KPMG

Securitytest potentiële Corona-apps

Ministerie van VWS
A2000020142

Eindrapportage
—
19 april 2020

Inhoudsopgave

KPMG Advisory N.V.

Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 7890

Vertrouwelijk

Amstelveen, 18 April 2019

Aan de Directie van het Ministerie van VWS

Geachte heer Roozendaal, Beste Ron,

In overeenstemming met ons voorstel van 17 april 2020, met referentie A2000020142, doen wij u hierbij ons rapport toekomen naar aanleiding van onze werkzaamheden.

Het doel van de opdracht zoals aan ons verstrekt was om u inzicht te verschaffen in hoeverre voldoende aandacht is geschonken aan beveiliging en betrouwbaarheid van oplossingen zoals getoond in de Appathon van 18 en 19 april jl, bestaande uit één of meerdere apps, backend systemen en de communicatie met deze systemen.

Aard van de opdracht

De aard van de werkzaamheden houdt in dat wij geen accountantscontrole, beoordelingsopdracht of andere assurance opdracht hebben uitgevoerd. Daarom kan aan dit rapport geen zekerheid met betrekking tot de getrouwheid van financiële of andere informatie worden ontleend.

Ons advies in dit rapport is uitsluitend gebaseerd op de uitkomsten van de overeengekomen werkzaamheden en de uitkomsten daarvan. Indien wij aanvullende werkzaamheden hadden verricht, of een controle-, een beoordelings- of een assurance opdracht zouden hebben uitgevoerd, waren wellicht andere onderwerpen geconstateerd die voor rapportering in aanmerking zouden zijn gekomen. Wij zullen onze rapportage niet aanpassen voor toekomstige veranderingen, aanpassingen in wet en regelgeving of gewijzigde juridische en administratieve interpretaties van wet en regelgeving.

Verantwoordelijkheid van de directie van het Ministerie van VWS

Voor de volledigheid merken wij op dat u verantwoordelijk bent voor de juistheid en de volledigheid van de aan ons, in het kader van bovengenoemde werkzaamheden, ter beschikking gestelde informatie. Wij aanvaarden geen verantwoordelijkheid voor de kwaliteit, juistheid of volledigheid van de aan ons aangeleverde informatie.

Verspreidingskring van het rapport

Het rapport is uitsluitend bedoeld voor u als opdrachtgever. Zonder onze uitdrukkelijke en voorafgaande schriftelijke toestemming is het niet toegestaan deze rapportage, dan wel delen van deze rapportage, te gebruiken voor andere doeleinden, openbaar te maken en/of aan derden te verstrekken. KPMG aanvaardt geen aansprakelijkheid voor het gebruik van deze rapportage anders dan waarvoor deze is opgesteld en aan u als opdrachtgever beschikbaar is gesteld.

Wij bedanken voor de open en constructieve samenwerking bij het verrichten van onze werkzaamheden en de totstandkoming van onze rapportage.

Tot het verstrekken van nadere toelichting zijn wij gaarne bereid.

Hoogachtend,

KPMG Advisory N.V.

Ing. J.A.M. Hermans RE

Partner

Achtergronden onderzoek.

Op 11 april jl.. heeft het Ministerie van VWS (hierna: VWS) met de Uitnodiging slimme digitale oplossingen Corona (hierna: "de Uitnodiging") de markt verzocht voorstellen in te dienen op de volgende vier onderdelen:

1. Slimme digitale oplossingen die kunnen bijdragen aan bron- en contactopsporing;

2. Slimme digitale oplossingen die kunnen bijdragen aan zelfmonitoring en begeleiding op afstand;

3. Overige digitale oplossingen die kunnen bijdragen aan de transitiestrategie;

4. Randvoorwaarden waaronder dergelijke oplossingen kunnen worden ingezet.

Ten aanzien van onderdeel 1 is een zevental partijen gevraagd deel te nemen aan een zogenaamde Appathon (welke plaatsvindt / heeft gevonden op 18 en 19 april 2020), met als doel VWS op een transparante wijze te kunnen laten vaststellen of en in welke mate de oplossing voldoet aan de uitgangspunten genoemd in de Uitnodiging.

Parallel aan deze Appathon heeft VWS KPMG gevraagd de geboden oplossingen van de zeven partijen te onderzoeken, met als doel inzicht te verschaffen in hoeverre voldoende aandacht is geschonken aan beveiliging en betrouwbaarheid van deze oplossingen, bestaande uit één of meerdere apps, back-end systemen en de communicatie met deze systemen.

Het onderzoek dat per leverancier heeft plaatsgevonden bestaat uit twee delen, te weten:

