

To: (10)(2e) (10)(2e) @minvws.nl
 Cc: (10)(2e) (10)(2e) @minvws.nl; (10)(2e) (10)(2e) (10)(2e) @minvws.nl
 From: (10)(2e) (10)(2e)
 Sent: Sun 4/19/2020 1:37:00 PM
 Subject: KPMG rapport
 Received: Sun 4/19/2020 1:37:01 PM
[Finale rapportage Ministerie van VWS Corona Apps 19042020definitief.pdf](#)

Hoi (10)(2e),

Bijgevoegd vind je de definitieve versie van het KPMG rapport over de technische veiligheids- en betrouwbaarheidstesten van 6 van de 7 deelnemers van de Appathon. Met (10)(2e) heb ik afgesproken dat je van onderstaande alinea voor de kamerbrief een tekst voor de website kunt maken.

Veiligheid en betrouwbaarheid van de Corona apps zijn uiteraard van cruciaal belang. Daarom heeft KPMG als onafhankelijke partij in opdracht van VWS onderzoek gedaan naar de technische veiligheid en betrouwbaarheid van de aangeboden apps en achterliggende systemen. Vanwege de beperkte tijd is door middel van zogenaamde penetratietesten en een technische beoordeling van de broncodes naar 11 aspecten onderzoek gedaan. Daarbij is de broncode en documentatie gebruikt waarmee de deelnemers de appathon in gegaan zijn. De deelnemers aan de appathon hebben de specifieke rapportages over hun oplossing zaterdag nacht van KPMG ontvangen, zodat zij die hebben kunnen gebruiken om hun oplossing veiliger te maken.

Het onderzoek schetst in het algemeen geen positief beeld van de veiligheid en betrouwbaarheid van de oplossingen. Met de broncode en documentatie waarmee de deelnemers de appathon ingegaan zijn, is geen van de geleverde apps volledig "gereed voor gebruik". Zo is technische documentatie over de componenten grotendeels afwezig en soms laat de codekwaliteit te wensen over. Dat maakt testen arbeidsintensief en onderlinge vergelijking van apps moeilijk. Het onderzoek heeft voor alle geteste oplossingen vanuit de onderzoeksvragen medium tot ernstige bevindingen opgeleverd. De beveiliging van de gegevens die op de telefoon en in sommige gevallen het achterliggende systeem wordt opgeslagen bleek kwetsbaarheden te bevatten, waardoor persoonlijke data zichtbaar kan zijn en soms ook te manipuleren is. Sommige apps verwerken meer persoonlijke informatie dan strikt noodzakelijk en slaan die op zonder versleuteling. Uit het onderzoek van de broncodes blijkt een gebrek aan toepassing van "secure coding" principes. Daardoor bevatten zowel de app als het achterliggende systeem kwetsbaarheden die voorkomen hadden kunnen worden. Sommige apps vragen toegang tot de microfoon of foto's, wat wantrouwen kan opleveren.

Ik trek uit dit onderzoek de conclusie dat het verstandig was om tijdens de appathon ook onafhankelijk onderzoek te laten doen naar de technische veiligheid en betrouwbaarheid van de oplossing. De bevindingen uit het onderzoek maakt dat alle deelnemende oplossingen hun veiligheid moeten en kunnen verbeteren. Daarnaast constateer ik dat in het vervolgtraject de technische veiligheid en betrouwbaarheid van de oplossing meer tijd en aandacht vraagt.

Met vriendelijke groet, warm regards

(10)(2e)

(10)(2e)

(10)(2e)

Ministerie van Volksgezondheid, Welzijn en Sport / Ministry of Health, Welfare and Sport of The Netherlands |

(10)(2e)

Bezoekadres/Visiting: De Resident | Parnassusplein 5 | 2511 XV | Den Haag/The Hague | (10)(2e)

Postadres/Mail: Postbus/POBox 20350 | 2500 EJ | Den Haag/The Hague | The Netherlands

(10)(2e)

| (e)

(10)(2e)

@minvws.nl

(10)(2e)

@minvws.nl