

# ANTWOORD

VAN GEDEPUTEERDE STATEN

OP VRAGEN VAN

J. Mooiman (PVV)  
(d.d. 23 augustus 2019)

Nummer  
3543

Onderwerp  
Grote zorgen veiligheid ICT systemen Provincie Zuid-Holland

Aan de leden van Provinciale Staten

*Toelichting vragensteller*

*Uit een bericht van Binnenlands Bestuur (\*) komt naar voren dat uit de op basisbeveiliging.nl staande Faalkaart blijkt dat het over het algemeen slecht is gesteld met de veiligheid van ICT van Nederlandse gemeenten en provincies.*

*Tot schrik van de PVV zijn de resultaten voor de Provincie Zuid-Holland zwaar onvoldoende. Op de Faalkaart is te zien dat onze provincie in de slechtste categorie valt. Als naar de data wordt gekeken blijkt dat op 22-8-2019 (week 34) er 224 risico's zijn waargenomen, waarvan 29 "hoog risico" en 76 "gemiddeld risico". Zuid-Holland is hiermee de derde meest kwetsbare provincie. (\*\*)*

*Het doel van de genoemde website is om de beveiliging en privacy voor o.a. provincies te verbeteren, en hoogleraar Aiko Pras (Universiteit Twente) is van mening dat de Faalkaart een goed instrument kan zijn om de overheids-ICT te verbeteren. De waarde van de Faalkaart wordt ook door het SIDN fonds onderschreven, opgericht door de Stichting Internet Domeinregistratie Nederland, de autoriteit die het .nl domein beheert.*

*Hoogleraar Pras toonde onlangs ook al aan dat de cruciale digitale infrastructuur van Nederland kwetsbaar is en dat o.a. het kennisniveau van Nederlandse politici over ICT tekort schiet. (\*\*\*)*

*De PVV Zuid-Holland maakt zich grote zorgen over de staat waarin de veiligheid van de Zuid-Hollandse ICT zich bevindt met alle gevolgen van dien voor onze burgers, ondernemers en provinciale overheid en stellen daarom de volgende vragen aan Gedeputeerde Staten:*

1. *Bent u bekend met de zogenoemde Faalkaart en deelt u de mening dat de resultaten voor de Provincie Zuid-Holland zéér zorgwekkend zijn? Zo nee, waarom niet?*

Antwoord

GS hebben kennisgenomen van de Faalkaart, vinden het belangrijk dat tekortkomingen waar nodig worden gerepareerd, maar zijn niet van mening dat de

resultaten zéér zorgwekkend zijn voor de veiligheid van de IT systemen van de provincie.

De provinciale 'corporate' website

De Faalkaart heeft betrekking op provinciale websites. De primaire 'corporate' website van de provincie Zuid-Holland is [www.zuid-holland.nl](http://www.zuid-holland.nl). Via deze website wordt belangrijke informatie over de provincie verstrekt. Ook de besluiten van PS en GS zijn hierop te vinden. Deze website is een zogenaamde *transactiewebsite*. Als enige provinciale website vindt hier interactie met burgers en bedrijven plaats in de vorm van digitale contact- en aanvraagformulieren. Deze formulieren worden vanaf de website geautomatiseerd verwerkt naar de interne ICT-systemen van de provincie. Mede door deze koppeling is het risicoprofiel voor deze website hoger dan voor andere provinciale websites

De veiligheid van de corporate website wordt jaarlijks op een aantal manieren getoetst. Ten eerste laat de afdeling Informatisering en Automatisering van de provincie jaarlijks beveiligingsonderzoeken op deze website uitvoeren. Daarnaast toetst het Forum Standaardisatie jaarlijks of deze website aan verplichte beveiligingsstandaarden voor de publieke sector voldoet. Het Forum Standaardisatie is opgericht door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en onderhoudt de lijst met verplichte open standaarden voor de publieke sector en toetst de toepassing ervan. In de meest recente meting van maart 2019 is geconstateerd dat [www.zuid-holland.nl](http://www.zuid-holland.nl) aan alle verplichte internetstandaarden voldoet.

NB: In onderstaande tabel wordt ook het [www.pzh.nl](http://www.pzh.nl) vermeld. Dit is echter geen publiek toegankelijke webadres. De bezoeker die dit webadres intypt, wordt naar de veilige [zuid-holland.nl](http://zuid-holland.nl) website geleid. In de volgende paragraaf wordt uitgelegd waarom dit bij een geautomatiseerde test tot verkeerde constatering kan leiden.

