Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Aan: DG RIVM / pSG VWS

Van: CIO RIVM

Betreft: Analyse datalek Infectieradar

Datum: 8 Juni 2020

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 030 (10)(2e)
info@rivm.nl

memo Analyse datalek infectieradar

Analyse datalek infectieradar.

Datum: 8 juni 2020

Datum
8 juni 2020

Ons kenmerk

Uw kenmerk

Behandeld door
(10)(2e)

Kopie aan

Bijlage(n)

Samenvatting

Via de vragenlijstapplicatie van Formdesk waren aanmeldformulieren van deelnemers van Infectieziekteradar op te vragen. Daarin stond privacy gevoelige informatie. Het ging om aanmeldformulieren van 49 personen. De aanmeldformulieren van de andere 55.000 deelnemers waren niet in te zien. De informatie van de 49 personen is alleen ingezien door 2 personen die het systeem hebben getest en dit aan ons hebben teruggekoppeld (inclusief hun eigen aanmeldformulieren). Zij hebben de gegevens vernietigd. De kwetsbaarheid zit bij Formdesk, onze leverancier van de vragenlijstapplicatie. Er is geen misbruik gemaakt van het datalek bij Infectieradar.

Op het moment dat het nieuws over dit datalek naar buiten kwam was de applicatie voor Infectieradar offline. Ook andere RIVM-vragenlijsten van Formdesk zijn zaterdag offline gehaald. Formdesk heeft een oplossing voor het probleem gemaakt die nu door het RIVM en een externe partij getest wordt. Pas als zeker is dat de vragenlijsten veilig worden opgeslagen gaan we verder met infectieradar. Op dat moment activeren we ook de andere vragenlijsten van Formdesk.

Formdesk heeft direct onderzocht of er misbruik is gemaakt van het datalek bij Infectieradar. Ook gaan zij onderzoeken of bij andere vragenlijsten van het RIVM misbruik is gemaakt van deze kwetsbaarheid. Het RIVM heeft melding gedaan bij de Autoriteit Persoongegevens.

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 geen actie op ondernomen door

Formdesk. Het RIVM heeft vervolgens onvoldoende gecontroleerd of deze kwetsbaarheid was verholpen.

Datum

8 Juril 2020

Ons kenmerk

Het RIVM heeft een zaterdag 6 juni een reactie gegeven voor het NOS-journaal. 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 worden maandagochtend 8 juni geïnformeerd. Daarna plaatst het RIVM een bericht op de website met een update.

De Melding

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. Vanuit het RIVM is na ontvangst van de melding intern afgestemd en direct daarna de vragenlijsten offline gehaald. Na het offline halen van de vragenlijsten is er contact gelegd met de leverancier Formdesk en een onderzoek gestart. Aangezien Formdesk ook voor andere onderzoeken binnen het RIVM wordt gebruikt zijn ook deze ook preventief offline gehaald.

Bevindingen onderzoek RIVM/Formdesk tot nu toe en genomen maatregelen

1. Formdesk heeft de kwetsbaarheid in hun product onderzocht en bevestigd.
2. 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.
3. Na de RIVM melding heeft Formdesk een patch opgeleverd die de kwetsbaarheid herstelt.
4. 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.
5. De patch is ook geïnstalleerd op de RIVM omgevingen en daarna getest en akkoord bevonden. Echter de andere 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.

Wat vooraf ging

Initieel (tot maart 2020) draaide Infectieradar op een ander platform. Vanwege o.a. beveiligingsproblemen is deze versie alleen voor enkele uren beschikbaar geweest. Op 26 maart is Infectieradar, in zijn huidige vorm, beschikbaar gesteld via Formdesk. In de besluitvorming voor deze 2e start zijn ten aanzien van Informatiebeveiliging en Privacy in overleg met VWS CPO de volgende zaken betrokken: een risicoanalyse voor informatiebeveiliging en een security PENtest voor Formdesk, uitgevoerd in 2019. Vervolgens is er in maart 2020 een Privacy Impact Analyse en een risicoacceptatie voor het gebruik van Infectieradar met Formdesk opgesteld en zijn de restrisico's geaccepteerd.

In de risicoacceptatie is de nu geconstateerde kwetsbaarheid IDOR al als risico onderkend. Daartoe is in de risicoacceptatie een mitigerende maatregel beschreven. Deze maatregel betrof een 'edit once URL', waarmee bij mogelijk gokken van de ID het formulier na verzending niet meer kan worden ingezien. Inmiddels is duidelijk waarom dat deze maatregel die in het risicoacceptatie document stond niet volledig is opgevolgd door Formdesk. Er heeft dus bij het RIVM onvoldoende controle plaats gevonden op het daadwerkelijk implementeren van de benoemde maatregel.

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.

En nu? Verdere vervolgsacties

Melden data lek bij AP:
RIVM zal bij de AP melding doen vanwege het lekken van de informatie van 47 deelnemers van infectieradar. Hiertoe wordt in samenspraak met Formdesk een meldformulier ingevuld en aan de AP gezonden. Daarbij hoort ook het informeren van de 47 deelnemers over het feit dat de NOS inzage heeft gehad in hun formulier. Deze melding zal maandag verzonden worden binnen de vereiste 72 uur.

Uitvoeren extra PENtest:
Deze test zal op alle RIVM Formdesk omgevingen worden uitgevoerd. Op basis van de resultaten zullen de omgevingen weer in gebruik genomen worden. Het besluit over volledige ingebruikname infectieradar zal apart door DG RIVM na overleg met het departement genomen moeten worden. 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. Vanuit het CIb is het van groot inhoudelijk belang dat zowel infectieradar z.s.m. weer

volledig beschikbaar is, voor de benodigde epidemiologische duiding. Ook andere onderzoeken (i.i.g. Pienter corona) hebben z.s.m. toegang nodig tot de omgeving. Voor Pienter corona is deze week een verzending van pakketjes aan 7000 deelnemers gepland en aangekondigd.

Communicatie:
Er is gecommuniceerd met de journalist en onderzoeker (betrokkenen bij het datalek). Er wordt met een specifiek bericht gecommuniceerd met de deelnemers van wie de gegevens zijn ingezien door journalist en onderzoeker. Er wordt met een generiek bericht gecommuniceerd met de overige deelnemers.

Interne communicatie betreffende het tijdelijk niet beschikbaar zijn van de Formdesk omgevingen naar alle leidinggevenden. Bij voorkeur z.s.m.

Conclusie:

We zijn geconfronteerd met een beveiligingslek in een product van een externe leverancier. Dit lek raakt naast het RIVM vele andere organisaties. Naast de door de NOS verkregen toegang is er geen sprake geweest van een datalek. Er is bij het RIVM onvoldoende controle geweest op de opvolging van de bevindingen in de risicoanalyse. Er is een patch voor het probleem, deze zal nog extra getoetst worden. Schade zit vooral in de reputatie/imago RIVM/VWS/ICT voorzieningen ter ondersteuning van COVID-19 onderzoek. Het RIVM voert extra PEN testen in om de geconstateerde risico's in de toekomst nog beter te voorkomen.