5.1.2e

Ministerie van Volksgezondheid, Welzijn en Sport
Programma Realisatie Digitale Ondersteuning
5.1.2e 5.1.2e 5.1.2e 5.1.2e

Amstelveen, 11 december 2020

Betreft: Testfase GGD Contact

Geachte 5.1.2e

Er is een voornemen om op 14 december 2020 te beginnen met een praktijktest van GGD Contact. Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) verzoekt mij advies voor het beginnen van een praktijktest te gevenvanuit het oogpunt informatiebeveiliging en privacybescherming. Daarbij baseer ik mij op voor mij beschikbare documenten (via Microsoft Teams, mailberichten en losse verstrekking), eigen onderzoek en de ervaringen in het project.

Op basis van hetgeen wat mij tot het moment van schrijven is verstrekt, voorzie ik bij het beginnen met de gewenste praktijktest van "GGD Contact" **niet hoge risico's, die beheersbaar zijn.** Bedacht moet worden dat in het licht van de huidige hoeveelheid besmettingen en de hele COVID-19-crisis er tijdsdruk is. Tijdsbesparing met bron- en contactonderzoek verhoogt de ruimte voor kwaliteit (dieper graven) alsmede de capaciteit (meer gevallen kunnen behandelen).

Gelet op de context is niet beginnen schadelijker dan wel beginnen met de testen. Daarnaast maken diverse aanvullende onderzoeken deel uit van de van de testfase. Ik licht mijn advies nader toe.

Huidige situatie
Dit advies ziet op de huidige situatie, waarbij GGD West-Brabant begint met testen in een gesloten omgeving met maximaal tien medewerkers, die vanuit kantoor hun werkzaamheden verrichten. Het ministerie is als aannemer verantwoordelijk voor de bouw van de technische omgeving (de app en het portaal). Daarnaast rust er een politieke verantwoordelijkheid op deze toepassing. Bij test voert het ministerie het beheer uit (juridisch de verwerker), terwijl de GGD West-Brabant als verwerkingsverantwoordelijke optreedt.

Het beheer van de serversystemen wordt uitgevoerd door Intermax, die daarmee een subverwerker vormt. Middels verwerkersovereenkomsten en een opdrachtverlening krijgt deze samenwerking juridisch sluitend vorm. Er is een DPIA welke op dit moment wordt voorzien van de benodigde adviezen van de functionarissen voor de gegevensbescherming (fg's) van het ministerie en de GGD West-Brabant. Zodra die er zijn is daarmee de juridische borging aanwezig.

Over GGD Contact
GGD Contact is een van de apps die op advies van het Outbreak Management Team worden gemaakt. Deze applicaties werden reeds op 6 april 2020 door de minister aangekondigd. Het doel van deze app (GGD Contact) is om een deel van het bron- en

contactonderzoek verder te automatiseren en zowel de kwaliteit van de data te verbeteren als de werkdruk te verlagen. Een dergelijke oplossing is waardevol bij infectieziektebestrijding. Tijdens de huidige Corona-pandemie is er veel behoefte aan deze oplossing. Er wordt door de GGD-en gewerkt met scenario's waarin bron- en contactonderzoek afschalen als de werkdruk toeneemt. GGD Contact kan ervoor zorgen dat afschalen pas later noodzakelijk is. De verwachting is dat er substantiële tijdsbesparing voor de onderzoekers van het bron- en contactonderzoek is. Belangrijker nog: het systeem helpt fouten in de administratie te voorkomen en/of fors te verminderen.

Het succes van de oplossing staat of valt met het bieden van een betrouwbare- en veilige oplossing. Zowel de deelname aan het bron- en contactonderzoek als het gebruik van de app is vrijwillig. Om te zorgen dat de bereidheid tot gebruik van de app hoog is, moet de burger kunnen vertrouwen op een verantwoorde omgang met persoonsgegevens. Daarnaast heeft de minister aangeven dat informatiebeveiliging en privacybescherming goed zullen worden geborgd. Omdat het Ministerie de software voor de app en backend bouwt moet dit dan ook zwaar wegen voor een oplossing daadwerkelijk gebruikt kan worden.

Het Ministerie van VWS ontwikkelt GGD Contact. Het richt momenteel ook de serveromgeving (back-end) in om met de app te communiceren. Net als bij CoronaMelder is het uitgangspunt dat de oplossing opensourcesoftware betreft en het uitgangspunt is om waar het maar mogelijk is transparantie te geven en onderzoeken en adviezen beschikbaar te stellen. Dit moet helpen met bouwen aan het eerder genoemde vertrouwen de app te gebruiken.