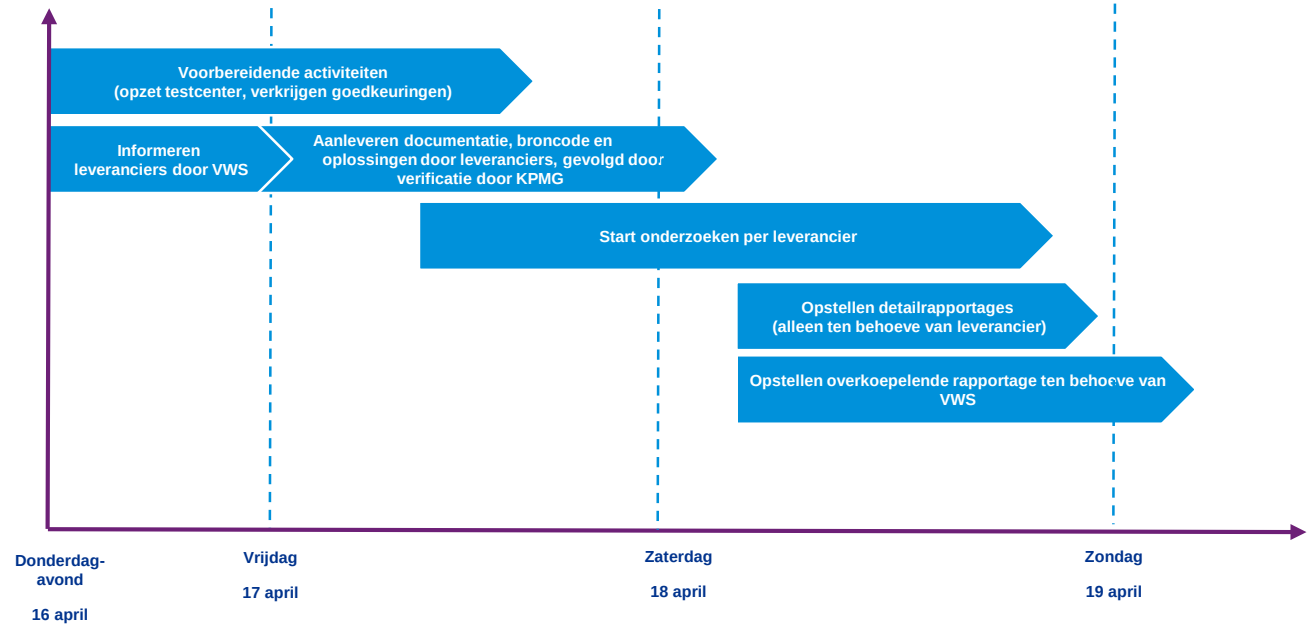
1. Gelimiteerde initiële penetratietest.

2. Quickscan broncode-onderzoek.

Tijdens het onderzoek zijn voor beide delen een aantal onderzoeksvragen opgesteld, onderbouwd met een gestructureerde onderzoeksaanpak, teneinde vergelijkbaarheid van de te onderzoeken aspecten per leverancier te waarborgen. Deze onderzoeksvragen worden in dit rapport nader gespecificeerd.

Achtergronden onderzoek.

Het onderzoek kenschetste zich door de zeer korte tijdlijnen, te weten twee dagen. In onderstaande figuur zijn de activiteiten weergeven welke in deze twee dagen hebben plaatsgevonden.



In deze rapportage zullen wij onze bevindingen van ons onderzoek weergeven, waarbij onze bevindingen zullen worden ingedeeld in de volgende categorieën:

- Algemene bevindingen
- Bevindingen per onderzoeksvraag

Onderzoeksvragen gelimiteerde initiële penetratietest

KPMG heeft de volgende onderzoeksvragen gehanteerd bij de uitvoering van de gelimiteerde initiële penetratietest. Deze onderzoeksvragen zijn geplot op de gehanteerde testmethodiek en consistent uitgevoerd voor alle applicaties in scope, waar mogelijk.

1.	Kan een kwaadwillende gevoelige informatie bemachtigen door het ongeautoriseerd kunnen communiceren met de achterliggende infrastructuur van applicatie X?	**Hoogste prioriteit**
2.	Kan een kwaadwillende de achterliggende infrastructuur van applicatie X compromitteren of ernstig verstoren door het injecteren van kwaadaardige code? Waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem en data niet kan worden gewaarborgd.	
3.	Kan een kwaadwillende foutieve data inbrengen of correcte data verwijderen door misbruik van de achterliggende infrastructuur van applicatie X? Waardoor de data in de achterliggende infrastructuur minder betrouwbaar wordt en niet meer goed kan worden bepaald welke gebruikers COVID19 infectie hebben en welke niet.	
4.	Kan een kwaadwillende de communicatie tussen applicatie X en de achterliggende infrastructuur onderscheppen en/of misbruiken (het kanaal zelf of bijvoorbeeld via de API)? Dit scenario heeft een hogere kans bij het gebruik van publieke hotspots zoals guest Wi-Fi en/of publieke hotspots.	
5.	Kan een kwaadwillende gevoelige data verkrijgen uit de opslagruimte van applicatie X op het mobiele apparaat van de eindgebruiker? Dit scenario kan zich voordoen als het mobiele apparaat kwetsbaar is en applicatie X gevoelige data (bewust of onbewust) op slaat op het apparaat. Hierdoor kan de privacy van de gebruiker alsmede mogelijke andere gebruikers (als hierover ook data is opgeslagen doordat deze gebruikers bijvoorbeeld in de buurt waren) worden aangetast.	
6.	Kan een kwaadwillende communicatie tussen applicatie X en de achterliggende infrastructuur compromitteren door misbruik van andere kanalen dan het primaire kanaal (de te verwachten API-interface)? Denk hierbij aan aanvullende kanalen zoals e-mail, SMS of andere TCP/UDP netwerkinterfaces.	**Laagste prioriteit**

Onderzoeksvragen gelimiteerde initiële penetratietest

KPMG heeft de volgende onderzoeksvragen gehanteerd bij de uitvoering van het quickscan broncode-onderzoek. Deze onderzoeksvragen zijn omgezet in een “wasstraat” waar geautomatiseerde en manuele onderzoeken consistent uitgevoerd voor alle applicaties in scope, waar mogelijk.

