De Winter Information Solutions
Maluslaan 16
1185 LA Amstelveen

(10)(2e) (10)(2e)
(10)(2e)
Telefoon: (10)(2e)

Ministerie van Volksgezondheid, Welzijn en Sport
(10)(2e)

Amstelveen, 15 juli 2020

Betreft: Go/No go-advies

Geachte heer (10)(2e) Beste (10)(2e)

U heeft mij gevraagd advies uit te brengen met betrekking tot de haalbaarheid van de introductie van CoronaMelder vanuit het perspectief van informatiebeveiliging en privacybescherming. Het plan is om 1 september 2020 de app te introduceren voor breed gebruik.

Vanuit privacybescherming en informatiebeveiliging bezien is het – voor zover ik nu kan overzien – mogelijk om tot een positief oordeel te komen voor het breed inzetten CoronaMelder per 1 september 2020. Daarbij moet ik wel een tweetal voorbehouden maken. Ten eerste moet het plan dat ik heb neergelegd met onderzoeken dan tijdig en geheel worden uitgevoerd. Eventuele bevindingen worden opgevolgd, worden weerlegd of eventuele rest risico's worden geaccepteerd. Er is weinig ruimte voor uitloop van meer dan enkele dagen, omdat veel onderzoek staat of valt met de beschikbaarheid van de totale oplossing. Ten tweede moet het door de minister gevraagde advies van de Autoriteit Persoonsgegevens wel beschikbaar zijn.

Rond privacybescherming is veel geregeld. Dat rechtvaardigt de conclusie dat er sprake is van een oplossing waar maximaal wordt ingezet op het borgen van de privacy. Ik licht dat zo nader toe. In landen als Duitsland, Estland, Zwitserland, Finland, Oostenrijk en Italië met een op dezelfde techniek gestoelde app blijkt ook dat er geen ernstige privacyrisico's zijn. De referentie DPIA van de makers van het DP3T-protocol maakt duidelijk dat zij zich op het standpunt stellen dat het mogelijk is dat er juridisch bezien helemaal geen persoonsgegevens worden verwerkt. De analyse voor de eigen DPIA maakt duidelijk dat met de maatregelen de privacyrisico's beperkt zijn. Daarom hoeven deze niet in de weg te staan van een app waar de privacy is geborgd. Momenteel loopt er een second opinion van Privacy Management Partners om aanvullende verbeterslagen te maken. Onzeker blijft echter het advies van de Autoriteit Persoonsgegevens dat de minister gevraagd heeft. Uit hun communicatie is niet helder op te maken, wanneer zij met een advies komen en wat dit advies zal behelzen.

Door het hele project heen speelt informatiebeveiliging een belangrijke rol. Dat zien we terug in het ontwerp, de gemaakte risicoinschattingen, de kwaliteitsslagen bij de softwareontwikkeling, het zeer uitgebreide programma van onderzoeken, de second opinion op de onderzoeken en de actieve monitoring op misbruik met bij behorende opvolging (het security operations center). Hierdoor worden risico's tot een zeer beheersbaar niveau teruggebracht. De kwaliteitsslagen tijdens de softwareontwikkeling en de uitgebreide verificatieslagen moeten leiden tot een app, die aan beveiligingsstandaarden voldoen en waar de minister dat onderbouwd kan aantonen. Dit gaat verder dan de stappen, die in de meeste andere landen voor dit soort apps zijn gezet. Naar mijn mening ligt er nu een aanpak voor, die fors steviger is dan wat in de industrie bij het maken van andere apps gebruikelijk is.

De Winter Information Solutions
Maluslaan 16
1185 LA Amstelveen

(10)(2e) (10)(2e)
(10)(2e)
Telefoon: (10)(2e)

Privacybescherming
CoronaMelder doet veel om de privacy zo goed mogelijk te borgen. Ik loop de belangrijkste punten langs:

1. Er wordt gebruik gemaakt van het DP3T-protocol dat staat voor Decentralized Privacy-Preserving Proximity Tracing. Dit protocol zorgt ervoor dat er bij het gebruik van de app geen sprake is van herleidbaarheid naar een persoon. Anders dan andere apps in diverse andere landen is er geen centrale administratie. De hele inrichting is zo gemaakt dat nergens bekend is wie welke sleutels in handen heeft. Alle bewerkingen worden op de telefoon gedaan. Er worden geen waarschuwingen gestuurd. Een notificatie wordt op het toestel zelf berekend. Bij het opzetten van de app is er sprake van privacy by design en security by design.
2. De app werkt met sleutels, die dagelijks wisselen. Deze zijn volledig willekeurig. Bij het bepalen is geen herleidbaarheid naar de persoon of het toestel. Om te bepalen of een sleutel bij een toestel hoort, moet er binnen 14 dagen na het berekenen van de sleutel fysieke toegang tot het toestel zijn. Het raden van de code is zeer onwaarschijnlijk, omdat er veel combinaties mogelijk zijn (115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936).
3. Sleutels worden niet langer dan 14 dagen bewaard.
4. Via Bluetooth zendt de telefoon een RPI (Rolling Proximity Indicator). Dit kenmerk wisselt iedere 10 tot 20 minuten heeft, waardoor een gebruiker van wie een signaal over langere tijd wordt uitgezonden niet herkenbaar is.
5. Wanneer iemand positief is getest op COVID-19 en zijn of haar sleutels beschikbaar stelt, zouden een beperkt aantal partijen uit netwerkverkeer kunnen afleiden dat er sprake is van een besmetting. Daarom vinden er willekeurig uploads van dummy-gegevens plaats. Zo is niet meer in te schatten of het hier gaat om een besmetting of dummy data.
6. Als een gebruiker na besmetting de sleutels opstuurt om vrij te geven voor andere gebruikers dan moet de GGD dat via een unieke code bevestigen. Daarna worden gepubliceerd voor de andere apps om op te halen. Blijft de bevestiging 24 uur uit dan worden de sleutels weggegooid. Zo worden nepwaarschuwingen voorkomen. De GGD kan alleen de code bevestigen, maar heeft geen inzicht in de sleutels.
7. Als een gebruiker sleutels naar de server verstuurt dan wordt data direct ontkoppelt van het internetadres, zodat er geen herleidbaarheid naar verzender kan ontstaan. Het internetadres wordt alleen voor bewaking op aanvallen gebruikt en binnen zeven dagen verwijderd. Er zijn harde afspraken dat deze gegevens niet voor andere doelen kunnen worden gebruikt.
8. Wanneer de app sleutels ophaalt dan worden deze gebruikt voor een berekening of er een melding moet worden gedaan. Na de berekening worden deze sleutels weggegooid.
9. Als de gebruiker een melding krijgt en wegdrukt dan laat dat geen sporen na. Zo kunnen derden niet zien dat er een melding is afgegeven.
10. Wanneer iemand de app deïnstalleert dan worden de opgeslagen gegevens ook verwijderd.
11. Zoals ik hierna uitleg worden er veel beveiligingsmaatregelen genomen om de data beschermen.

De Winter Information Solutions
Maluslaan 16
1185 LA Amstelveen
(10)(2e) (10)(2e) (10)(2e)
(10)(2e)
Telefoon: (10)(2e)

Informatiebeveiliging

Om compleet beeld te krijgen van de stand van informatiebeveiliging wordt een breed palet aan onderzoeken uitgevoerd. Daarin kijken we enerzijds naar de staat en gedrag van de software, de omgeving van de server, maar ook naar het voldoen aan beveiligingsstandaarden, het bestaan van achterdeuren of het juist niet hebben gebouwd van functionaliteit en het ontworpen cryptografieraamwerk. Omdat het gaat een breed pallet van onderzoeken, is er gekozen om verschillende soorten onderzoek uit te voeren en daarvoor verschillende bedrijven te vragen. Dit onderstreept ook de onafhankelijkheid van de onderzoekers. Omdat naar de aard van de onderzoeken er onvermijdelijk overlap is, ontstaat ook een gezonde vorm van peer-review. Verschillende ogen zien verschillende zaken, waardoor de kans dat iets wordt gemist kleiner wordt. De belangrijkste tests zijn:

1. Penetratietesten. Bij een penetratietest proberen 'hackers' wegen te vinden om in een systeem te komen of te misbruik. Dat digitaal kraken is gericht op het vinden van foutmodi, die een beveiligingsprobleem vormen. Deze testen worden uitgevoerd volgens standaarden. Hierdoor verifiëren dat aan een set minimale standaarden wordt voldaan. De bevindingen worden voorzien van een internationale score voor beveiligingszwakheden (de common vulnerability scoring systeem). Hierdoor is de urgentie genormeerd vastgesteld. Er zijn op dit moment drie pentesten:
    1. De nulmeting. Deze kijkt naar het geheel van de server en de app. Daarbij weten we dat er momenteel nog ontwikkeling plaats vindt. Deze test is begonnen op 3 juli 2020 en loopt nog voort. NFIR voert dit uit. De rapportage is nog niet beschikbaar. Maar deze test schetst wel een beeld dat een voldoende veilige omgeving haalbaar is.
    2. Website Coronamelder.nl. Deze test is uitgevoerd door Hack Defense. Er zijn hier een lage bevinding en twee informatieve bevindingen uitgekomen.
    3. Pentest CoronaMelder. Op 10 augustus 2020 zal NFIR een penetratietest starten met als doel de server en de app te testen. Dit moet eventueel leiden laatste bevindingen voor de livegang op 1 september
2. Codereviews. Bij dit onderzoek wordt de broncode door experts onderzocht. Ze geven zekerheid of daadwerkelijk de software wordt gebouwd, die we verwachten. Daarnaast wordt gekeken of er geen onvoorziene functionaliteit (zoals achterdeuren) worden gebouwd. Tijdens deze onderzoeken wordt ook duidelijk of er beveiligingsproblemen zijn. Waar een penetratietest zoekt door aanvallen uit te voeren, wordt hier door analyse gekeken naar zwakheden. We voeren er twee uit:
    1. De app wordt onderzocht het bedrijf Secura.
    2. De gebouwde serversoftware wordt onderzocht door het bedrijf Radically Open Security.
3. Cryptoraamwerk. Het door het ministerie ontwikkelde framewerk wordt onderzocht door Radically Open Security als een peerreview.
4. Audit. Om er zeker van te zijn dat bij de server de beveiligingsafspraken worden nageleefd, inderdaad aan afspraken rond de beveiliging in het datacenter wordt voldaan, wordt een losse audit uitgevoerd. Deze opdracht kan pas worden verstrekt op het moment dat de productieomgeving beschikbaar is. De recente wisseling van de Belastingdienst naar het CIBG betekent dat ik op zeer korte termijn deze waarborgen nader ga inkleuren.
5. Software distributie. Om te waarborgen dat de broncode van de app, die publiekelijk beschikbaar ook daadwerkelijk dezelfde software als de software die via de app-store beschikbaar komt, wordt een notarisverklaring opgesteld.
6. Overall review. Tot slot voert beveiligingsbedrijf Fox-IT een review uit op het gehele stelsel van verificatieslagen om ervoor te zorgen dat zo compleet mogelijk wordt gecontroleerd dat daadwerkelijk wordt voldaan aan de eisen.