*Resultaten web provincies*

| Domeinnaam   | DNSSEC | HSTS   | HTTPS Afgedwongen | TLS    | TLS NCSC |
|--|--------|--------|-------------------|--------|----------|
| <a href="http://provincie.drenthe.nl">provincie.drenthe.nl</a>           | WAAR   | WAAR   | ONWAAR            | WAAR   | WAAR     |
| <a href="http://www.bij12.nl">www.bij12.nl</a>                           | WAAR   | ONWAAR | WAAR              | WAAR   | WAAR     |
| <a href="http://www.brabant.nl">www.brabant.nl</a>                       | WAAR   | ONWAAR | WAAR              | WAAR   | ONWAAR   |
| <a href="http://www.drenthe.nl">www.drenthe.nl</a>                       | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.flevoland.nl">www.flevoland.nl</a>                   | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.fryslan.frl">www.fryslan.frl</a>                     | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.fryslan.nl">www.fryslan.nl</a>                       | WAAR   | ONWAAR | ONWAAR            | ONWAAR | ONWAAR   |
| <a href="http://www.gelderland.nl">www.gelderland.nl</a>                 | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.ipo.nl">www.ipo.nl</a>                               | ONWAAR | ONWAAR | WAAR              | WAAR   | WAAR     |
| <a href="http://www.limburg.nl">www.limburg.nl</a>                       | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.noord-holland.nl">www.noord-holland.nl</a>           | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.overijssel.nl">www.overijssel.nl</a>                 | WAAR   | WAAR   | ONWAAR            | WAAR   | WAAR     |
| <a href="http://www.provincie-utrecht.nl">www.provincie-utrecht.nl</a>   | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.provinciegroningen.nl">www.provinciegroningen.nl</a> | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.prvlimburg.nl">www.prvlimburg.nl</a>                 | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.pzh.nl">www.pzh.nl</a>                               | WAAR   | ONWAAR | ONWAAR            | ONWAAR | ONWAAR   |
| <a href="http://www.zeeland.nl">www.zeeland.nl</a>                       | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |
| <a href="http://www.zuid-holland.nl">www.zuid-holland.nl</a>             | WAAR   | WAAR   | WAAR              | WAAR   | WAAR     |

Meting informatieveiligheidsstandaarden maart 2019

Tot slot zijn alle organisaties die DigiD op hun website gebruiken – waaronder de provincie – verplicht te voldoen aan een zware beveiligingsnorm. Via een jaarlijks

ICT-beveiligingsassessment ziet Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, hierop toe. Ook in 2019 heeft Logius aan onze provincie goedkeuring verleend.

#### Overige provinciale websites

Naast de corporate website beschikt de provincie over een veelvoud van andere websites die divers van aard zijn. Hierop wordt informatie verstrekt over specifieke onderwerpen (zoals het coalitieakkoord, de begroting en archeologie) en er worden bijvoorbeeld filmpjes, foto's of kaarten getoond. Kenmerkend is dat er geen transacties plaatsvinden, er wordt geen DigiD gebruikt en er bestaat geen verbinding tussen de website en de interne ICT-systemen in de provinciale datacenters. Het risicoprofiel van dit soort websites is lager.

Om die reden zijn binnen de overheid de streefbeeldafspraken over de toepassing van de informatieveiligheidsstandaarden voor websites de afgelopen jaren juist gericht geweest op de transactiewebsites van de overheid (zoals [www.zuid-holland.nl](http://www.zuid-holland.nl)). Dit zijn afspraken die in het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) zijn vastgesteld en die jaarlijks worden getoetst door het Forum Standaardisatie.

Desalniettemin is de afspraak op dit moment dat (sinds einde 2018) alle overheidswebsites moeten voldoen aan een aantal beveiligingsstandaarden. De Faalkaart laat zien dat dit voor deze categorie provinciale websites nog niet in alle gevallen zo is.

#### Duiding

Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen. De provincie heeft hier aandacht en streeft ernaar om alle websites te laten voldoen aan het hierboven genoemde afsprakenstelsel.

Er is vanuit de Faalkaart geen contact met de provincie Zuid-Holland geweest over de wijze van testen en het beoordelen van de resultaten. Dit maakt het voor de provincie lastig om de in de Faalkaart genoemde tekortkomingen exact te duiden. Dit komt omdat er meerdere redenen kunnen zijn waarom een dergelijke geautomatiseerde test bij een website een foutmelding oplevert en daardoor plaatsing op de Faalkaart. Een eerste controle (na de publicatie van de Faalkaart) van de testresultaten door de afdeling Informatisering & Automatisering van de provincie, laat zien dat bij circa een kwart van de websites de genoemde tekortkomingen niet (meer) worden aangetroffen of dat een andere oorzaak heeft geleid tot een vermelding op de Faalkaart.

