DigiD beveiligingsassessment

2016-2017

Decos Information Solutions

DigiD groepsaansluiting "Burgerberichten"
Aansluitnummer "1000401"
Kenmerk BKBO/161216/AR

27 april 2017
Dit assurancerapport heeft 10 pagina's
www.bkbo.nl

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van de Decos Information Solutions (hierna: "opdrachtgever") hebben wij een DigiD ICT-beveiligingsassessment uitgevoerd op de webomgeving van DigiD groepsaansluiting "Burgerberichten" met het aansluitnummer "1000401" van de Decos Information Solutions conform de "Handleiding uitvoering ICT-beveiligingsassessment" versie 2.1 van Logius. De opdracht omvatte het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op de ICT beveiliging van de webomgeving van DigiD groepsaansluiting "Burgerberichten".

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de *werking* van interne beheersingsmaatregelen van DigiD groepsaansluiting "Burgerberichten" en brengen daarover geen oordeel tot uitdrukking.

De opdrachtgever maakt gebruik van serviceorganisatie Microsoft Azure voor het hosten van de webapplicatie(s) waarbij de infrastructuur is opgesteld in Ierland. Decos Information Solutions maakt voor haar beschrijving geen gebruik van de uitsluitingmethode ('carve-out method'). Onze werkzaamheden strekken zich dan ook 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 per 27 april 2017 van de maatregelen gericht op de ICT beveiliging van de webomgeving van DigiD groepsaansluiting "Burgerberichten".

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht en de NOREA richtlijn 3000, '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 per 27 april 2017.

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 per 27 april 2017.

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

Interne beheersingsmaatregelen bij een organisatie kunnen vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

De "Norm ICT-beveiligingsassessments DigiD" is een door Logius beperkte selectie van beveiligingsrichtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicaties" van het Nationaal Cyber Security Centrum (= NCSC) en daarom is BKBO niet in staat om een overall oordeel te verschaffen omtrent de beveiliging van de DigiD-aansluiting.

Logius heeft de 28 beveiligingsrichtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD webapplicaties. Wij adviseren u als Opdrachtgever om in aanvulling op de richtlijnen in de "Norm ICT-beveiligingsassessments DigiD", ook de 31 andere richtlijnen van het NCSC te adopteren.

Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere bevindingen 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 27 april 2017. 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", waarbij "voldoet" geïnterpreteerd dient te worden 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" en "voldoet niet" geïnterpreteerd dient te worden 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.

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd	☑
B0-6	Maak gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen	☑
B0-7	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd	☑
B0-8	Penetratietests worden periodiek uitgevoerd	☑
B0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd	☑
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/toegangsbeheer	☑
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd	☑
B0-14	Leg afspraken met leveranciers vast in een overeenkomst	☑
B1-1	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke	☑
B1-2	Beheer- en productieverkeer zijn van elkaar gescheiden	☑
B1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld	☑
B2-1	Maak gebruik van veilige beheermechanismen	☑
B3-1	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt	☑

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft	☑
B3-3	De webapplicatie normaliseert invoerdata voor validatie	☑
B3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer	☑
B3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparameteriseerde queries	☑
B3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde	☑
B3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting)	☑
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd	☑
B3-16	Zet de cookie attributen 'HttpOnly' en 'Secure'	☑
B5-1	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn	☑
B5-2	Maak gebruik van versleutelde (HTTPS) verbindingen	☑
B5-3	Sla gevoelige gegevens versleuteld of gehashed op voor zover betrekking hebbend op DigiD [1]	☑
B5-4	Versleutel cookies	☑
B7-1	Maak gebruik van Intrusion Detection Systemen (IDS)	☑
B7-8	Voer actief controles uit op logging	☑
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld	☑

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 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, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande 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 TPM rapporten inzake serviceorganisatie(s).

Op verzoek kunnen klanten en toekomstige klanten van Decos Information Solutions de beschikking krijgen over de managementsamenvatting inclusief alle bijlagen..

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. 27 april 2017

Bureau voor Kwaliteitsborging Bij de Overheid

drs. M.B.H. IJpelaar RE CEH CISA, partner

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 per 27 april 2017.

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 groepsaansluiting "Burgerberichten" ("DigiD webomgeving").

Burgerberichten.nl is het platform waarop burgers kunnen inloggen, digitaal een aanvraag kunnen indienen, de voortgang van hun aanvraag bij hun (lokale) overheidsorganisatie kunnen volgen en bestanden kunnen downloaden (zoals een beschikking). De data wordt live opgehaald uit het lokale Decos zaaksysteem van de gemeente (waar deze aanvragen worden opgeslagen en behandeld) en niet opgeslagen op burgerberichten.nl.

Website	**Eigenaar**
www.burgerberichten.nl/gemeenteeijsdenmargraten	Decos
www.burgerberichten.nl/hollandskroon	Decos
www.burgerberichten.nl/noordwijk	Decos
www.burgerberichten.nl/HLT	Decos
www.burgerberichten.nl/schadefondsgeweldsmisdrijven	Decos
www.burgerberichten.nl/servicecentrum-mer	Decos
www.burgerberichten.nl/ozhz	Decos
www.burgerberichten.nl/omgevingsdienstijmond	Decos
Beta.burgerberichten.nl/gemeenten/verhuizen	Decos
Beta.burgerberichten.nl/gemeenten/aangifteoverlijden	Decos

Deze functionaliteit wordt geboden door de volgende webapplicatie(s):

- Decos Burgerberichten

Deze applicatie betreft geheel standaard software en wordt onderhouden door Decos Information Solutions. De infrastructuur waarop de applicatie draait wordt beheerd door Microsoft Azure Cloudservices.

Het onderzoek heeft zich gericht op de webapplicaties, de URLs 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.

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

Decos Information Solutions heeft het hosten en een deel van het systeembeheer van de infrastructuur uitbesteed aan Microsoft Azure Cloudservices. Als gevolg hiervan zijn een deel van de maatregelen belegd bij deze service-organisatie. Het onderzoeken van de maatregelen is uitgevoerd binnen ons onderzoek en opgenomen in ons rapport. Hiervoor is geen TPM verklaring beschikbaar maar is o.a. "gesteund" op een actuele en geldige ISO27001 verklaring van BSI en een ISAE3402 Type II verklaring van Deloitte over dezelfde cloud infrastructuur..