De Winter Information Solutions
Maluslaan 16
1185 LA Amstelveen
(10)(2e) (10)(2e)
(10)(2e)
Telefoon: (10)(2e)

Voordat broncode van de server of de app beschikbaar komt, vinden er diverse kwaliteitsslagen plaats:

1. Er wordt een platform ingezet dat de broncode controleert op inhoud. Met dit systeem kunnen fouten (bugs), onderliggende problemen (code smells) en beveiligingszwakheden worden gevonden. Deze fouten worden actief tijdens het ontwikkelen gezocht. Daarnaast checkt de software op:
    1. Het niet houden aan programmeerstandaarden waardoor de app niet onderhoudbaar zou zijn.
    2. Gebrekkige uitleg in de code waardoor deze door het volume al snel niet meer te onderhouden is.
    3. Verificatie op code die dubbel aanwezig is.
2. Tijdens de ontwikkeling worden unit tests uitgevoerd. Dit betekent dat ieder onderdeel van de software ook los wordt getest van een test over het geheel.
3. Er is een quality assurance team dat handmatig testen uitvoert op de werking van software. Binnen het team wordt de documentatie daarvoor verzameld en beschikbaar gesteld.
4. Een ander team voert zogenaamde code reviews uit op de broncode. Dit betekent dat er handmatig wordt gekeken naar de broncode om zo fouten, beveiligingsproblemen en andere problemen op te sporen.
5. Naast de interne slagen is de broncode vrijgegeven als open-sourcesoftware. Dankzij de inzet van een community manager is er een gemeenschap van kritisch meekijkende experts, die aanvullende feedback geven. Hierdoor is er in de fase voor de livegang aanvullende meerwaarde gecreëerd als kwaliteitsslag.
6. Er komt een coordinated vulnerability disclosure beleid. Dat betekent dat eventuele problemen van derden in ontvangst worden en in overleg met de vinder wordt gekeken wat er moet gebeuren. Zo kunnen ethische hackers problemen aandragen.
7. Intern worden een aantal stappen gezet om de kwaliteit en beveiliging van de totale oplossing (app plus backend) te toetsen:
    1. Penetratietest door pentesters in dienst van de overheid.
    2. Codereview door overheidsreviewers.
8. Verificatie van configuratie en hardening (het veilig instellen van systemen).

Inzet van een Security Operations Center voor bewaking en monitoring dat beschikt over goede SOPs (Standaard Operating Procedures), waardoor bij incidenten er ook eenduidig en goed handelingsperspectief is. Daarnaast werkt het SOC volgens het 4-eyes principe wat betekent dat er altijd bij handelingen iemand meekijkt om fouten te voorkomen of zeer fors te reduceren. Daarnaast wordt er ingezet op het inzetten van een 'high availability omgeving' om de kans op verstoringen op de server zo klein mogelijk te maken. Voor weerbaarheid tegen DDoS-aanvallen is een passende technische oplossing gezocht.

Naast al deze maatregelen wordt er momenteel op Europees niveau beveiligingsonderzoek gedaan naar de laag van Apple en Google. Dit beveiligingsonderzoek wordt uitgevoerd door het al eerder genoemde Radically Open Security.

De Winter Information Solutions
Maluslaan 16
1185 LA Amstelveen

(10)(2e) (10)(2e)
(10)(2e)
Telefoon: (10)(2e)

Op basis van al deze gegevens vorm ik uiteindelijk het gefundeerde totaalbeeld hoe de stand informatiebeveiliging en privacybescherming is op het moment van livegang. Tot slot wil ik nog melden dat ik denk dat het Ministerie van VWS – ondanks het snelle ontwikkeltraject – een zeer zorgvuldig proces voor informatiebeveiliging en privacybescherming doorloopt.

Ik hoop u hierbij voldoende te hebben geïnformeerd.

Met vriendelijke groet,

(10)(2e) (10)(2e)