DigiD beveiligingsassessment

2020

Gemeente Gooise Meren

DigiD aansluiting Digitale Belastingbalie -
Gemeente Gooise Meren
Aansluitnummer 1003677
Kenmerk BKBO/200817-3/AR

19 januari 2021
Dit assurancerapport heeft 11 pagina's
www.bkbo.nl

FEIT

Ook al zegt men dat
de wetenschap voor niets staat,
blijft het een feit
dat de zon voor niets opgaat.

Jules Deelder

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van Gemeente Gooise Meren (hierna: "opdrachtgever") hebben wij een DigiD ICT-beveiligingsassessment uitgevoerd op de webomgeving van DigiD aansluiting "Digitale Belastingbalie - Gemeente Gooise Meren " met het aansluitnummer "1003677" van Gemeente Gooise Meren zoals gespecificeerd in hoofdstuk 3 Object van onderzoek. Het onderzoek is conform de 'Handleiding uitvoering ICT-beveiligingsassessment' versie 2.2 van Logius uitgevoerd.

Wij hebben de regelgeving van de NOREA voor kwaliteitsbeheersing toegepast en onderhouden een inzichtelijk stelsel van kwaliteitsbeheersing met inbegrip van gedocumenteerde beleidslijnen en procedures met betrekking tot het naleven van ethische voorschriften, professionele richtlijnen en van toepassing zijnde, door wet- of regelgeving gestelde, vereisten.

De opdracht omvatte het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op de ICT-beveiliging van de webomgeving van aansluitnummer "1003677" en aansluitnaam "Digitale Belastingbalie - Gemeente Gooise Meren ".

De opdrachtgever maakt gebruik van serviceorganisatie Gouw IT voor de ontwikkeling, beheer en onderhoud en het hosten van de webapplicatie(s).

De opdrachtgever maakt voor haar beschrijving gebruik van de uitsluitingsmethode ('carve-out method'). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de serviceorganisatie.

1.2 Verantwoordelijkheden van de opdrachtgever

De opdrachtgever is verantwoordelijk voor de beschrijving van het object van onderzoek, het verlenen van DigiD-diensten, het onderkennen van de beveiligingsrisico's van de DigiD webomgeving en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de "Norm ICT-beveiligingsassessments DigiD" zoals opgesteld door Logius.

1.3 Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van oordelen per beveiligingsrichtlijn van de vigerende "Norm ICT-beveiligingsassessments DigiD" van Logius, over de opzet en het bestaan van de maatregelen gericht op de ICT beveiliging van de webomgeving van DigiD aansluiting met aansluitnaam "Digitale Belastingbalie - Gemeente Gooise Meren " en aansluitnummer "1003677".

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht en de NOREA richtlijn 3000/D, 'Richtlijn Assurance-opdrachten door IT-auditors'. Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en bestaan.

Een assuranceopdracht om te rapporteren over *opzet* en *bestaan* van interne beheersingsmaatregelen bij een organisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de auditor van de organisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan.

Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de *werking* van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen; wij brengen derhalve daarover geen oordelen tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor onze oordelen te bieden.

1.4 Beperkingen

Wij kunnen geen verantwoordelijkheid aanvaarden voor wijzigingen in de door ons gehanteerde feiten en omstandigheden na de datum waarop wij de desbetreffende werkzaamheden hebben afgerond, tenzij wij tijdig van de wijzigingen in de door ons gehanteerde feiten en omstandigheden op de hoogte zijn gebracht.

De "norm ICT-beveiligingsassessments DigiD" is een selectie van beveiligingsrichtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicatie" van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om een overall oordeel te verschaffen omtrent de beveiliging van de DigiD-aansluiting.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen van de betreffende DigiD-aansluiting en brengen daarover geen oordeel tot uitdrukking.

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Wij adviseren de organisatie om in aanvulling op de richtlijnen in de "Norm ICT-beveiligingsassessments DigiD", ook de andere richtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicaties" van het NCSC te adopteren. Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

In de volgende paragraaf geven wij onze oordelen ten aanzien van de 'Norm ICT-beveiligingsassessments DigiD'.

1.5 Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius wordt een oordeel gegeven over de opzet en het bestaan per 19 januari 2021 De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande tabel en een toelichting is te vinden in hoofdstuk 2.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of met redelijke mate van zekerheid wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de conclusies in deze tabel weergegeven als "voldoet" of "voldoet niet". Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 in alle materiële opzichten effectief zijn". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 niet in alle materiële opzichten effectief zijn".

