AH 2176
2021Z04470

Antwoord van minister De Jonge (Volksgezondheid, Welzijn en Sport)
(ontvangen 29 maart 2021)

1. Herinnert u zich uw brief waarin schrijft dat de kwetsbaarheden in IT-systemen voor testen en traceren die blijken uit de risicoanalyse niet openbaar worden gemaakt? 1) Deze kwetsbaarheden zijn inmiddels toch opgelost en vormen daardoor toch geen bedreiging meer?

Er zijn mitigerende maatregelen genomen waarmee eerder geconstateerde kwetsbaarheden tot het minimum zijn gereduceerd. Om alle kwetsbaarheden op te lossen zullen enkele applicaties – waaronder HP Zone – moeten worden vervangen. Hierover worden nu concrete afspraken gemaakt en acties in gang gezet tussen GGD, RIVM en VWS. Daarnaast vindt er actieve monitoring plaats op de IT systemen. Indien afwijkingen zich voordoen wordt hier 7 dagen per week direct actie op ondernomen.

2. Bent u bereid de risico-analyses alsnog openbaar te maken zodat de Kamer op basis van zo volledig en transparant mogelijke informatie haar taak kan uitvoeren?

In mijn brief aan uw Kamer van 12 februari ben ik op dit verzoek ingegaan. Zowel de NCSC als het Red team heeft mij geadviseerd openbaarmaking op dit moment teveel risico's kent. Zoals eerder toegezegd zal ik bij het opleveren van de audit heroverwegen of het mogelijk is deze analyse of delen van deze analyse openbaar te maken. Mijn inzet is om zo transparant mogelijk te zijn.

3. Maakt het oefenen met cyberscenario's deel uit van het aanpakken van de kwetsbaarheden en wordt dit structureel ingezet? Zo nee, waarom niet?

Ja, er worden structureel cyberaanvallen testen ingezet. De resultaten daarvan worden gebruikt om kwetsbaarheden proactief te traceren en op te lossen.

4.
Wordt inmiddels wel 'volcontinu' en 'volautomatisch' gecontroleerd op misbruik van de GGD-systemen?

Ja, er wordt continu en grotendeels automatisch gemonitord op misbruik van de GGD systemen. Indien er afwijkingen worden geconstateerd, vindt hier direct een afgewogen actie op plaats.

5. Wordt een scheiding gemaakt tussen persoonsgegevens en de andere gegevens of wordt dit nog steeds gecombineerd opgeslagen?

De gegevens worden gecombineerd opgeslagen, echter de functionaliteiten zijn dermate sterk gereduceerd dat de kans op frauduleuze handelingen zo veel mogelijk is verkleind.

6. Ligt er bij alle GGD's een draaiboek klaar in het geval van een volgend datalek om onmiddellijk actie te ondernemen en het lek direct te dichten?

Het recent ingerichte en nu volledig operationele SOC (Security Operations Center) van GGD GHOR Nederland staat in nauw contact met alle GGD'en en onderneemt direct actie als er incidenten optreden. De te nemen maatregelen zijn afhankelijk van het incident.

7. Hoe wordt beter gecommuniceerd dat burgers hun gegevens kunnen laten verwijderen uit de GGD ITsystemen? Er is teveel verwarring over de consequenties van de verwijdering ten aanzien van vaccinatie; kunt u ervoor zorgen dat verwijdering van testgegevens niet van invloed is op vaccinatie?

Als eerdere gegevens gewist zijn, kan er nog steeds een afspraak worden gemaakt om gevaccineerd te worden. Op de website van GGD GHOR Nederland is informatie beschikbaar over het verwijderen van persoonsgegevens bij de GGD'en: https://ggdghor.nl/actueel-bericht/informatie-over-verwijderen-persoonsgegevens-bij-de-ggden/ . Ook op de websites van de regionale GGD'en is informatie beschikbaar. Bij vragen kan contact opgenomen worden met het landelijk informatienummer: 085-1308226 dat op werkdagen bereikbaar is van 9.00 – 17.00 uur.

8. Kunt u deze vragen voor 17 maart 2021 beantwoorden?

We streven ernaar om de antwoorden sneller dan de reguliere procedure af te wikkelen maar vóór 17 maart 2021 is niet haalbaar.

1) Kamerstuk 27 529 nr. 258

(https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/12/kamerbrief-over-stand-van-zakenbriefdigitale-ondersteuning-pandemiebestrijding)