7.	Wat is het algemene beeld van de (technische) kwaliteit van de broncode van de applicatie?
8.	Worden er door automatische tooling in de “wasstraat” reële kwetsbaarheden inzake de betrouwbaarheid en beveiligbaarheid in de broncode gevonden?
9.	Zijn er andere data-uitgangen (inclusief logging) in de broncode te vinden die niet in het ontwerp zijn gedefinieerd?
10.	Is de geleverde software (zowel front-end als back-end) voor de goede werking afhankelijk van externe bibliotheken? Zo ja zijn deze bibliotheken courant, worden ze onderhouden en/of bevatten ze bekende kwetsbaarheden inzake de betrouwbaarheid en beveiligbaarheid?
11.	Is de broncode opgezet in lijn met onze verwachtingen vanuit de technische en functionele documentatie? (Zijn bijvoorbeeld beschreven privacy mechanismen geïmplementeerd, past de omvang bij de beschrijving, etc.)?

Beperkingen van het onderzoek

Deelonderzoek met beperkte diepgang

- Tijdens ons onderzoek hebben wij de gebruikte apps, de backend alsmede communicatie tussen de componenten met een beperkte diepgang kunnen onderzoeken (als gevolg van de korte tijdslijnen).

- Daarnaast willen we er op wijzen dat de wijze van de implementatie van het complete concept en het naleven van de juiste beheer- en beveiligingsmaatregelen bepalend zijn voor het kunnen voldoen aan de voor deze concepten benodigde security en privacy vereisten. We willen er dan benadrukken dat een integraal security en privacy onderzoek gericht op het gehele concept bestaande uit organisatie, processen en technologie van belang is alvorens over te gaan tot volledige implementatie.

Borging van de anonimiteit van de leveranciers

- De resultaten van het onderzoek zijn gericht op het verschaffen van algemene inzichten te gebruiken door de commissie bij bevraging van de leveranciers. De resultaten van het onderzoek zijn niet bedoeld als selectie-instrument. In deze rapportage zullen geen verwijzingen naar specifieke leveranciers worden gedaan.

Gelet de zeer korte doorlooptijd van het onderzoek willen we wijzen op de volgende beperkingen van het onderzoek:

- Een beperkt aantal gedetailleerde testactiviteiten heeft niet kunnen plaatsvinden, door onder meer het niet tijdig beschikbaar zijn van de broncode, van de benodigde testomgeving alsmede tools te gebruiken voor deze test. Dit betekent dat mogelijk niet alle issues zijn gevonden. In onze rapportages zijn de situaties waar geen detail testactiviteiten hebben kunnen plaatsvinden aangemerkt.

- Voor een beperkt aantal bevindingen heeft geen additioneel diepgaand nader onderzoek plaats kunnen vinden, met als gevolg dat een aantal van deze bevindingen mogelijkerwijs na nader onderzoek als een zogenaamde "false-positive" betiteld zouden kunnen worden.

- Detailbevindingen van de penetratietesten en source code reviews zijn niet in detail afgestemd met de leverancier (zogenaamd "hoor-en-wederhoor"). Dit kan als gevolg hebben dat een aantal detailbevindingen bijgesteld dienen te worden, op basis van deze validatie.

- We hebben het onderzoek gedaan aan de hand van de door de leverancier beschikbaar gestelde documentatie, broncode alsmede apps en backend systemen. We hebben niet kunnen vaststellen of de geleverde documentatie en broncode volledig is. Daarnaast zijn er mogelijk aanpassingen gedaan aan de apps, backends of broncode tijdens ons onderzoek. Deze wijzigingen zijn niet meegenomen in de resultaten van ons onderzoek.

Beperkingen van het onderzoek - vervolg

Beperkingen ten aanzien van de gelimiteerde initiële penetratietesten:

- Het testen van iOS-apps brengt bepaalde inherente beperkingen met zich mee. Zo heeft Apple haar operating system (iOS) op een dergelijke manier beveiligd waardoor wij (afhankelijk van de iOS-versie) niet alles kunnen testen. Tevens kunnen wij maar beperkt testen en dus niet alle versies/apparaten combinaties afdekken.

- Mobiele apparaten hebben bepaalde inherente kwetsbaarheden welke niet onderzocht worden bij het uitvoeren van een penetratietest op een mobiele ap plicatie. Zo worden bijvoorbeeld mogelijk bepaalde unieke identifiers van geïdentificeerde bluetooth-apparaten opgeslagen in de logbestanden van mobiele apparaten. Dergelijke inherente kwetsbaarheden worden niet onderzocht tijdens een penetratietest op een applicatie.

- Met behulp van een beveiligingstest kan alleen worden aangetoond of het mogelijk is aanwezige beveiligingsmaatregelen te doorbreken. Er kan niet met zekerheid worden gesteld dat geïmplementeerde beveiligingsmaatregelen niet kunnen worden doorbroken. Een aanvaller met ongelimiteerd budget, kennis en tijd zal vrijwel altijd kunnen slagen in het doorbreken van de beveiliging. Tevens betreffen de werkzaamheden van KPMG een tijdsgebonden inspanning, waardoor niet alle mogelijke zwakheden uitputtend kunnen worden getest.

- Bij het uitvoeren van een beveiligingstest wordt gewerkt met de op dat moment bij KPMG bekende zwakheden en aanvalstechnieken. Het resultaat van een beveiligingstest is daarom altijd een momentopname betreffende zowel kennis van zwakheden en aanvalstechnieken, als getroffen beveiligingsmaatregelen.

Beperkingen ten aanzien van het quickscan broncode-onderzoek:

- Het quickscan broncode-onderzoek beperkt zich tot de door de leveranciers geleverde broncode. Er is beperkt navraag gedaan of de software compleet was en alles was opgeleverd.