De uitspraak "voldoet" of "voldoet niet" beperkt zich tot de eigen oordeelsvorming van de auditor. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de houderorganisatie en waarvan de auditor van de serviceorganisatie Gouw IT heeft aangegeven dat, om te voldoen aan deze beveiligingsrichtlijnen, interne beheersingsmaatregelen door de gebruikersorganisaties dienen worden geïmplementeerd. In Bijlage C is ten dienste van de assessmentbeoordeling door Logius een totaaloverzicht opgenomen van de door ons

onderzochte normen en de normen die door de IT-auditor van de serviceorganisatie zijn onderzocht. Uitdrukkelijk merken wij op dat we geen onderzoek hebben uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van de serviceorganisatie. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen [1]

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	☑
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	☑
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	☑
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken.	☑
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	☑
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	☑
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	☑

1.6 Beoogde gebruikers en doel

De minister van BZK wil een structurele en forse impuls geven aan de kwaliteitsverhoging van ICT-beveiliging bij overheidsorganisaties die gebruik maken van DigiD. Deze organisaties moeten jaarlijks een ICT beveiligingsassessment laten verrichten onder verantwoordelijkheid van een gekwalificeerde IT-auditor (RE), teneinde de DigiD gebruikende organisaties en Logius inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting.

Onze schriftelijke rapportage is alleen bestemd voor de opdrachtgever, haar cliënten en hun auditors en Logius aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren. De rapportage, bijlagen, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande

[1] *Indien bij een beveiligingsrichtlijn wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode dan wordt dit weergegeven als "voldoet". In een voetnoot wordt de volgende zin opgenomen: "Wij hebben vastgesteld dat deze organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Wij zijn echter van oordeel dat de organisatie voldoet aan deze norm. Non occurence kan zich alleen voordoen bij de normen B.05, U/TV.01, U/WA.02 en C.08."*

schriftelijke toestemming. De bijlagen met uitzondering van bijlage C zijn alleen bestemd voor de opdrachtgever en mogen niet zonder schriftelijke toestemming van de auditorganisatie en de opdrachtgever aan derden beschikbaar worden gesteld. Bijlage C is bedoeld om Logius een totaaloverzicht te verschaffen ('volledigheid van de scope') over de resultaten van verschillende assessments, indien gebruik is gemaakt van rapporten inzake serviceorganisatie(s).

Voor zover het de opdrachtgever en Logius is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

Vlijmen d.d. 19 januari 2021

Bureau voor Kwaliteitsborging Bij de Overheid b.v.

drs. M.B.H. IJpelaar RE CEH CISA, directeur	E.W.M. Sturkenboom, auditor in opleiding

2 Criteria

De criteria waarvan gebruik is gemaakt bij het uitvoeren van deze assurance opdracht hielden in dat:

a) De interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd.

b) De risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend.

c) De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan beveiligingsrichtlijnen niet zouden verhinderen.

3 Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting "Digitale Belastingbalie - Gemeente Gooise Meren " ("DigiD webomgeving"). Dit zijn de internet-facing webpagina's, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking hebben op het proces. Met systeemkoppelingen wordt de system-to-systemkoppeling (authenticatieverzoek en uitwisselen RID en verificatieverzoek van de webdiensten) bedoeld.

De opdrachtgever biedt de volgende functionaliteit aan waarvoor DigiD aansluiting "Digitale Belastingbalie - Gemeente Gooise Meren " door burgers ter authenticatie wordt gebruikt:

De eGouw7R2 module bestaat uit een aantal vaste formulier componenten en vrije formulier componenten. Per onderkend proces bestaat de mogelijkheid om een eigen formulier/wizard structuur te ontwikkelen.

Het onderdeel GouwVoormeldingen is geïntegreerd in eGouw7R2. Deze module biedt de mogelijkheid om de burger inzicht te geven in de totstandkoming van de WOZ-waarde. Deze kernfunctionaliteit betreft het voor de aanslagoplegging de WOZ-waarde inzichtelijk maken voor de burger en de mogelijkheid te geven tot het doen van een voorstel tot wijzen van waarde-(onderdelen). Deze functionaliteit wordt geboden door de volgende webapplicatie(s):

- eSuite Digitaal Belastingloket

Deze applicatie betreft geheel standaard software en wordt onderhouden door Gouw IT. De infrastructuur waarop de applicaties draaien wordt beheerd door Gouw IT.

Het onderzoek heeft zich gericht op de webapplicaties, de URL's waarmee deze applicaties kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

De opdrachtgever heeft de DigiD webomgeving grotendeels uitbesteed aan Gouw IT in de vorm van Software As A Service. Als gevolg hiervan zijn er een groot aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen bij deze service organisatie is uitgevoerd door een gekwalificeerde IT auditor op basis van dezelfde beveiligingsrichtlijnen en met hantering van hetzelfde onderzoekprotocol als ons onderzoek. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht en opgenomen in ons rapport. Waar relevant hebben wij,

per richtlijn, specifieke verwijzingen gemaakt naar het rapport van de IT auditor van de leverancier.

In bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.