Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3563

Vragen van het lid **Veldman** (VVD) aan de Minister van Volksgezondheid, Welzijn en Sport over *het bericht «Minister legt lek infectieradar bij ontwikkelaar, bedrijf reageert verbaasd»* (ingezonden 15 juni 2020).

Antwoord van Minister **De Jonge** (Volksgezondheid, Welzijn en Sport) (ontvangen 17 juli 2020).

Vraag 1
Bent u bekend met het bericht «Minister legt lek infectieradar bij ontwikkelaar, bedrijf reageert verbaasd»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u aangeven welke veiligheidsrisico's nog meer aan het licht zijn gekomen tijdens de veiligheidscheck bij het ontwikkelen van de site?

Antwoord 2
Het RIVM heeft – conform de standaard aanpak bij het RIVM voor informatiebeveiliging en risicomanagement – een quickscan uitgevoerd voor het bepalen van de maatregelen vanuit de Baseline Informatiebeveiliging Overheid / BIO (voorheen Baseline Informatiebeveiliging Rijk / BIR).
Formdesk betreft een zogenaamde SAAS-oplossing (Software As A Service). Hierbij draait de omgeving bij de leverancier en zorgt de leverancier voor het beheer van de omgeving en de ontwikkeling van de software. Het RIVM gebruikt Formdesk voor het online ontwerpen van formulieren, bijvoorbeeld aanvraagformulieren, registratieformulieren, bestelformulieren en enquêteformulieren.
Zoals gebruikelijk bij het gebruik van een SAAS-oplossing heeft het RIVM een risicoanalyse gemaakt en een pentest uitgevoerd. Voor het gebruik van de Formdesk-oplossing voor de Infectieradar is daarnaast ook een Privacy Impact Assessment (PIA) uitgevoerd.

[1] Nu.nl, «Minister legt lek infectieradar bij ontwikkelaar, bedrijf reageert verbaasd», 9 juni 2020, via: https://www.nu.nl/tech/6056789/minister-legt-lek-infectieradar-bij-ontwikkelaar-bedrijf-reageert-verbaasd.html

ah-tk-20192020-3563
ISSN 0921 - 7398
's-Gravenhage 2020

Bij deze analyses zijn – naast het risico op het ontstaan van een datalek – meerdere veiligheidsrisico's onderkend, namelijk risico's op:
– Onbevoegd aanpassen van de enquêteformulieren;
– Het maken van invoerfouten door formulierbeheerders;
– Onbevoegd inzien van ingevulde enquêtes vanuit de Formdesk omgeving;
– Onbevoegd inzien van ingevulde enquêtes tijdens transport van de Formdesk omgeving naar RIVM;
– Onbevoegd inzien van ingevulde enquêtes binnen het RIVM (scheiding e-mailadressen en symptomen);
– Manipulatie van de URL in relatie tot het ontwerpen van het enquêteformulier;
– Niet tijdig uitvoeren van beveiligingsupdates (patchmanagement).

Op alle genoemde risico's zijn door het RIVM (organisatorische of technische) maatregelen genomen.

Vraag 3
Hoe beoordeelt u de uitspraken van Formdesk dat de kwetsbaarheid niet eerder aan het licht is gekomen en ook niet aan Formdesk teruggekoppeld is?

Antwoord 3
Het RIVM heeft voor ingebruikname van de Infectieradar (op 25 maart) contact gehad met de leverancier van Formdesk over het oplossen van het risico op mogelijk misbruik van de URL-gegevens dat bij de risico-analyse van het RIVM geconstateerd was. De leverancier heeft vervolgens aangegeven hoe RIVM dit risico kon vermijden. RIVM heeft de maatregelen genomen die Formdesk heeft geadviseerd.
De feitelijke rolverdeling tussen RIVM en Formdesk wijkt af van hetgeen ik op 9 juni jl. heb gemeld. Toen heb ik, op basis van informatie van het RIVM, gemeld dat Formdesk de maatregel moest doorvoeren. Bij nader onderzoek is gebleken dat, zoals hierboven beschreven, het RIVM de maatregel heeft doorgevoerd die Formdesk heeft geadviseerd.
Op 6 juni bleek dat het risico op manipulatie van URL zich op een andere plek in de Formdesk software had voorgedaan. Dit was niet in de eerste risico-analyse naar voren gekomen, en de door Formdesk voorgestelde maatregelen die het RIVM heeft doorgevoerd, waren daarmee geen oplossing voor dit probleem. Achteraf gezien concludeert het RIVM dat dit probleem op 25 maart opgemerkt had kunnen worden indien ná implementatie van de door de leverancier van Formdesk geadviseerde maatregel en vóór het online plaatsen van Infectieradar een extra test op dit risico was uitgevoerd.

Vraag 4
Kunt u uw uitspraak uit het artikel, dat Formdesk op de hoogte was van het lek, onderbouwen?

Antwoord 4
Ik heb aangegeven dat de leverancier van Formdesk op de hoogte was van het risico dat uit de risico-analyse van het RIVM naar voren is gekomen. Dit risico is door het RIVM en de leverancier van Formdesk besproken naar aanleiding van de uitgevoerde risico-analyse. De leverancier van Formdesk heeft RIVM aangegeven hoe dit risico vermeden kon worden. RIVM heeft de maatregelen genomen die Formdesk heeft geadviseerd. Achteraf is gebleken is dat elders in de software een kwetsbaarheid aanwezig was, en dat daardoor een daadwerkelijk lek is ontstaan.

