snel mogelijk de mogelijkheden voor ondersteuning van bron- en contactopsporing m.b.v. 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 AVG-wetgeving (zie bijvoorbeeld het recente PEPP-PT-initiatief). Naast het waarborgen van privacy (AVG) is ook het waarborgen van de nationale veiligheid essentieel. In dit stuk wordt ingegaan op de voorwaarden vanuit het perspectief van de nationale veiligheid.

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, met gebruik van gewogen risicoanalyses. NCTV, NCSC en AIVD zijn de rijksoverheidspartijen die de expertise en advisering hiervoor leveren.

Risico's voor de nationale veiligheid

Om maximaal 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. Door aan de voorkant rekening te houden met de risico's rondom de nationale veiligheid wordt bijgedragen aan het creëren van dit draagvlak. Op langere termijn kunnen de apps bijdragen aan een sneller herstel van de Nederlandse samenleving (economisch voortzettingsvermogen, psychische gesteldheid bevolking, enz.) en daarmee ook de nationale veiligheid.

Er bestaat een gekende dreiging vanuit statelijke actoren ten aanzien van onder andere het vergaren van persoonsgegevens en bulkdata. Concreet betekent dit dat de gegevens uit verschillende apps, de apps zelf en de bijbehorende infrastructuur een zeer aantrekkelijke 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 generen.

De omvang van de risico's voor de nationale veiligheid zijn zeer sterk afhankelijk van de wijze waarop een apps opgezet wordt. Met name keuzes over gebruik van locatiegegevens, herleidbare koppeling aan personen en met wie zij contact hebben, wijze van ziekmelden, opslag van data (centraal of decentraal), en de leverancierskeuze hebben een sterke invloed op deze risico's.

Daarnaast is er 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. Deze actoren zetten een brede verscheidenheid aan middelen in om hun doelen te bereiken. Ook is voorstelbaar dat activistische opportunisten en complotdenkers misbruik zouden kunnen maken van de apps waardoor de effectiviteit van de apps (sterk) daalt. Tevens is het voorstelbaar dat criminelen proberen malafide gelijkende apps te laten installeren middels phishing e.d.

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 beperken.

Gebruik van contactgegevens en geen locatiegegevens
Het gebruik van anonieme contactgegevens (*proximity data*), 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 zij 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. De mogelijkheid die bij centrale opslag ontstaat tot het combineren van gegevens en eventuele daarbij behorende metadata zorgt ervoor dat de gegevens mogelijk tot een persoon herleidbaar zijn.

Geen persoonsgegevens en contactgegevens
De apps moet geen tot personen herleidbare gegevens (persoonsgegevens) opslaan. Herleidbaarheid van data tot personen of apparatuur moet tot een absoluut minimum beperkt worden.

Decentrale opslag
Om risico's voor de nationale veiligheid te beperken is decentrale opslag van data essentieel. 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 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.

Ontwikkeling apps door betrouwbare aanbieder
De ontwikkelaar van de apps is van belang voor eventuele risico's voor de nationale veiligheid. Om deze risico's 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 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 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, mits privacywet- en regelgeving van het land van vestiging zich op hetzelfde niveau bevindt als Nederland. Een en ander moet in overeenstemming zijn met de eisen en procedures in de Nederlandse aanbestedingswetgeving. Een gebruiker van de apps dient de mogelijkheid te hebben de authenticiteit van de apps vast te kunnen stellen.

Onafhankelijke kwaliteitscontrole
Om te garanderen dat de ontwikkeling, maar ook het beheer en onderhoud van de apps gebeurt op een wijze die maximale veiligheid van de software 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 openbare broncode en dat deze broncode in eigendom van de rijksoverheid is. 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 apps
    - Sla de gegevens op zo lang dit noodzakelijk is, rekening houdend met duur van de crisis en de incubatietijd
- Sla gegevens 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 TLS-richtlijnen
    - Volg hierbij de NCSC-richtlijnen 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
- Betrek onafhankelijke autoriteiten t.b.v. toezicht privacy en testen techniek
    - Betrek in een vroegtijdig stadium relevante toezichthouders
- 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.