Beveiliging van de app
Er zijn een aantal maatregelen genomen om te komen tot een veilige oplossing:

Op de server-omgeving:
- Bewaking. Continu monitoring van de systemen en pro-actieve bewaking.
- SOC/SIEM. Gelet op de dreiging is er continue bewaking (SOC/SIEM) geregeld, die wordt aangestuurd door een gecertificeerd CERT (Computer Emergency Response Team).
- Threat-hunting. Het proactief en iteratief zoeken in netwerken om geavanceerde bedreigingen te detecteren die bestaande beveiligingsoplossingen (proberen) te omzeilen en deze dreigingen succesvol te isoleren.Dit wordt gedaan door middel van hypothesegericht onderzoek en onderzoek op basis van bekende aanvalsindicatoren.
- Dreigingbeheer. Maatregelen voor dreigingsbeheer, zoals firewalls, inbraakdetectiesystemen (IDS), malware-sandbox en SIEM-systemen, welke doorgaans identificeren op basis van uitgevoerd onderzoek nadat er een waarschuwing is geweest voor een mogelijke bedreiging.

Rond de app:
- Versleuteling op het device van de eindgebruiker. Op het apparaat van de eindgebruiker (telefoon/tablet) zal de data die de gebruiker heeft ingevoerd versteuteld worden opgeslagen waarbij gebruik gemaakt wordt van de beste versleutelingsmogelijkheden die het apparaat biedt. Dit betekent dat andere apps

op het apparaat niet bij de gegevens kunnen komen en kunnen uitlezen wat er opgeslagen of verzonden is.

Verbinding App en Frontend (sluis):

- Tijdelijke unieke sleutels per sessie via TLS. Deze sleutelparen worden door de applicatie slechts voor de sessie gebruikt en worden nergens opgeslagen. Na het verdwijnen van de sleutels uit het geheugen van de server en client is er ook na afloop niks meer te doen met de versleutelde data ook al zou deze opgeslagen zijn.
- Veilige diffie hellman sleuteloverdracht tussen apps en backend. Hiermee worden sleutels op een correcte manier uitgewisseld waarbij en geen kennis over de uiteindelijke versleuteling wordt over de verbinding wordt gestuurd.
- End-To-End versleuteling van data in de app met pas decryptie in het portaal. Data verzonden tussen het apparaat van de gebruiker en de verwerkende server aan bij de GGD is End-to-End versleuteld zodat ook de aan het internet aangesloten ontvangende server (sluis) geen enkele informatie kan ontlenen aan de verzonden informatie.
- Tijdelijke unieke sleutels per app-sessie. Er wordt voor elke koppeling tussen de app en de backend een nieuw uniek sleutelpaar aangemaakt aan beide kanten.
- Attack surface minimization. Er wordt een minimaal aantal API's aan de buitenkant van de sluis aangeboden die vanaf het internet beschikbaar zijn. Er is dus geen mogelijkheid om vanaf het internet de "achterkant" van het systeem te benaderen.
- One time code overdracht via telefoon gesprek. Er wordt voor koppeling een eenmalige kort geldige code via de telefoon doorgegeven. Dit gebeurt pas na het normale verificatieproces waarbij de BCO medewerker weet welke persoon men aan de telefoon spreekt.
- Korte geldigheid aanmeldcodes. Door de tijd tussen het verstrekken van een aanmeldcode en het mogelijk gebruik van deze code kort te houden is misbruik vele malen moeilijker.
- Web application firewall met throttling. De inkomende verbindingen worden in de gaten gehouden, waarbij er automatisch ingegrepen wordt als er teveel (pogingen tot een) verbindingen worden opgezet door een andere computer op het internet.