- Er wordt in alle apps gebruik gemaakt van aanvullende standaard software componenten (zoals besturingssystemen, database- en webserversoftware), netwerk-voorzieningen en -protocollen. Kwetsbaarheden in deze componenten zijn niet in kaart gebracht.

- Er is sprake van een tijdsgebonden inspanning en de ingezette tooling is niet voor elk softwareplatform gelijk. Dit betekent dat mogelijk niet alle issues zijn gevonden en dat ook niet alle bevindingen volledig konden worden gevalideerd.

KPMG

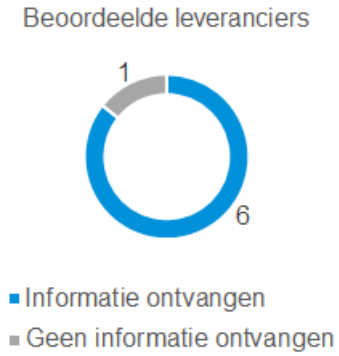
Algemene bevindingen en observaties

Algemene bevindingen - deelnemende leveranciers

Leveranciers meegenomen in het onderzoek

Op de avond van 16 april jl zijn zeven deelnemers van de Appathon door VWS geïnformeerd over hun deelname, alsook de informatiebehoefte van KPMG. KPMG heeft met de verschillende leveranciers een intake gedaan en gevalideerd of de benodigde informatie (bestaande uit technische documentatie, source code, app(s) en andere benodigde informatie) door de leverancier aangeleverd is.

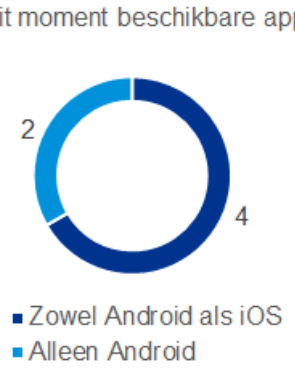
Op basis van de validatie waarin geconstateerd is dat de benodigde informatie niet kon worden verstrekt, is besloten één van de leveranciers uit te sluiten van verder onderzoek.



In het resterende deel van deze rapportage worden dan ook geen bevindingen ten aanzien van deze leverancier weergegeven.

Beschikbare apps gerelateerd aan Operating System

Tijdens de validatie van gegevens is tevens gebleken dat niet alle leveranciers op dit moment beschikken over een app op zowel het Androïd als iOS operating system.

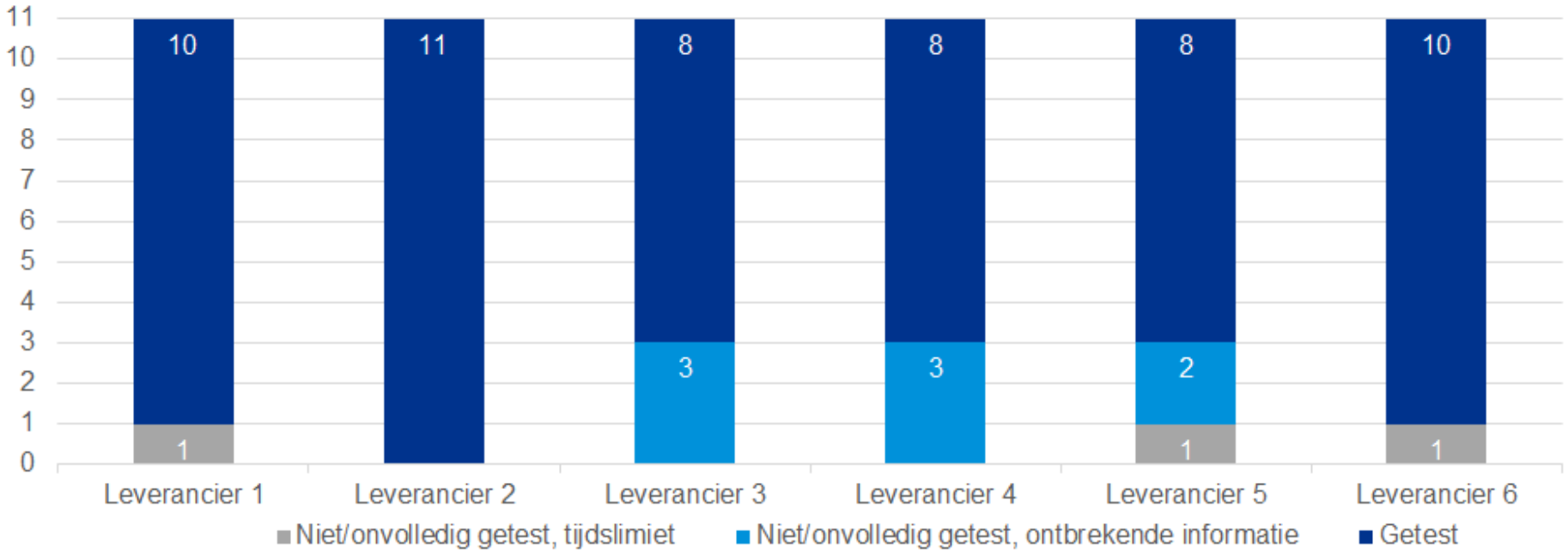


Er waren geen leveranciers die alleen een op iOS gebaseerde apps hebben ontwikkeld.

Algemene bevindingen - onderzoeksvragen

Zoals reeds toegelicht in dit rapport hebben wij onderzoek uitgevoerd op basis ven 11-tal onderzoeksvragen. Tijdens het onderzoek zijn we bij een aantal leveranciers niet in staat geweest om alle testactiviteiten voor het beantwoorden van de onderzoeksvragen uit te voeren, door niet beschikbaar zijn van alle relevante informatie, beschikbaarheid apps, deels door het deels niet beschikbaar zijn van testinfrastructuur en testtools, alsook door tijdgebrek van de testers.

