Factsheet Mondelinge Vraag

Onderwerp:
Vraag van het lid Van den Berg (CDA) over het bericht 'Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien'
Bron van artikel: Nos.nl, 6 juni 2020
Naam dossierhouder: (10)(2e)
Telefoonnummer dossierhouder: 06 (10)(2e)

Samenvatting van onderwerp dat voorligt	De site Infectieradar, waar Nederlanders kunnen doorgeven of ze de afgelopen week coronaklachten hebben gehad, bevatte een datalek. De formulieren met privacygevoelige informatie waren vindbaar via een aantal handelingen in de vragenlijstapplicatie. Nadat dit gemeld was, zijn de vragenlijsten direct offline gehaald.
De context van het onderwerp	Het RIVM houdt op verschillende manieren de verspreiding van infectieziekten in de gaten. Dat geldt ook voor het nieuwe coronavirus. Een van die manieren is door te kijken naar mensen met klachten die kunnen wijzen op een infectie. Dat doen ze met Infectieradar. Een onderzoek waar iedereen in Nederland aan mee kan doen. Mensen die zich als deelnemer aan Infectieradar hebben aangemeld geven één keer per week door aan Infectieradar of zij in de afgelopen week koorts of andere klachten hadden. Hiermee kan het RIVM volgen hoe gezondheidsklachten verspreid zijn in Nederland en hoe zich dat ontwikkelt in de tijd. Die gegevens kan het RIVM gebruiken voor wetenschappelijk onderzoek naar de verspreiding van het nieuwe coronavirus. Deelnemers ontvangen eerst een registratie met vragen over hun achtergrond. Over hun werk, leeftijd, en bestaande ziekten en aandoeningen. Daarna krijgen zij elke week een e-mail met de vraag of en zo ja, welke klachten zij in de afgelopen week hadden. Het gaat dan om klachten als een loopneus, hoesten, niezen en koorts. Ook als iemand geen klachten heeft is dit belangrijk om in te vullen.
Wat vinden wij van het bericht?	• Vervelend voor de deelnemers, zij zijn hierover op zondagavond 7 juni en maandag 8 juni via een persoonlijke e-mail geïnformeerd. • Vervelend ook voor het vertrouwen in de infectieradar, een mooi instrument om verspreiding van infectie te volgen. • En vervelend voor het algemene vertrouwen in hoe de overheid met gegevens omgaat. • U mag er als burger op rekenen dat wij met uw gegevens zorgvuldig omgaan. Dit is onvoldoende gebeurd en dat betreurt het RIVM. Hiervoor bieden zijn hun oprechte excuses aan. • Gelukkig is er na de melding snel gehandeld.
Kernboodschap	• Het datalek betrof aanmeldformulieren van 49 personen. De formulieren van de andere 55.000 deelnemers zijn niet ingezien. • De informatie van 49 personen is alleen ingezien door 2 personen die het systeem hebben getest en dit aan het RIVM hebben teruggekoppeld. Zij hebben de gegevens vernietigd. • Naast de door de NOS verkregen toegang is er geen sprake geweest van een datalek. • U mag er als burger op rekenen dat wij met uw gegevens zorgvuldig omgaan. Dit is onvoldoende gebeurd en dat betreurt het RIVM. Hiervoor bieden zij hun oprechte excuses aan.
Handelingsperspectief	• De deelnemers van Infectieradar waarvan de informatie zichtbaar is geweest

(wat kunnen we als VWS doen of toezeggen)	zijn hierover op zondagavond 7 juni via een persoonlijke e-mail geïnformeerd. • De overige deelnemers zijn op maandagochtend 8 juni geïnformeerd. Daarna plaatst het RIVM een bericht op de website met een update. • Ook heeft het RIVM melding gedaan bij de Autoriteit Persoonsgegevens. • De leverancier van de software, Formdesk, heeft een oplossing doorgevoerd die nu door het RIVM en een externe partij getest wordt. • Pas als zeker is dat de vragenlijsten veilig worden opgeslagen zullen we verder gaan met Infectieradar en de andere vragenlijsten van Formdesk.
Politieke afspraken (regeerakkoord, convenant, coalitieafspraken e.d.)	N.v.t.
Feiten&cijfers	Infectieradar is sinds 26 maart actief met 50.000 deelnemers. We streven naar in ieder geval 100.000 deelnemers. Op dit moment kunnen er maximaal 150.000 mensen mee doen. Als er meer mensen mee willen doen, dan wordt dit uitgebreid.
Overig (zoals heikele punten en pers)	• Vraag gesteld n.a.v. het bericht: 'Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien'. • Mogelijk wordt de verbinding gelegd tussen het datalek infectieradar en corona apps (zie Q&A).

