



# Terugkoppeling SON - VWS

Spoor 2a - Sociaal leven

29 juni 2021





## Inhoudsopgave

- Wat is er gebeurd?
- Wat waren de gevolgen?
- Welke acties hebben we genomen?
- Wat is de huidige status van de situatie?
- Hoe voorkomen we dat dit opnieuw gebeurt?



# Terugkoppeling



## In het weekend van 25 en 26 juni is de IT van SON op meerdere manieren onder vuur genomen

### Aanval op IT omgeving SON

- Op vrijdag 25 juni 2021 is er een (vergelijkbaar met een DDOS) aanval geweest op de IT omgeving van SON via het aanmeldportaal voor evenementorganisatoren. Het aanmeldportaal en de teststraatapplicatie maken ondanks het feit dat deze uiteraard gescheiden zijn ingericht, wel gebruik van een aantal gedeelde componenten, waaronder de mailfunctionaliteit. Doordat deze laatste overbelast werd door een grote hoeveelheid aan spammails die verstuurd werden, ontstonden er problemen met de beschikbaarheid van de teststraatapplicatie.

### Meldingen van inbreuk op gegevens SON

- Op vrijdag 25 juni 2021 werd SON benaderd door 2 personen (naam, nummer en email adres bekend) die meldden dat ze boekingsbevestigingen van anderen via het afsprakenportaal zouden kunnen inzien. Hier is onderzoek op gedaan en nadere informatie over opgevraagd, de voorlopige inschatting is dat dit zeer onwaarschijnlijk is. Desalniettemin zijn er vrijdagavond direct aanvullende maatregelen genomen om aanvullend te beveiligen. Er is communicatie met deze personen. Bewijs van een inbreuk hebben de personen niet aangeleverd en het is onduidelijk of ze dit kunnen.
- Op zaterdag 26 juni 2021 was er een melding van een derde incident. Burgers hebben gemeld bij de helpdesk van VWS dat zij gebeld werden door een Amerikaans callcenter op het moment van inlezen van het testresultaat in de CoronaCheck app. Het zou hier gaan om 5 meldingen. Nadere details over deze meldingen ontbreekt. Wat hier de achterliggende reden was en of hier daadwerkelijk sprake was van legitieme meldingen wordt nog onderzocht. Forensische specialisten zijn hier op ingezet. Tot nu toe geen enkele aanwijzing dat hier sprake is van een daadwerkelijk incident.



## Wachtrijen, vertraging van resultaten en creatieve organisatoren en bezoekers waren het gevolg.

### Gevolgen voor bezoekers

- De combinatie van IT problemen en de eerste keer dat er in teststraten veel bezoek was (totaal 227.000 testen), resulteerde in wachtrijen bij de teststraten. Vooral in de regio Amsterdam. In sommige gevallen bleek een teststraat onvoldoende bemenst te zijn.
- Doordat de teststraatapplicatie tijdelijk beperkt beschikbaar was, konden testuitslagen tijdelijk niet verwerkt worden en resultaten niet direct gedeeld worden met bezoekers. Achterstand is vooral zondag weggewerkt.
- Sommige bezoekers konden hierdoor niet naar hun evenement of activiteit. 2500 bezoekers hebben uiteindelijk geen coronatoegangsbewijs ontvangen.

### Ontstane situaties bij evenementen en activiteiten

- Er zijn signalen dat mensen zonder nieuwe test alsnog toegang (al dan niet via teststraat of de organisator van het evenement), met een alternatieve (negatieve) uitslag hebben gekregen. Dit zal zorgvuldig onderzocht en geëvalueerd worden.
- Organisatoren kwamen aan de poort met creatieve oplossingen door mensen alternatief te testen (zelftest) en van een alternatief coronatoegangsbewijs te voorzien.
- Er zijn meldingen van misbruik met de CoronaCheck app, waarbij één QR code door meerdere mensen gebruikt werd d.m.v. screenshots. Door een nalatige ID-check aan de poort kregen deze mensen toegang.

### Veel vragen bij helpdesk SON en VWS

- Er zijn veel vragen gesteld door bezoekers aan de burger helpdesk van SON en VWS.
- De afstemming tussen de twee helpdesken was niet optimaal, waardoor burgers niet (direct) een juist antwoord hebben ontvangen.