In onderstaande figuur wordt per leverancier weergegeven welke onderzoeksvragen we wel of niet hebben kunnen beantwoorden.



** De gebruikte nummering van leveranciers in dit rapport correspondeert NIET met de lijst van leveranciers zoals gepubliceerd door VWS*

Algemene observaties

Algemene observaties van de gelimiteerde initiële pentesten

- De ontwikkelaars van de applicaties hebben over het algemeen geen "secure coding" principes toegepast waardoor algemeen bekende en dus te verwachten beveiligingsmaatregelen niet zijn geïmplementeerd. Dit is ook van toepassing voor de achterliggende infrastructuur (misconfiguraties, verouderde software, beheerinterfaces exposed, etc.). Hierdoor ontstaan (ernstige) kwetsbaarheden die eenvoudig voorkomen hadden kunnen worden.

- In aanvulling op bovenstaande, willen we specifiek onder de aandacht brengen dat apps gebruik maken van "hardcoded" wachtwoorden die dus leesbaar zijn opgenomen in de leesbare broncode. Het is gebleken dat met deze wachtwoorden toegang kon worden verkregen tot databases en/of de achterliggende infrastructuur (inclusief datasets buiten het domein van de te testen COVID applicatie).

- De achterliggende infrastructuur (inclusief de API) kan veel al misbruikt worden zonder benodigde identificatie/authenticatie. Daar waar wel een beveiliging is toegepast is deze vaak eenvoudig te omzeilen door kwetsbare implementatie, of het niet of niet goed valideren van bijvoorbeeld beveiligingscertificaten, of het gebruik van self-signed certificates. Hierdoor kan veelvuldig toegang worden verkregen tot vertrouwelijke data en/of kan foutieve data worden opgevoerd.

- Bij het ontwerp van de applicaties is niet altijd uit gegaan van het principe om zo min mogelijk gevoelige gegevens op de telefoon van de eindgebruiker op te slaan. Data die wordt opgeslagen wordt ook nog eens zonder versleuteling opgeslagen.

- Door de gewenste functionaliteit (track/trace) zijn er bij de Android telefoons relatief veel toegangspermissies nodig, daar zitten ook enkele op het eerste gezicht vreemde verzoeken bij zoals toegang tot de microfoon of foto's. De gewenste permissies zijn mogelijk te verklaren vanuit de gewenste functionaliteit maar de eindgebruiker zal dit naar waarschijnlijkheid ook wantrouwen en niet accepteren.

Algemene observaties - vervolg

Algemene observaties van het quickscan broncode-onderzoek

- De aangeleverde software kent een behoorlijke diversiteit in de mate waarin ze "gereed voor gebruik" zijn: geen van de systemen is echter "af". Dit verhindert ook een goede vergelijkende beoordeling van de bevindingen; waar bijvoorbeeld in één applicatiecomponent een matig hashing algoritme wordt gebruikt ontbreekt deze functionaliteit bij andere oplossingen in het geheel.

- Technische documentatie over de componenten is grotendeels afwezig gebleken. De broncode-onderzoekers hebben veel tijd besteed aan het uitzoeken hoe de componenten in elkaar zaten, (zo nodig) gecompileerd moesten worden en werkten.

- Algemene maatregelen om codekwaliteit te bevorderen zijn beperkt aangetroffen. We zagen afwijkingen van coding standaarden en "magic literals" (een anti-patroon waarbij nummers en tekenreeksen direct in de code gebruikt worden). Verder zijn er ook weinig unit testen en maar beperkt inline documentatie aangetroffen in de broncode .

Detail bevindingen per onderzoeksvraag

Onderzoeksvraag 1

1. Kan een kwaadwillende gevoelige informatie bemachtigen door het ongeautoriseerd kunnen communiceren met de achterliggende infrastructuur van applicatie X?

Leverancier	Test
1	✓
2	✓
3	—
4	—
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- De ontwikkelaars van de applicaties hebben over het algemeen geen "secure coding" principes toegepast waardoor algemeen bekende en dus te verwachten beveiligingsmaatregelen niet zijn geïmplementeerd. Dit is ook van toepassing voor de achterliggende infrastructuur (misconfiguraties, verouderde software, beheerinterfaces exposed, etc.). Hierdoor ontstaan (ernstige) kwetsbaarheden die eenvoudig voorkomen hadden kunnen worden.
- Het gebruik van "hardcoded" wachtwoorden die dus leesbaar zijn opgenomen in de leesbare broncode. Hierdoor kon toegang tot gevoelige data worden verkregen.
- De achterliggende infrastructuur (inclusief de API) kan veelal misbruikt worden zonder benodigde identificatie/authenticatie. Daar waar wel een beveiliging is toegepast is deze vaak eenvoudig te omzeilen door kwetsbare implementatie, of het niet of niet goed valideren van bijvoorbeeld beveiligingscertificaten, of het gebruik van self-signed certificates. Hierdoor kan veelvuldig toegang worden verkregen tot vertrouwelijke data en/of kan foutieve data worden opgevoerd.
- Een kwaadwillende kan de achterliggende infrastructuur manipuleren omdat er geen of zeer beperkte controle wordt uitgevoerd op de data die van/naar deze infrastructuur verstuurd wordt.

