

FW: Gestelde vragen door audit commissie 29-08-2023 betreffende ENSIA 2022 stukken

Beste Laurette en Stefan,

Bij deze de antwoorden op de vragen die gesteld zijn door de audit commissie omtrent de ENSIA 2022 stukken. De beantwoording is langs de wethouder geweest.

Waarom is de 1^e bijlage niet gewoon openbaar? Het gaat toch gewoon om het "systeem" en niet per se over de inhoudelijke risico's?

Helaas is niet met zekerheid vaststellen wat er met de 1^e bijlage wordt bedoeld. Daarom de beantwoording voor zowel de *Raadsinformatienota* als voor *Bijlage 1 DigiD*. Vraagsteller heeft gelijk dat in de bijlages dit jaar weinig inhoudelijke risico's werden besproken. Dit jaar waren er namelijk geen bevindingen en was de toon dus algemener van aard. De reden dat de *Raadsinformatiebrief* toch onder geheimhouding valt is dat de resultaten van ENSIA hierin worden meegedeeld. Als er dus wel bevindingen zijn dan staat in de *Raadsinformatienota* aan welke normen niet wordt voldaan, waarom en hoe dat wordt opgelost. Deze informatie is vertrouwelijk, het stuk valt daarom ieder jaar onder de geheimhouding, ongeacht of de resultaten goed of minder goed zijn.

Voor *Bijlage 1 DigiD* geldt dat de inhoud nog specifieker is, daarin is namelijk ook terug te zien welke applicatie/aansluiting de kwetsbaarheid betreft. Gezien openbare stukken via het internet terug te vinden zijn is het mogelijk dat een kwaadwillende kan zien welke kwetsbaarheid er waar is vastgesteld. Van deze informatie kan misbruik gemaakt worden. Het openbaar toegankelijk maken van deze informatie brengt een beveiligingsrisico met zich mee. Daarom wordt geheimhouding opgelegd op basis van uitzonderingsgrond 2:

"Het openbaar maken van informatie blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:

- a. de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;*
- b. de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;"*

Los daarvan is het advies vanuit de ENSIA om geheimhouding te betrachten voor de *Raadsinformatienota* en de *Bijlage 1 DigiD* en *Bijlage 2 Suwinet*. Daarin gaan wij als gemeente mee.

Wel kunnen we volgend jaar het dreigingsbeeld en de algemene stand van zaken los trekken van de *Raadsinformatienota*. Door dit deel apart aan te leveren naast de *Raadsinformatienota* is er in ieder geval een deel van de stukken openbaar beschikbaar. Daarmee kunnen we enigzins tegemoet komen aan de wens om zoveel mogelijk informatie omtrent ENSIA openbaar te houden.

Waarom wordt er in ENSIA stukken niets genoemd over buitenlandse software en hardware?

ENSIA heeft een hele specifieke scope, de software die met ENSIA wordt geaudit wordt geleverd door binnenlandse partijen. Er is dus geen buitenlandse software in scope van de ENSIA, het onderwerp wordt om die reden dan ook niet specifiek genoemd. Uiteraard is er buiten ENSIA om zeker aandacht voor de herkomst en locatie van onze software leveranciers en hun toeleveranciers. Er wordt scherp

opgelet dat deze zich bevinden binnen de zone van de Europese Unie. Dit conform landelijke en Europese regelgeving.

Mocht ik nog iets kunnen betekenen dan hoor ik het natuurlijk graag!

Met vriendelijke groet,

Andrea van der Ham
Adviseur Informatiebeveiliging



Gemeente Dordrecht

Spuiboulevard 300
3311 GR DORDRECHT

+ Postbus 8, 3300 AA DORDRECHT
(14078

* aa.van.der.ham@dordrecht.nl

☎ 06-38681835

Afwezig op woensdag

P Neem alstublieft het milieu in acht voordat u besluit deze mail te printen.