## SON heeft zoveel mogelijk actie ondernomen om impact te beperken



### Genomen acties

- Als reactie op de aanval is het aanmeldportaal direct uit voorzorg offline gehaald.
- De helpdesk van SON en VWS hebben hun aanpak op elkaar afgestemd.
- De testaanbieders zijn zo goed mogelijk geïnformeerd over de beperkte beschikbaarheid van de teststraatapplicatie en de genomen oplossingen.
- Proactieve communicatie via statements op [www.stichtingopennederland.nl](http://www.stichtingopennederland.nl).
- De logging op de andere systemen en infrastructuur binnen SON is onderzocht en er zijn geen indicaties van verlies of andere aantasting van persoonsgegevens gevonden. Medische persoonsgegevens zijn overigens conform de wettelijke eisen versleuteld opgeslagen in de database en daardoor veel lastiger toegankelijk voor aanvallers.
- Er zijn aanvullende beveiligingsmaatregelen genomen en de capaciteit van de applicatie is verder verhoogd om de grote volumes (mede door het inhaal effect) aan te kunnen.



### Effect van de acties

- Een nieuwe aanval of mogelijke risico's voortkomend uit de aanval werden en worden voorkomen. Dit betekent dat organisatoren zich tijdelijk niet kunnen aanmelden via het aanmeldportaal.
- De vragen worden beter beantwoord, zonder dat er onnodig een doorverwijzing plaatsvindt.
- Een zo goed mogelijk geïnformeerde testaanbieder en proactief bereikte media en burger.



## Op dit moment is de situatie weer stabiel en zijn de belangrijkste gevolgen geïdentificeerd.

- De ICT omgeving van SON is inmiddels weer stabiel en mensen kunnen zonder problemen bij een negatieve testuitslag een coronatoegangsbewijs ontvangen en genereren.
- Afgelopen weekend totaal 227.000 testen, met zaterdag 130.000 als piek. Uiteindelijk ontvingen ongeveer 2500 mensen uiteindelijk geen testuitslag. Dit probleem concentreerde zich vooral rond Amsterdam.
- SON doet aangifte m.b.t. de hack die vrijdag heeft plaatsgevonden op het aanmeldportaal.
- Geen enkele indicatie gevonden van verlies of aantasting persoonsgegevens.
- Evaluatie met de testaanbieders in volle gang om ze beter voor te bereiden en eventuele misstanden te bespreken
- Aanmeldportaal wordt overgezet naar andere omgeving en nader getest om herhaling te voorkomen.
  - Note: Weer beschikbaar stellen van het aanmeldportaal is nog onduidelijk waardoor een nieuwe prognose m.b.t. vraagbehoefte niet mogelijk is (schatting is dat 70% van de evenementen zich nog niet heeft aangemeld bij SON). Er wordt gewerkt aan tijdelijke vervangende aanmeldingsmogelijkheid per mail.
- De helpdesk van VWS en SON zijn beter op beter elkaar afgestemd en zullen dit deze week verder optimaliseren.
- In overleg met de departementen contact met de organisatoren over het toelaten van mensen met geldig coronatoegangsbewijs.





## De komende dagen voeren we de volgende verbeteringen door



- Er is een uitgebreide evaluatie gedaan waarvan de verschillende verbeteringen op dit moment worden doorgevoerd.
- Verschillende verbeteringen worden in de IT doorgevoerd om aanvallen nog beter weerstand te bieden en de performance te garanderen
- Deze week worden verschillende stress testen op de applicatie uitgevoerd en de capaciteit bij leveranciers is naar het maximale niveau gebracht
- Het crisisbeheersingsprotocol met daarin de verantwoordelijkheden, een helder communicatiestructuur en alternatieve scenario's wordt verder aangescherpt. .
- Verbeterpunten naar aanleiding van de evaluatie met de testaanbieders worden deze week nog doorgevoerd.
- Gesprek met de organisatoren over de toelating met geldig coronatoegangsbewijs.
- De bemensing buiten kantooruren en in de weekenden wordt structureel versterkt.