Onderzoeksvraag 2

2. Kan een kwaadwillende de achterliggende infrastructuur van applicatie X compromitteren of ernstig verstoren door het injecteren van kwaadaardige code? Waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem en data niet kan worden gewaarborgd.

Leverancier	Test
1	X
2	✓
3	✓
4	—
5	—
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- De achterliggende infrastructuur bevat diverse (ernstige) kwetsbaarheden die misbruikt kunnen worden waardoor een aanvaller toegang krijgt tot de data (lezen en/of manipuleren) en ook mogelijke toegang tot het onderliggende besturingssysteem. Betreft onder andere:
  - Onveilige configuratie van besturingssystemen, databases en (applicatie)diensten
  - Verouderde software
  - Beheerinterfaces exposed naar het internet (adminportals, databases, etc.)
- Tevens kan een kwaadwillende de achterliggende infrastructuur manipuleren omdat er geen of zeer beperkte controle wordt uitgevoerd op de data die van/naar deze infrastructuur verstuurd wordt.

Onderzoeksvraag 3

3. Kan een kwaadwillende foutieve data inbrengen of correcte data verwijderen door misbruik van de achterliggende infrastructuur van applicatie X? Waardoor de data in de achterliggende infrastructuur minder betrouwbaar wordt en niet meer goed kan worden bepaald welke gebruikers COVID19 infectie hebben en welke niet.

Leverancier	Test
1	✓
2	✓
3	—
4	—
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- De achterliggende infrastructuur (inclusief de API) kan veelal misbruikt worden zonder benodigde identificatie/authenticatie. Daar waar wel een beveiliging is toegepast is deze vaak eenvoudig te omzeilen door kwetsbare implementatie, of het niet of niet goed valideren van bijvoorbeeld beveiligingscertificaten. Hierdoor kan toegang worden verkregen tot vertrouwelijke data en/of kan foutieve data worden opgevoerd.
- De ontwikkelaars van de applicaties hebben over het algemeen geen "secure coding" principes toegepast waardoor algemeen bekende en dus te verwachten beveiligingsmaatregelen niet zijn geïmplementeerd. Dit is ook van toepassing voor de achterliggende infrastructuur (misconfiguraties, verouderde software, beheerinterfaces exposed, etc.). Hierdoor ontstaan (ernstige) kwetsbaarheden die eenvoudig voorkomen hadden kunnen worden.

Onderzoeksvraag 4

4. Kan een kwaadwillende de communicatie tussen applicatie X en de achterliggende infrastructuur onderscheppen en/of misbruiken (het kanaal zelf of bijvoorbeeld via de API)? Dit scenario heeft een hogere kans bij het gebruik van publieke hotspots zoals guest Wi-Fi en/of publieke hotspots.

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	X
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- Applicatie en de achterliggende infrastructuur doen geen of beperkte controles op identificatie en authenticatie van de zender/ontvanger (ook niet in het geval waar certificaten worden gebruikt omdat zogenaamde certificate pinning niet wordt toegepast). Hierdoor kan een aanvaller eenvoudig toegang krijgen tot de communicatie door een man-in-the-middle aanval. Dit soort aanvallen zijn eenvoudig op te zetten bij publieke hotspots.
- Bij de communicatie tussen de app en de achterliggende infrastructuur wordt gebruik gemaakt van zwakke versleuteling.

Onderzoeksvraag 5

5. Kan een kwaadwillende gevoelige data verkrijgen uit de opslagruimte van applicatie X op het mobiele apparaat van de eindgebruiker? Dit scenario kan zich voordoen als het mobiele apparaat kwetsbaar is en applicatie X gevoelige data (bewust of onbewust) op slaat op het apparaat. Hierdoor kan de privacy van de gebruiker alsmede mogelijke andere gebruikers (als hierover ook data is opgeslagen doordat deze gebruikers bijvoorbeeld in de buurt waren) worden aangetast.

Leverancier	Test
1	✓
2	✓
3	—
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- Bij het ontwerp van de applicaties is niet altijd uit gegaan van het principe om zo min mogelijk gevoelige gegevens op de telefoon van de eindgebruiker op te slaan. Data die wordt opgeslagen wordt ook nog eens zonder versleuteling opgeslagen.
- Tevens zijn niet alle applicaties ontworpen/geïmplementeerd met een adequaat wachtwoordbeleid.

Onderzoeksvraag 6

6. Kan een kwaadwillende communicatie tussen applicatie X en de achterliggende infrastructuur compromitteren door misbruik van andere kanalen dan het primaire kanaal (de te verwachten API-interface)? Denk hierbij aan aanvullende kanalen zoals e-mail, SMS of andere TCP/UDP netwerkinterfaces.

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	—
6	X

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- In een paar gevallen maken de applicaties en de achterliggende infrastructuur gebruik van additionele kanalen (naast het primaire kanaal, de API). Door het gebruik van deze additionele kanalen is er een risico op extra kwetsbaarheden alsmede het risico dat een andere partij de gegevens kan correleren tot groepen of zelfs individuele personen. Bijvoorbeeld door herleidbaarheid van identificatie gegevens van de telefoon (SMS, Bluetooth, UUID, telefoonnummers, etc.) of andere herleidbare/correleerbare informatie.