Spreektekst:

- De site Infectieradar, waar Nederlanders kunnen doorgeven of ze de afgelopen week coronaklachten hebben gehad, bevatte een datalek.
- Privacygevoelige informatie was vindbaar door een aantal handelingen in de vragenlijstapplicatie van Formdesk. Nadat dit gemeld was, zijn de vragenlijsten direct offline gehaald.
- Het datalek betrof aanmeldformulieren van 49 personen. De formulieren van de andere 55.000 deelnemers zijn niet ingezien.
- De informatie van 49 personen is alleen ingezien door 2 personen die het systeem hebben getest en dit aan het RIVM hebben teruggekoppeld. Zij hebben de gegevens vernietigd.
- De deelnemers van Infectieradar waarvan de informatie zichtbaar is geweest zijn hierover op zondagavond 7 juni via een persoonlijke e-mail geïnformeerd.
- De overige deelnemers zijn op maandagochtend 8 juni geïnformeerd. Daarna plaatst het RIVM een bericht op de website met een update.
- Ook heeft het RIVM melding gedaan bij de Autoriteit Persoonsgegevens.
- Pas als zeker is dat de vragenlijsten veilig worden opgeslagen zullen we verder gaan met Infectieradar.
- U mag er als burger op rekenen dat wij met uw gegevens zorgvuldig omgaan. Dit is onvoldoende gebeurd en dat betreurt het RIVM. Hiervoor bieden zij hun oprechte excuses aan.

Wat vinden wij van voorliggende:

- Vervelend voor de deelnemers, die allemaal persoonlijk zijn geïnformeerd. Vervelend ook voor het vertrouwen in de infectieradar, een mooi instrument om infectie te volgen. En vervelend voor het algemene vertrouwen in hoe de overheid met gegevens omgaat.
- Gelukkig is er na de melding snel gehandeld.

Wat is ons handelingsperspectief?

- De deelnemers van Infectieradar waarvan de informatie zichtbaar is geweest zijn hierover op zondagavond 7 juni via een persoonlijke e-mail geïnformeerd.
- De overige deelnemers zijn op maandagochtend 8 juni geïnformeerd. Daarna plaatst het RIVM een bericht op de website met een update
- Ook heeft het RIVM melding gedaan bij de Autoriteit Persoonsgegevens.
- De leverancier van de software, Formdesk, heeft een oplossing doorgevoerd die nu door het RIVM en een externe partij getest wordt.
- Pas als zeker is dat de vragenlijsten veilig worden opgeslagen zullen we verder gaan met Infectieradar en de andere vragenlijsten van Formdesk.

Q: Om wat voor datalek gaat het?

- Op 6 juni 10:41 ontving het RIVM een melding van een kwetsbaarheid op Infectieradar.nl en wel ten aanzien van Insecure Direct Object References (IDOR).
- Door hergebruik en manipulatie van een ID in het internetadres (URL) bleek het uiteindelijk mogelijk een ander formulier in te zien.

Q: Hoe kon dit gebeuren?

- Voordat Infectieradar online is gegaan zijn verschillende beveiligingsonderzoeken gedaan door een extern bedrijf en het RIVM.
- Daarin is de fout die nu naar voren is gekomen opgemerkt, maar naar nu blijkt is daar onvoldoende actie op ondernomen door Formdesk.
- Het RIVM heeft vervolgens onvoldoende gecontroleerd of deze kwetsbaarheid was verholpen.
- Formdesk zelf heeft ook de verplichting om in het kader van de informatiebeveiliging hun product regelmatig te toetsen. Dat is onder andere gedaan door het uitvoeren van PENtesten; echter daarin is nooit de nu geconstateerde kwetsbaarheid ontdekt.

Q: Is er kans op misbruik van de gegeven?

- Op verzoek van het RIVM is Formdesk een onderzoek gestart, om vast te stellen of er naast de door de NOS uitgevoerde activiteiten nog andere pogingen zijn gedaan zijn om informatie van deelnemers aan infectieradar te benaderen. De uitkomst daarvan is dat er geen andere pogingen zijn gedaan.
- De NOS onderzoeksjournalisten hebben 47 formulieren + de eigen formulieren ingezien. Zij hebben de gegevens vernietigd.
- Na bestudering van alle logfiles sinds de start van deze versie van infectieradar heeft Formdesk bevestigd dat er geen verdere inzage is geweest door anderen in de gegevens van deelnemers aan infectieradar.