Portaal:

- Transport versleuteling (TLS) op alle verbindingen. De verbinding tussen het apparaat en de ontvangende server aan bij de GGD is versleuteld volgens de hoogst gebruikelijke standaarden.
- TLS pinning in de apps. Gebruikte certificaten en/of de vertrouwde certificaat uitgever worden vastgelegd in applicatie.
- Eenrichtingsverkeer tussen de app en portaal (via de sluis). Hiermee is het zeker dat er alleen vanuit de portaal acties uitgevoerd kunnen worden.
- Een aantal queue based koppelingen (redis). Dit voorkomt een overbelasting van de backend door de sluit. Tevens je nooit meer kan doen dan data in/uit een queue halen. De verwerking aan de binnenkant vindt dus onafhankelijk van het process wat zich aan de buiten afspeelt plaats. Tussen de ontvangende en de verwerkende server is er alleen de mogelijkheid om door de verwerkende server acties te initiëren. Hiermee bepaalt de verwerkende server de snelheid en de acties. Vanuit het internet is hier dus geen actieve mogelijkheid toe.
- Portaal ontsloten via diginet. Hiermee is de portaal alleen bereikbaar vanaf diginet aangesloten GGD'en en is de zekerheid van veiligheid van de oorsprong voor deze acties zeker gesteld.

- Login via identity hub met bestaande ggd account providers. Hierdoor is er geen extra beheerslaag voor gebruikerstoegang nodig waarmee er dus 'vergeten' kan worden om hieruit verlopen accounts op te ruimen.
- Two-factor op identity hub login via Google authenticator. Hiermee is het zeker dat een medewerker niet alleen een username en password weet maar ook een geactiveerd device in het bezit heeft.
- Containerized hosting voor compartimentering en minimalizatie van attack surface. Hierbij worden alle delen van de applicatie apart opgestart met slechts de minimale benodigheden die nodig zijn voor het functioneren.
- Containers opgedeeld in meerdere netwerken waarbij precies is ingeregeld welk component bij welk ander component mag. Hiermee is firewalling tussen de componenten aanwezig. En kan een component niet meer dan van te voren toegestaan.
- JWT authorisatie tussen sluis en portal. Dit zijn cryptografisch ondertekende toegangssleutels voor automatische toegang, waarbij de toegang ook weer in te trekken is indien dit nodig is.
- Rollen systeem voor portal. Gebruikers binnen het systeem hebben slechts beperkte toegang tot het deel waartoe ze toegang horen te hebben.

Dataexchange (rivm / ggd):

- Transport versleuteling (TLS) op alle verbindingen. De verbinding tussen het apparaat en de ontvangende server aan bij de GGD is versleuteld volgens de hoogst gebruikelijke standaarden.
- TLS pinning in de apps. Hierbij wordt extra aandacht geschonken aan het zekerstellen dat de server ook de juiste is door te controleren of het certificaat van de server ook van te voren bekend is.
- Digitale handtekening op uitgaande data. Uitgaande data wordt automatisch digitaal ondertekend zodat de ontvangende partij altijd kan valideren dat de data correct en geheel is overgekomen.
- RPA-technologie voor koppeling met hpzone. Hiermee wordt de datakoppeling tussen HPzone en de portaal geautomatiseerd tot op het nivo dat de koppeling nooit meer mag qua rechten dan een gebruiker zelf zou kunnen in HPzone.
- sftp koppeling met rivm via ssh keys beveiligd. Dataoverdracht op basis van public/private sleutels, waardoor geen wachtwoorden meer nodig zijn en deze dus ook niet gekraakt, gegokt of afgeluisterd kunnen worden.

Software maatregelen

- Open-sourcesoftware. Hiermee is het voor elke belanghebbende mogelijk om zelf de correcte werking van de software te (laten) controleren.
- Code reviews er zullen in een volgend stadium codereviews worden uitgevoerd op de software. De software wordt inhoudelijk beoordeeld door partijen die hierin gespecialiseerd zijn.
- Pentests. Er zijn pentests uitgevoerd en deels worden er nog pentests uitgevoerd gebaseerd op standaarden voor dergelijke onderzoeken en gestandaardiseerde rapportage. De implementatie van de oplossing wordt door gespecialiseerde partijen gecontroleerd.
- Het gebruik van standaard open-sourcesoftware voor encryptie en decryptie.
- De software voor de zelf gebruikte encryptie (libsodium) staat het gebruik van foute parameters of onveilige (oude) encryptie methoden niet toe omdat deze niet worden ondersteund.