Onderzoeksvraag 7

7. Wat is het algemene beeld van de (technische) kwaliteit van de broncode van de applicatie?

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- De applicaties zijn in het algemeen klein en hebben slechts beperkte technische schuld (de verwachte benodigde inspanning om een oplossing voor de bevindingen te implementeren).
- Op één uitzondering na konden we de geleverde applicatiecomponenten met tools analyseren wat betekent dat de onderzoekers waar nodig de broncode ook konden compileren.
- Wel zijn er weinig maatregelen aangetroffen die codekwaliteit bevorderen. Hierdoor zijn nog een behoorlijk aantal afwijkingen, inclusief “magic literals”, van de “coding standards” aangetroffen. Ook wordt er slecht beperkt gebruik gemaakt van unit testen. In vrijwel alle oplossingen zijn in de inline documentatie “Todo’s” en “Fixme’s” aangetroffen die er op duiden dat de oplossing niet af is. Het verschil in technische kwaliteit tussen prototypen en nagenoeg volwassen implementaties is duidelijk merkbaar.

Onderzoeksvraag 8

8. Worden er door automatische tooling in de “wasstraat” reële kwetsbaarheden inzake de betrouwbaarheid en beveiligbaarheid in de broncode gevonden?

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- In alle oplossingen zijn kwetsbaarheden gevonden waar aandacht aan moet worden besteed. De gevonden kwetsbaarheden in de broncode zijn gedocumenteerd en worden aan de leveranciers gemeld.
- Hierbij merken wij op dat in een aantal gevallen er geen (of beperkt) authenticatie was geïmplementeerd in de communicatie met de back-end applicatie en dat ook andere beveiligingsmaatregelen in de broncode in enkele gevallen ontbraken.

Onderzoeksvraag 9

9. Zijn er andere data-uitgangen (inclusief logging) in de broncode te vinden die niet in het ontwerp zijn gedefinieerd?

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- Er zijn geen data-uitgangen aangetroffen die niet werden verwacht.
- Wel zijn er, met name, locatiegegevens beschikbaar in de apps, en soms zelfs doorgegeven aan het back-end systeem, waar verder (nog) niets mee wordt gedaan; dit kan het vertrouwen van gebruikers in de app schaden. Daarnaast is het in theorie mogelijk dat de leverancier deze gegevens in de toekomst wél verwerkt zonder dat de gebruiker daarvan op de hoogte gesteld wordt – de permissie om de gegevens vanuit de app benaderbaar te maken is immers reeds gegeven bij de initiële installatie.
- Een aandachtspunt is dat in een aantal oplossingen de foutafhandeling niet correct is geïmplementeerd; hierdoor bestaan risico's dat foutboodschappen met gevoelige gegevens ongewenst op bijvoorbeeld schermen wordt getoond.

Onderzoeksvraag 10

10. Is de geleverde software (zowel front-end als back-end) voor de goede werking afhankelijk van externe bibliotheken? Zo ja zijn deze bibliotheken courant, worden ze onderhouden en/of bevatten ze bekende kwetsbaarheden inzake de betrouwbaarheid en beveiligbaarheid?

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- Voor de meeste oplossingen wordt gebruik gemaakt van frameworks en bibliotheken. Een enkele oplossing gebruikt hierin de laatste versies en geautomatiseerde methoden (dependency managers) om dat zo te houden. Andere oplossingen gebruiken verouderde versies; in een aantal daarvan zijn ook kwetsbaarheden bekend.

Onderzoeksvraag 11

11. Is de broncode opgezet in lijn met onze verwachtingen vanuit de technische en functionele documentatie? (Zijn bijvoorbeeld beschreven privacy mechanismen geïmplementeerd, past de omvang bij de beschrijving, etc.)?

Leverancier	Test
1	✓
2	✓
3	✓
4	✓
5	✓
6	✓

✓ Getest

X Niet/onvolledig getest, tijdslimiet

— Niet/onvolledig getest, ontbrekende informatie

- Er is in het algemeen zeer beperkt documentatie aangetroffen; in het algemeen is wel de grofweg functionaliteit aangetroffen zoals die vanuit de pitches is begrepen. Wel is bij een aantal oplossingen nog niet alle benoemde functionaliteit geïmplementeerd.
- De verwachte uitrol van de API voor het uitwisselen van Bluetooth identifiers door Apple en Google is in enkele gevallen de reden voor het (nog) ontbreken van functionaliteit.
- Op één oplossing na, die met een telefoonnummer werkt, wordt beoogd dat gegevens van de gebruiker anoniem worden doorgegeven. Specifieke privacy mechanismen zijn niet aangetroffen.

Appendices

1. Scope
2. Aanpak

Scope

zoals beschreven in ons voorstel d.d. 17 april
met als referentienummer A2000020142

Scope

Scope van de gelimiteerde initiële penetratietest

Voor de gelimiteerde initiële penetratietest gebruiken wij een scenario-gebaseerde aanpak waarbij wij kwetsbaarheden onderzoeken gebaseerd op de OWASP Mobile Top 10 (versie 2016) en de OWASP Top 10 (versie 2017). De scope van de initiële penetratietest bestaat uit de volgende drie componenten:

- COVID-19 app. Hierbij zullen wij onder andere risico's 'M2: Insecure Data Storage', en 'M5: Insufficient Cryptography', onderzoeken om te bepalen in hoeverre gevoelige informatie op een onveilige manier bewaard wordt.

- Communicatie tussen app en backend. Hierbij zullen wij onder andere risico's 'M3: Insecure Communication' en 'M5: Insufficient Cryptography‘ onderzoeken. Wij richten ons hierbij op het scenario dat een aanvaller toegang heeft tot het lokale netwerk van de eindgebruiker, toegang heeft tot het mobiele apparaat van de eindgebruiker, of als Man-in-The-Middle kan acteren.

