Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
www.rijksoverheid.nl

Kenmerk
1755492-211084-DICIO

Uw brief

Bijlage(n)
5

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 1 oktober 2020
Betreft Broncode review CoronaMelder

Geachte voorzitter,

Naar aanleiding van de het artikel dd. 29 september jl. in de Volkskrant, over een vermeend probleem met de privacy van CoronaMelder, zijn vragen ontstaan over de bevindingen van het bedrijf 'Radically Open Security' (ROS) en de manier waarop ik uw Kamer daarover heb geïnformeerd. Uw Kamer heeft mij hierover, in het proces van de behandeling van de Tijdelijke wet notificatie-applicatie covid-19, ook vragen gesteld.

Betreffende rapportage is net na verzending van mijn brief van 28 augustus ontvangen. In deze brief meldde ik al dat "de verwachting (…) is dat de beveiligingsonderzoeken die nog lopen de komende dagen geen radicaal ander beeld gaan opleveren". Ik ben van mening dat dit ook het geval is. Directe openbaarmaking van de rapportage was niet mogelijk. Het betreft in dit geval namelijk een onderzoek naar de broncode van de serversystemen van CoronaMelder. De onderzoekers hebben breed gekeken naar systemen, daarbij deden zij ook bevindingen die niet direct over de software van CoronaMelder zelf gaan. Van twee bevindingen moesten bedrijven op de hoogte worden gebracht. De twee betreffende punten zijn internationaal aangemeld onder het 'Common Vulnerability Exposure'-programma. De meldingen hebben CVE-2020-24721 en CVE-2020-24722 als nummer meegekregen. Er is, zoals te doen gebruikelijk, gekozen betrokken partijen (Apple en Google) direct te informeren en enige tijd te geven voorafgaand aan openbaring om bevindingen op te lossen voor publicatie.

Ik wil het vrijgeven zo snel mogelijk én verantwoord doen. Dat is hier ook gebeurd. Mijn voornemen was de rapportage te openbaren met de volgende voortgangsbrief over CoronaMelder die ik verwacht volgende week aan de Tweede Kamer te sturen. Gezien de vragen die deze week zijn ontstaan heb ik besloten dat eerder te doen. Als bijlage bij deze brief ontvangt u de betreffende onderzoeken en de aangepaste duidingsrapportage waarin de bevindingen van een reactie zijn voorzien.

Eén van de bevindingen van ROS is in de media een "privacyprobleem" genoemd. Dat is niet het geval. Het ging om een bewuste functionaliteit in de app gedurende de praktijktest die daarna verwijderd is. Ik licht dat graag toe. Als een gebruiker van CoronaMelder positief getest wordt op corona dan kan deze dat met hulp van de GGD vrijwillig in de app melden. Dat gebeurt in het telefoongesprek dat de GGD voert met mensen die positief zijn getest als start van de reguliere bron- en contactopsporing. Tijdens de praktijktest kon de GGD-medewerker zien of dat zogenaamde "uploaden" van de in de besmettelijke periode uitgezonden willekeurige codes ook daadwerkelijk gelukt was. Dat vinkje is waar de bevinding van ROS over gaat.

Deze functionaliteit was geen gevaar voor de anonimiteit. De GGD-medewerker die je aan de telefoon hebt weet immers al wie je bent, kon niet bij je willekeurige codes zelf en alleen díe medewerker, alleen op dat moment, kon het vinkje zien. Daardoor kon de GGD-medewerker helpen om te bevestigen dat het voor sommige mensen complexe proces was gelukt.

Tegelijkertijd is gebruik van de app vrijwillig. Het is dus belangrijk dat mensen "ja" kunnen zeggen als de GGD vraagt of ze hun willekeurige codes willen uploaden en het alsnog niet doen zonder dat dat zichtbaar is. Zo is zeker dat de GGD-medewerker niet onbedoeld enige vorm van drang uitoefent op het alsnog uploaden van de codes. Om deze reden was deze functionaliteit al verwijderd voordat deze week publicaties verschenen over de bevinding. Hiermee is aan de ene kant vrijwilligheid van gebruik van CoronaMelder nog steviger geborgd, maar aan de andere kant kunnen mensen ook niet geholpen worden bij het zeker stellen dat het uploaden gelukt is.

Advies Autoriteit Persoonsgegevens
In voorbereiding op het debat van maandag as. over de Tijdelijke wet notificatieapplicatie covid-19 stuur ik u hierbij tevens, op verzoek van uw griffie, het advies van de Autoriteit Persoonsgegevens. Er is door de Autoriteit Persoonsgegevens geen nader oordeel uitgebracht.

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Hugo de Jonge