Q&A's veiligheid- en betrouwbaarheidstesten appathon

FACTS

- KPMG is als onafhankelijke partij op 16 april door VWS gevraagd de veiligheid en betrouwbaarheid van de apps te beoordelen.
- KPMG is als mantelpartij van de Rijksoverheid benaderd. Andere veiligheidsexperts die zich hebben aangeboden mee te helpen zijn uitgenodigd in het expert panel deel te nemen.
- Daarvoor hebben de deelnemers aan de appathon op 16 april instructies gekregen KPMG toegang te geven tot een testomgeving en de broncode.
- KPMG heeft geheimhouding: de eventueel gevonden kwetsbaarheden worden niet openbaar gemaakt. Dit om te voorkomen dat kwetsbaarheden misbruikt worden.
- Er is maar beperkt getest in deze fase van de selectie. Dat komt door de beperkte tijd om de testen uit te voeren en de mate van gereedheid en testbaarheid van de oplossingen van de deelnemers. Ook worden de oplossingen tijdens de appathon verder aangepast en verbeterd waardoor niet alle aanpassingen getest kunnen worden.
- KPMG heeft twee soorten testen uitgevoerd: penetratie- of pentesten en een code review. De pentesten hebben als doel om in de app in te breken en informatie te bemachtigen. Daarvoor zijn alle mogelijke geavanceerde technieken gebruikt. Met de code review bekijkt KPMG of er in de broncode verwijzingen staan die de veiligheid en betrouwbaarheid in gevaar brengen.
- De deelnemers hebben zelf de rapportage over de testen gekregen, met advies over hoe de fouten opgelost kunnen worden. Deze worden niet openbaar.
- KPMG heeft met het oog op het maatschappelijke belang van de veiligheid en betrouwbaarheid van de apps ook een openbare rapportage opgesteld. Hierin zijn geen specifieke kwetsbaarheden benoemd maar wel een beeld gegeven over de veiligheid en betrouwbaarheid van de apps.
- Zodra een of meerdere apps geselecteerd zijn, zullen hierop uitgebreide veiligheids- en betrouwbaarheidstesten uitgevoerd worden, ook door meerdere partijen. Zo borgen we ook dat alle gevonden fouten ook daadwerkelijk opgelost zijn.

Q:
Waarop zijn de apps precies getest?

A:

- KPMG is als onafhankelijke partij gevraagd de veiligheid en betrouwbaarheid van de apps te beoordelen
- Hiervoor hebben zij zogenaamde penetratietesten uitgevoerd en bekijken ze de broncode van de apps
- In de penetratietesten, of pentesten, hebben de experts gekeken of zij in de app (en eventuele achterliggende systemen) in kunnen breken, informatie kunnen bemachtigen en de app kapot kunnen maken. Hiervoor hebben zij geavanceerde hacking-technieken gebruikt.
- De experts hebben gekeken of kwaadwillenden in staat zijn om via de app bij gevoelige data op de telefoon te komen, of de communicatie tussen de app en

andere apps en systemen veilig is en of die communicatie overgenomen kan worden. Ook is er getest of kwaadwillenden foute data in de app in kunnen voeren.
- Tevens is de broncode van de apps onderzocht op onnodige communicatie met derden en achterdeurtjes.

Q:
Wat zijn de resultaten van de testen?
A:
- 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".
- Alle deelnemers aan de appathon hebben een uitgebreide set rapporten van KPMG ontvangen waarmee zij hun software veiliger en betrouwbaar maken.

Q:
Is het testen wel eerlijk gedaan? Is een app niet meer getest dan een ander?
A:
- Alle apps zijn in principe op dezelfde manier getest. Dit gebeurde aan de hand van zogenaamde testscripts.
- Omdat de apps verschillend werken, kon niet bij elke app hetzelfde getest worden.
- Elke app is 20 uur getest, verspreid op vrijdag 17 april en zaterdag 18 april.