- Backend-interface. Hierbij zullen wij onder andere risico's 'M10: Extraneous Functionality', 'A1: Injection', en 'A3: Sensitive Data Exposure' onderzoeken. Hierbij richten wij ons op het ongeautoriseerd ontsluiten van data uit de backend, het ongeautoriseerd aanpassen van data in de backend, en het onbeschikbaar maken van de backend (met uitzondering van Distributed Denial-of-Service (DDoS) aanvallen).

Scope van het quickscan broncode-onderzoek

Het quickscan broncode-onderzoek zal zich richten op de door de leverancier opgeleverde broncode en overige artefacten inclusief documentatie. Er zal, gezien het gewenste tijdspad, geen navraag gedaan worden naar op het oog missende elementen; deze elementen zullen als detailbevinding worden gerapporteerd. De kwaliteit van onderliggende softwarecomponenten, zoals besturingssystemen, database- en webserversoftware, is geen onderdeel van de scope.

Aanpak

zoals beschreven in ons voorstel d.d. 17 april
met als referentienummer A2000020142

Aanpak

Wij voeren een ***gelimiteerde initiële penetratietest*** uit, met een maximale gegeven doorlooptijd van 24 uur, op de COVID-19 app, de bijbehorende backend en de communicatie tussen de app en de backend volgens het "white box"-principe. Dit houdt onder andere in dat wij voorafgaand uitgebreide toegang krijgen tot documentatie, systeemconfiguratie, en andere opgevraagde informatie. We zullen geen uitvoerige systeemconfiguratiereviews uitvoeren, maar zullen deze informatie gebruiken voor het efficiënt uitvoeren van onze testen.

Tegelijkertijd krijgen we een beeld over wat een aanvaller mogelijk zou kunnen doen indien deze informatie niet beschikbaar is voor hem. Op basis van deze informatie stellen wij vast welke scenario's het meest relevant zijn om te testen tijdens de penetratietest. Op basis van deze scenario's doorlopen wij de volgende drie fases van onze penetratietest:

1. *Identificatiescanfase*: verschillende identificatiescans uitvoeren op de backend-omgeving. Met deze stap verkrijgen wij gedetailleerde informatie over welke poorten en services actief zijn.

2. *Kwetsbaarhedenscan*: wij gebruiken efficiënte tools die bekende kwetsbaarheden identificeren in systemen. Deze tools en scans worden toegepast op de backend-omgeving. Ook wordt er handmatig gescand voor eventuele kwetsbaarheden, zowel op infrastructuur- als applicatieniveau die ingaan op de app, de backend en de communicatie tussen de app en de backend.

3. *Uitbuiting*: wij voeren handmatige controles uit om vast te stellen of de in de vorige stappen verkregen kwetsbaarheden daadwerkelijk aanwezig zijn (de zogenaamde “false positive”-verificatie). Wij testen verder handmatig op kwetsbaarheden en buiten deze uit waar mogelijk. Op deze manier kunnen wij de impact bepalen van de kwetsbaarheden.

In het ***quickscan broncode-onderzoek***, met een maximale gegeven doorlooptijd van 24 uur, met nadruk op de Betrouwbaarheid zullen we de opgeleverde broncode van zowel de front- en (indien van toepassing) backend-applicatie inspecteren. Met behulp van automatische tooling zullen we veel gebruikte softwaremetrieken zoals het aantal regels code (LOC), Complexiteit en Duplicatie bepalen. Vanuit beschikbare tooling voor het specifieke ontwikkelplatform zullen we zo mogelijk bevindingen krijgen op Betrouwbaarheid, Beveiligbaarheid en Onderhoudbaarheid. Vanuit de focus van dit onderzoek zullen we de bevindingen op *Betrouwbaarheid* en *Beveiligbaarheid* handmatig nalopen.

We zullen verder controleren of de software afhankelijk is van externe bibliotheken, of deze bibliotheken courant zijn en of er voor deze bibliotheken bevindingen op het gebied van Betrouwbaarheid en Beveiligbaarheid bekend zijn.

Ten slotte, zullen we controleren of de broncode in lijn is met onze verwachtingen die gebaseerd zijn op de technische en functionele documentatie en of er data-uitgangen of interfaces zijn (inclusief logbestanden) behalve die zijn gespecificeerd. We zullen daarbij aandacht geven of de beschreven privacy-mechanismen zijn geïmplementeerd. Als er cryptografische algoritmen worden gebruikt (binnen de geleverde software) dan zal worden nagelopen of deze algoritmen veel gebruikt getest en actueel zijn.

Ing. J.A.M. Hermans RE

Partner
KPMG Advisory N.V.
Tel: + 31 20 656 8394
Mob: + 31 6 51 366 389
hermans.john@kpmg.nl

ir. R. Heil MSC CISSP GICSP CISA

Partner
KPMG Advisory N.V.
Tel: +31 20 656 8033
Mob: +31 6 51 369 785
heil.ronald@kpmg.nl

Drs. J.M.A. Koedijk CISA CISM

Partner
KPMG Advisory N.V.
Tel: + 31 20 656 8251
Mob: + 31 6 22 903 688
koedijk.joost@kpmg.nl

KPMG

KPMG on social media

KPMG app

Deze rapportage is opgesteld voor het Ministerie van Volksgezondheid, Welzijn en Sport om inzicht te geven in beveiligings- en betrouwbaarheidsaspecten van Apps die zijn ontwikkeld ten behoeve van de Coronavirusapp Appathon. KPMG Advisory N.V. aanvaardt geen aansprakelijkheid voor gebruik van deze rapportage voor enig ander doel en ten opzichte van enig andere partij dan het Ministerie van Volksgezondheid, Welzijn en Sport.