Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Via Overheid.nl verzonden
ENSIA auditcommittee (ensia@vng.nl)
Datum : 17 mei 2023
Betreft : Consultatie Regeling dienstverleners informatieveiligheidsaudits Wdo

Geachte Minister,

Dank voor de geboden gelegenheid om te reageren op het voorstel voor een Ministeriële Regeling dienstverleners informatieveiligheidsaudits Wdo (hierna: Regeling).
Deze reactie versturen wij als audit committee van ENSIA. ENSIA is een initiatief van gemeenten en de ministeries van BZK en SZW. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. ENSIA wordt door gemeenten, provincies, waterschappen en enkele onderdelen binnen de rijksoverheid gebruikt om zich te verantwoorden over de staat van informatiebeveiliging op basis van de BIO (Baseline Informatiebeveiliging Overheid) en het gebruik van de Geo-basisregistraties. ENSIA structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid.

Diverse leden van het audit committee van ENSIA zijn lid van NOREA en hebben aan de reactie van NOREA op de Regeling meegewerkt. Wij onderschrijven de reactie van NOREA. Wij hebben de volgende aanvulling.

Aandacht voor relatie kosten, risico's en continue feitelijke veiligheid.
Op dit moment worden jaarlijks ongeveer 2000 DigiD-audits uitgevoerd voor aansluithouders (kosten per audit tussen de 5.000 en 15.000 euro) om aan te tonen dat aansluithouders voldoen aan de eisen en de aansluiting mogen blijven gebruiken op hun website. Dit nog afgezien van de subcontractors, die in meer of mindere mate ook moeten voldoen aan de eisen en de interne uren die gemaakt worden in de voorbereiding en de uitvoering van de DigiD-audit. Het verdient aanbeveling om opnieuw de vraag te stellen of de kosten zich verhouden tot de risico's en of misschien op een andere manier (meer) zekerheid verkregen kan worden. Er dient een beter inzicht te komen in de risicobeheersing door DigiD-audits en de overige beveiligingsmaatregelen, o.m. als gevolg van NIS2. Dit als onderdeel van een integrale risico- en impactafweging van de stelselhouder BZK waarbij onder andere aandacht wordt gegeven aan de specifieke belangen van gemeenten met hun brede dienstverlening. Deze integrale risico- en impactafweging van de stelselhouder BZK missen wij op dit moment.

In dit verband merken wij op dat de oorspronkelijke DigiD-audit bedacht is op een moment dat er maar 1 baseline was (BIR2011) en de overheid als geheel nog grote stappen te zetten had op het gebied informatieveiligheid. Op dat moment was de DigiD-audit een goede prikkel en heeft het bijvoorbeeld in het eerste jaar van de DigiD-audit ervoor gezorgd dat alle "cowboy" hosting providers zijn uitgefilterd, wat direct bijgedragen heeft aan een veiliger en integer DigiD-stelsel. De DigiD-audit is in de afgelopen 11 jaar eigenlijk nog steeds dezelfde audit, terwijl er grote veranderingen zijn geweest (BIO en ENSIA) en nog steeds plaatsvinden (NIB2/CSA/Basisbeveiliging.nl). Dit ook op het gebied van methoden en technieken.

De DigiD-audit richt zich met name op veiligheid op 1 moment. Internetscans door potentiële aanvallers worden voortdurend uitgevoerd. Wij adviseren om een verkenning uit te voeren naar de nieuwe inzichten inzake de beheersing van cyberdreigingen. Een voorbeeld is het gebruik van een sensor of een agent op de webserver die voortdurend de status van belangrijke eigenschappen monitort en rapporteert aan centrale omgeving bij een onafhankelijke partij. (Dat zou Logius kunnen zijn als hoeder van een integer

toegangsstelsel.) Met een dergelijke aanpak zou het toegangsstelsel permanent beveiligd zijn en is er permanent inzicht in de status van iedere webserver waarop een toegangsvoorziening gerealiseerd is. Op deze manier wordt tegelijk het patchmanagement live gecontroleerd en kan direct ingesprongen worden op kwetsbaarheidsmeldingen van bijvoorbeeld het NCSC. Een dergelijke sensor kost een fractie van een DigiD-audit en levert het gehele jaar relevante controle- en stuurinformatie waarmee de minister het stelsel veilig kan houden en direct kan ingrijpen. Bijna de helft van de huidige maatregelen set, inclusief werking, zou kunnen worden aangetoond door gebruik te maken van voornoemde continuous monitoring.

Met vriendelijke groet,

Audit committee ENSIA