Q: Welke maatregelen worden genomen n.a.v. dit datalek?

- Vanuit het RIVM is na ontvangst van de melding en interne afstemming direct de vragenlijsten offline gehaald. Aangezien Formdesk ook voor andere onderzoeken binnen het RIVM wordt gebruikt zijn ook deze ook preventief offline gehaald.
- Formdesk heeft de kwetsbaarheid in hun product onderzocht en bevestigd.
- Op verzoek van het RIVM is Formdesk een onderzoek gestart, om vast te stellen of er naast de door de NOS uitgevoerde activiteiten nog andere pogingen zijn gedaan zijn om informatie van deelnemers aan infectieradar te benaderen. De NOS onderzoeksjournalisten hebben 47 formulieren + de eigen formulieren ingezien. Na bestudering van alle logfiles sinds de start van deze versie van infectieradar heeft Formdesk bevestigd dat er geen verdere inzage is geweest door anderen in de gegevens van deelnemers aan infectieradar.
- Na de RIVM melding heeft Formdesk een patch opgeleverd die de kwetsbaarheid herstelt.
- Op verzoek van het RIVM heeft Formdesk bevestigd dat de kwetsbaarheid zich niet beperkt tot infectieradar of het RIVM maar dat alle klanten die Formdesk producten gebruiken hiermee geconfronteerd kunnen worden. Formdesk heeft 7 juni alle klanten (binnen en buiten de rijksoverheid) een bericht gestuurd met de bevestiging van de kwetsbaarheid in hun product en van de patch die zij beschikbaar hebben.
- De patch is ook geïnstalleerd op de RIVM omgevingen en daarna getest.
- Echter de RIVM Formdesk omgevingen zijn nog niet voor gebruik vrijgegeven omdat RIVM nog eerst een extra PENtest wil laten uitvoeren door externe partij. Dit zal vanaf maandag 8 juni plaatsvinden.

Q: Beperkt dit datalek van Formdesk zich tot de infectieradar?

- Op verzoek van het RIVM heeft Formdesk bevestigd dat de kwetsbaarheid zich niet beperkt tot infectieradar of het RIVM maar dat alle klanten die Formdesk producten gebruiken hiermee geconfronteerd kunnen worden.
- Formdesk heeft 7 juni alle klanten (binnen en buiten de rijksoverheid) een bericht gestuurd met de bevestiging van de kwetsbaarheid in hun product en van de patch die zij beschikbaar hebben.

Q: Is de infectieradar nog beschikbaar?

- Voor diverse lopende onderzoeken binnen het RIVM is het belangrijk dat de infectieradar z.s.m. weer volledig beschikbaar is.
- Echter, pas als zeker is dat de vragenlijsten veilig worden opgeslagen zullen we verder gaan met Infectieradar en de andere vragenlijsten van Formdesk. Dit wordt momenteel getest.
- Momenteel kunnen mensen zich wel aanmelden, maar worden de wekelijkse vragenlijsten niet verstuurd; aanmeldingen worden nog steeds veelvuldig gedaan, ook na de publiciteit van dit weekend.

Q: Hoe zijn de mensen die het betreft geïnformeerd over dit datalek?

- De deelnemers van Infectieradar waarvan de informatie zichtbaar is geweest zijn hierover op zondagavond 7 juni via een persoonlijke e-mail geïnformeerd.
- De overige deelnemers zijn op maandagochtend 8 juni geïnformeerd.
- Daarna plaatste het RIVM een bericht op de website met een update

Q: Hoe zit het met de beveiliging van de Corona-apps?

- Privacy en beveiliging zijn van begin af aan uitganspunten. Ik doe geen concessies aan de privacy en beveiligingseisen, daarom neem ik die in het ontwerp al mee.
- Bij het ontwikkelen van de apps wordt dus gebruik maakt van de uitgangspunten van privacy by design en security by design. Ik heb daarvoor een aantal van de beste experts uit het land betrokken bij de ontwikkeling van de apps.
- Daarbij doen we alles in openheid zodat alle experts mee kunnen kijken en verbeteringen aan kunnen dragen.
- Uiteraard zullen wij de apps voor in gebruikname uitgebreid laten testen.

Q: Zit er een link tussen de infectieradar en de Corona-apps?

Nee, er is geen link tussen de infectieradar en de Corona-apps.