Q:
Waarom worden de testresultaten niet openbaar gemaakt?
A:
- KPMG heeft bij uitzondering een rapport met een algemene beoordeling van de veiligheid en betrouwbaarheid van de oplossingen, zónder specifieke kwetsbaarheden te benoemen beschikbaar gesteld. Deze is op rijksoverheid.nl gepubliceerd.
- De deelnemers aan de appathon hebben de rapportages van de specifieke veiligheids- en betrouwbaarheidstesten voor hun eigen oplossingen gekregen, met advies hoe zij hun oplossing kunnen verbeteren.
- Als er voor een of meer van deze oplossingen gekozen wordt, wordt de definitieve versie uitgebreid getest door meerdere partijen. Zo weten we zeker dat de eerder gevonden fouten opgelost zijn.
- Zo krijgen we tijdens de appathon zicht op hoe veilig en betrouwbaar de oplossingen zijn en kunnen de deelnemers zelf hun oplossing verbeteren.

Q:
Welke garanties kunt u geven dat de apps niet gehacked kunnen worden?
A:
- Door de veiligheid en betrouwbaarheid van de apps regelmatig en door meerdere partijen te testen, zoals we ook in de appathon hebben gedaan, zij het in een beperkte mate.
- Met deze informatie kunnen de ontwikkelaars de apps continu verbeteren.

- Echter, absolute garanties dat software niet te hacken is, zijn niet te geven

Q:
Wie houdt hierop toezicht?
A:

- Na de beproeving is het proces van informatie ophalen (de marktconsultatie) afgerond. We sluiten het boek en gaan ons beraden op of er een app moet komen, en zo ja, waaraan die app moet voldoen.
- Dan wordt ook het beheer, de doorontwikkeling en het toezicht op de app geregeld.

Q:
Welke informatie kan er bij een hack worden buitgemaakt? Zitten hier medische- of persoonsgegevens bij?
A:

- Een van de eisen is dat er géén persoonsgegevens opgeslagen worden in de app.
- Mocht er ingebroken worden in de app, zal de hacker geen persoonsgegevens vinden.
- Ook voor de medische informatie die de app vastlegt, zoals test uitslagen, eisen we dat deze veilig bewaard worden.

Q:
Kan de betrouwbaarheid van de app beïnvloed worden en wat zijn daarvan de gevolgen voor het werk van de GGD?
A:

- Het proces met de appathon is er juist op gericht geweest om de experts uit verschillende perspectieven bij elkaar te brengen en hun inzichten met elkaar te laten delen.
- De GGD's en het RIVM zijn nauw betrokken bij dat proces om juist input te geven op de betrouwbaarheid van de app.

Q:
Kan er via de app's ingebroken worden bij de GGD?
A:

- Een van de eisen die we stellen is dat de apps veilig communiceren, en alleen als die communicatie noodzakelijk is
- De apps zijn ook getest op veilige communicatie met andere systemen, zoals dat van de GGD.

Internationaal

Q:
Voor Oostenrijk en Tsjechië niet fijn dat Nederland de app die zij voor ogen hebben als onvoldoende beschouwen terwijl zij er al mee bezig zijn. Waarom is voor Nederland de app niet goed genoeg?
A:

- Of een app 'goed genoeg' is hangt sterk af van de rol van de app in het hele pakket aan maatregelen. Die verschillen per land.
- De Nederlandse harde eisen aan de apps zijn mede gebaseerd op de nieuwe Europese Toolkit voor Corona-apps. Of de apps in de andere landen ook aan die eisen zijn getest, is niet duidelijk.
- Dankzij de appathon en de tests die we hebben laten doen door onder andere KPMG hebben we een aantal kwetsbaarheden ontdekt bij de deelnemende apps
- We vermoeden dat de apps in België, Oostenrijk en Tsjechië (en Singapore) dezelfde code gebruiken als de apps die in NL zijn getest.
- We hebben de ontwikkelaars van de apps de specifieke kwetsbaarheden en bevindingen meegegeven, zodat ze deze zo snel mogelijk kunnen oplossen
- Ook hebben we de ministeries van deze landen daarvan op de hoogte gebracht.
- Daarmee helpen we bovenstaande landen om het risico op misbruik van die kwetsbaarheden te verkleinen