Hosting maatregelen

- Hosting in gekwalificeerd data center. De subverwerker Intermax is ISO 9001, ISO 27001, ISO 20000, ISO 14001, NEN 7510, ISEA 3402 Type II, SOC2 gecertificeerd. Veel van de onderzoeken welke ten grondslag ligt aan de certificering is uitgevoerd door professor 5.1.2e 5.1.2e van Noordbeek. Hierdoor is er vertrouwen dat de maatregelen aan de hostingzijde in orde zijn.
- HSM voor backing alle secret keys en random input voor key generatie. De bovengenoemde sleutels aan de kant van de portaal worden beheerd onder controle een HSM installatie. Deze levert de waarborgen dat sleutelbeheer op een veilige manier plaatsvindt en de encryptiesleutels voorzien zijn van gewaarborgde randomness.
- Injected secrets aan de server kant (geen secrets in code). De sleutels voor automatische communicatie, decryptie van de databasevelden en andere zaken staan niet bij de applicatie opgeslagen, maar in een apart proces wat deze bij het opstarten aanlevert aan het serverproces.
- Firewalls. Tussen de verschillende processen, tussen de verschillende machines. Op basis van hardware en software op meerdere lagen. Het fout configureren van 1 firewall mag niet leiden tot een kritieke situatie waarbij er toegang mogelijk zou zijn tot een process waar men geen toegang tot zou mogen hebben.
- Passieve analyse mitigatie. Alle payloads even groot zodat er uit passief meegeluisterd verkeer niet af te leiden is of en wat voor type data er uitgewisseld wordt.
- Ghost responses zodat een hacker niet kan zien of een aanval met een key succes heeft. Niet van echt te onderscheiden antwoorden voor niet echte gebruikers. Indien een niet-echte gebruiker verzoekt om informatie voor een bepaalde sleutel wordt er wel antwoord teruggegeven zodat het op passief netwerk niveau niet ontdekken is of dit correcte data is.
- Actieve en passieve datasecurity. Encryptie van gevoelige velden voordat ze de database in gaan. Door de applicatie worden privacygevoelige velden en velden die tot herleidbaarheid van een persoon zouden kunnen leiden versleuteld opgeslagen.
- Sleutel rotatie op de encryptie van de gevoelige datasets. Zodat oude backups na verlopen van de key geldigheid niet meer te ontsleutelen zijn.
- At rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat als er andere processen falen (backups, schijven, toewijzingen van datablokken) er geen toegang tot de data mogelijk is. Intermax maakt hiervoor een storageomgeving, die binnen enkele weken is opgetuigd.
- Versleutelde backups. Backups worden versleuteld opgeslagen. Dit op een manier zodat de backups alleen terug te halen zijn door geautoriseerde personen en alleen op expliciete opdracht.
- Passive vulnerability scanning. Er worden geautomatiseerde scans uitgevoerd op de technische omgeving om zwakheden te detecteren als deze optreden. Dit doorlopend testen is in aanvulling op regulier penetratietesten.

Penetratietesten

Voor de daadwerkelijke livegang worden er penetratietesten uitgevoerd. Het doel hiervan is om op basis van standaarden te controleren of er sprake is van fouten op basis van standaarden. Het geeft een momentopname.

Er heeft een pentest plaatsgevonden op de apps, waaruit is gebleken dat er geen fouten zijn gevonden, die als 'hoog' dienen te worden aangemerkt.

Op de serveromgeving zal eveneens een pentest worden uitgevoerd. Omdat de doorlooptijd van een dergelijke test fors kan zijn (enkele weken) is besloten in eerste aanleg te volstaan met een scan aangevuld met aanvullende scans (passive vulnerability scanning). De ratio daarbij is dat voor het belangrijkste gedeelte de toegang tot de serveromgeving in een afgeschermde omgeving plaatsvindt.

BSPA-toetsing
Na daadwerkelijke livegang zal er een BSPA (Baseline Security Product Assessment) worden gestart om daarmee zeker te stellen dat ook de broncode en de systemen bij uitgebreid en langdurig timeboxed onderzoek blijkt te voldoen. Daarbij is het doel nadrukkelijk certificering vanuit de AIVD te bemachtigen.

Totaalbeeld

Onderdeel	**Conclusie**
Mobiele App - GGD Contact (iOS & Android)	In goede staat zonder ernstige risico's
Backend	Geschikt voor de praktijktest, geen onverantwoord risico.
Privacyrecht	Privacyrechtelijk zijn de maatregelen genomen.
Privacy	Er zijn maatregelen genomen, die invulling geven aan een privacyvriendelijke verwerking.
Overige beletselen	Er is een geschikt beheer. Er is wel sprake van doorontwikkeling en dat is een onzekere factor.

Daarom kom ik tot de slotsom dat nu beginnen met een praktijktest in mijn ogen niet onverantwoord is. Het is wel zaak actief te monitoren en blijven in te zetten om uiteindelijk terecht te komen op BIO BBN3 (VIRBI).

Hartelijke groet,

5.1.2e