2. *Wat is en wordt door de provincie ondernomen om de ICT-omgeving zo veilig mogelijk te maken voor onze burgers, ondernemers en provinciale overheid? Graag een gemotiveerd antwoord.*

#### Antwoord

Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen.

Daarom is binnen onze provincie de ambitie 'corporate website, tenzij' geformuleerd, waarbij de corporate website altijd het eerste uitgangspunt is, tenzij het om een project gaat waar de provincie een van de vele deelnemers is en niet de trekker. Dit wordt verder uitgewerkt bij de vernieuwing van het digitaal platform Zuid-Holland, waarbij de provincie streeft naar kwaliteit op het gebied van informatieveiligheid, gebruiksvriendelijkheid, actualiteit, toegankelijkheid, leesbaarheid en vindbaarheid.

3. *Welke (aanvullende) maatregelen mogen wij van u verwachten n.a.v. de bijzonder zorgwekkende cijfers voor de Provincie Zuid-Holland? Graag een gemotiveerd antwoord.*

Antwoord

De provincie is voornemens om in 2023 aantoonbaar te voldoen aan de ISO27001 norm voor beheersing van informatieveiligheid met risicomangement als vertrekpunt. In de tweede helft van 2019 worden hiervoor de eerste plannen gemaakt en concrete stappen gezet.

4. *Wat wordt door de Provincie en eventuele partners ondernomen om het kennisniveau inzake ICT veiligheid van de provinciale overheid (politici, bestuurders, ambtenaren en gezien haar rol ook de griffie) op pijl te houden en waar mogelijk verder te vergroten?*

Antwoord

Informatieveiligheid is een onderwerp dat regelmatig op de agenda staat van het portefeuilleoverleg met de gedeputeerde. Voor de provinciale organisatie is begin 2019 een bewustwordingscampagne (Up-to-data) gestart met informatie en activiteiten rond informatieveiligheid, privacy en informatiebeheer. Vorige week onder meer een bijeenkomst met een hacker. De bewustwordingscampagne heeft een continu karakter en zal de komende jaren voortduren.

*Uit een bericht van Trouw (\*\*\*\*) blijkt dat de gemeente Den Haag eind november 2018 een wedstrijd met prijzenpot organiseerde voor ethische hackers om een dag lang de Haagse systemen te hacken.*

*De hackers vonden maar liefst 62 zwakke plekken in de Haagse systemen, waarvan 10 vielen in de categorie "hoge impact" en 1 zelfs zo ernstig was dat een systeem direct moest worden uitgezet. De wedstrijd was daarmee erg "succesvol" en goedkoper dan het inhuren van een bedrijf om hetzelfde werk te doen.*

5. *Deelt u de mening dat het regelmatig controleren van de provinciale systemen op zwakke plekken van groot belang is om de veiligheid van gevoelige informatie zo goed mogelijk op peil te houden? Zo ja, bent u bereid in navolging van de gemeente Den Haag een soortgelijke activiteit te organiseren voor ethische hackers? Zo nee, waarom niet?*

Antwoord

Ja, wij zijn van mening dat regelmatige controle belangrijk is. De in de Faalkaart genoemde websites maken echter een beperkt deel uit van de provinciale informatiesystemen en bevatten openbare informatie. Er is hier geen sprake van bedreiging van de veiligheid van gevoelige informatie.

De provincie neemt continu maatregelen om de veiligheid van de informatievoorziening te waarborgen en net als de gemeente den Haag maakt de provincie gebruik van ethische hackers. De provincie zet hen al enige jaren in op contractbasis.

Den Haag, 24 september 2019

Gedeputeerde Staten van Zuid-Holland,  
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit

### **BRON**

(\*) <https://www.binnenlandsbestuur.nl/digitaal/nieuws/faalkaart-toont-kwetsbaarheid-ict-overheden.10559222.lynkx>

(\*\*) <https://basisbeveiliging.nl/#report-zuid-holland>

(\*\*\*) <https://www.binnenlandsbestuur.nl/digitaal/nieuws/belangrijke-nederlandse-ict-infrastructuur-is.10414668.lynkx>

(\*\*\*\*) <https://www.trouw.nl/nieuws/den-haag-laat-zich-bewust-hacken-een-stuk-goedkoper-dan-een-bedrijf-inhuren~bd68f62c/?referer=https%3A%2F%2Fwww.google.nl%2F>