Vraag 5
Kunt u aangeven of er na de melding van het lek door de NOS contact is geweest met Formdesk? Zo ja, welke vervolgacties zijn er op basis van dit contact ondernomen?

Antwoord 5
RIVM heeft op 6 juni, na de melding van de NOS, onmiddellijk contact gezocht met de leverancier van Formdesk. Vervolgacties waren onder meer het offline halen van Infectieradar en andere toepassingen van Formdesk voor het RIVM. Vervolgens zijn RIVM en de leverancier een onderzoek gestart naar het datalek. De leverancier van Formdesk heeft op dezelfde dag middels een patch het datalek gedicht.

Vraag 6
Kunt u toelichten van hoeveel deelnemers van de infectieradar het aanmeldformulier door andere mensen bekeken is dan henzelf? Kunt u aangeven welke vervolgacties er ondernomen worden voor die deelnemers?

Antwoord 6
De leverancier heeft het RIVM bevestigd dat niemand anders dan de journalist en de aan hen meldende beveiligingsexpert gegevens hebben geopend. Het ging om 49 aanmeldformulieren. Verder zijn de gegevens van de deelnemers van Infectieradar niet door anderen ingezien. Het RIVM heeft een melding gedaan bij de Autoriteit Persoonsgegevens van het datalek. Ook heeft het RIVM de deelnemers waarvan de gegevens zijn ingezien en alle overige deelnemers inmiddels geïnformeerd. De journalist die het lek meldde, heeft het RIVM laten weten dat de geopende formulieren niet zijn ingezien en zijn vernietigd. Zie ook: https://www.rivm.nl/nieuws/geen-misbruik-datalek-infectieradar.

Vraag 7
Heeft het datalek in de infectieradar ook effect op alle Nederlanders boven de 18 jaar die hun keuze met het oog op het registreren in het nieuwe donorregister nog moeten maken? Met andere woorden: heeft dit datalek een negatief effect op de bereidheid van de mensen om zich te registreren?

Antwoord 7
Voor de goede orde, dit incident staat los van het Donorregister en de nieuwe donorwet. En dit datalek is onvergelijkbaar met het datalek dat zich bij het Donorregister heeft voorgedaan. Dat gezegd hebbende, is het natuurlijk voorstelbaar dat mensen door dit (nieuwe) incident minder vertrouwen krijgen in de overheid als beheerder van hun gegevens. Ik heb tot op heden echter geen signalen dat dit van significante betekenis is voor mensen om al dan niet hun keuze in te vullen in het Donorregister. Het aantal burgers dat een keuze heeft ingevuld in het Donorregister neemt nog steeds toe.

Vraag 8
Kunt u aangeven hoe u het beschaamde vertrouwen van gebruikers gaat herstellen?

Antwoord 8
Het datalek in de infectieradar is bovenal zeer vervelend voor de deelnemers waarvan de gegevens door de NOS zijn ingezien. Zij zijn via een persoonlijke e-mail hierover geïnformeerd. Daarnaast is het ook vervelend voor het publieke vertrouwen in de infectieradar, wat een nuttig instrument is om verspreiding van infectie te volgen. Burgers mogen erop rekenen dat de overheid zorgvuldig met hun gegevens omgaat. Dit is onvoldoende gebeurd en dat betreurt het RIVM. Om een dergelijke situatie in de toekomst te voorkomen worden de RIVM Formdesk omgevingen pas vrijgegeven als er een extra pentest is uitgevoerd door een externe partij.

Vraag 9
Welk verband ligt er tussen de infectieradar en de grotegriepmeting.nl? Is er contact geweest met de initiatiefnemers van de grotegriepmeting.nl en zo nee, waarom niet?

Antwoord 9
De Grote Griepmeting (GGM) is een onderzoek dat heeft gelopen van 2003 tot 2017. Vanaf de start in 2003 is er nauwe samenwerking geweest tussen GGM en het RIVM. De GGM heeft later deelgenomen aan het Europees samenwerkingsverband Influenzanet (georganiseerd door de ISI-foundation in Italië). Dit samenwerkingsverband heeft EU-gelden ontvangen voor de ontwikkeling van open-source software. De GGM werd daar destijds ook uit betaald voor haar bijdrage aan deze ontwikkelingen. De gegevens van de GGM zijn door het RIVM gebruikt voor de influenza surveillance en er zijn vele wetenschappelijke artikelen gepubliceerd met auteurs van de GGM en het RIVM. Helaas moest de GGM stoppen in 2017 vanwege gebrek aan middelen.
Door de uitbraak van COVID-19 ontstond bij het RIVM de noodzaak om weer informatie te krijgen over mogelijk aan COVID-19 gerelateerde klachten in de

bevolking. Daarom werd de Infectieradar opgezet. Tijdens de voorbereiding daarvan heeft het RIVM contact gezocht met de initiatiefnemers van GGM. Helaas bleek een vruchtbare samenwerking niet mogelijk zonder grote investeringen. Het RIVM heeft toen besloten zonder deze samenwerking verder te gaan.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Buitenweg (GroenLinks), ingezonden 11 juni 2020 (vraagnummer 2020Z10734).