THIRD PARTY MEDEDELING 2017

LEVERANCIER:

LIAAN CONSULT B.V.

APPLICATIE:

E-DIENSTVERLENING

VERSIE 7.2

KENMERK: **1709R.AH117**
DATUM: **29 SEPTEMBER 2017**

audit, risk & compliance

INHOUDSOPGAVE

Deze rapportage bevat 8 pagina's

VERTROUWELIJK
Cliënten van Liaan Consult B.V.

3angles B.V.
Communicatieweg 9-3
3641 SGMIJDRECHT

+31(0)85 060 3855
www.3angles.nl
info@3angles.nl

1. Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van Liaan Consult B.V. hebben wij een ICT-beveiligingsassessment DigiD uitgevoerd op de webomgeving van DigiD-aansluitingen zoals gespecificeerd in hoofdstuk 3 Object van onderzoek. Het onderzoek wordt uitgevoerd conform de 'Handleiding uitvoering ICT-beveiligingsassessment' versie 2.1 van Logius.

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 DigiD-aansluitingen.

1.2 Verantwoordelijkheden van Liaan Consult B.V.

Liaan Consult B.V. 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 beheers-maatregelen om te voldoen aan de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

1.3 Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, per beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius een oordeel te geven over de opzet en het bestaan van de maatregelen gericht op de ICT-beveiliging van de webomgeving van DigiD-aansluitingen.
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 beheersmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en bestaan.

Een assurance-opdracht om te rapporteren over opzet en bestaan van interne beheersmaatregelen bij een organisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van interne beheersmaatregelen. 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 beheersmaatregelen 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 beheersmaatregelen die bij de beschrijving waren inbegrepen; wij brengen derhalve daarover geen oordeel tot uitdrukking. Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop 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 webapplicaties' 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-aansluitingen.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen van de betreffende DigiD-aansluitingen 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' van Logius.

1.5 Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals 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 28 september 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'. Daarbij dient 'voldoet' geïnterpreteerd te worden als "Wij zijn van oordeel dat de interne beheersmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 in alle materiële opzichten effectief zijn" en dient 'voldoet niet' geïnterpreteerd te worden als "Wij zijn van oordeel dat de interne beheersmaatregelen 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. 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'.

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.	Voldoet
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.	Voldoet
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Voldoet
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.	Voldoet
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Voldoet
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Voldoet
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Voldoet
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.	Voldoet

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 DigiD laten uitvoeren 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-aansluitingen.

Onze schriftelijke rapportage is uitsluitend bestemd voor Liaan Consult B.V., 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, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming.

Voor zover het Liaan Consult B.V. en Logius is toegestaan de rapportage 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.

Mijdrecht, 29 september 2017

3angles B.V.
Namens deze

drs. A.J.A. Hassing RE RA
Register EDP-auditor

2. Criteria

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. In dit onderzoek zullen wij ons derhalve op de 'Norm ICT-beveiligingsassessments DigiD' richten. De criteria waarvan gebruik gemaakt wordt bij het uitvoeren van de assurance-opdracht hielden in dat:

a) de interne beheersmaatregelen 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 beheersmaatregelen, 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-aansluitingen. Liaan Consult B.V. biedt de volgende functionaliteit aan waarvoor DigiD-aansluitingen ter authenticatie wordt gebruikt:

- Formulieren waarmee o.a. uitkeringen kunnen worden aangevraagd;
- Een formulierengenerator;
- De DigiD-koppeling zelf.

Deze functionaliteit wordt geboden door de webapplicatie e-Dienstverlening versie 7.2. De applicatie betreft standaard software en wordt onderhouden door Liaan Consult B.V. De infrastructuur waarop de webapplicatie draait wordt beheerd door Solvinity B.V.

Het onderzoek heeft zich gericht op de webapplicatie, de URL's waarmee deze applicatie kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

4. Verantwoordelijkheid gebruikersorganisatie

Bij de opzet en implementatie van interne beheersmaatregelen bij de serviceorganisatie neemt deze voor een aantal beveiligingsrichtlijnen van de 'Norm ICT-beveiligingsassessments DigiD' aan, dat enkele interne beheersmaatregelen door de houderorganisaties zullen worden geïmplementeerd om te voldoen aan deze beveiligingsrichtlijnen.

In onderstaande tabel wordt aangegeven voor welke beveiligingsrichtlijn(en) deze aanname is gedaan en welke gewenste interne beheersactiviteit bij de gebruikersorganisaties kunnen worden geïmplementeerd om te voldoen aan de desbetreffende beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

De geschiktheid van de opzet en het bestaan van deze aanvullende interne beheersmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van de 'Norm ICT-beveiligingsassessments DigiD' wordt alleen voldaan, indien aanvullende interne beheersmaatregelen van een gebruikersorganisatie samen met de interne beheersmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet en geïmplementeerd.

Nr	Beschrijving van de beveiligingsrichtlijn	Beheersactiviteit gebruikersorganisatie
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.	De gebruikersorganisatie dient zelf de afspraken met leveranciers vast te leggen in overeenkomsten.
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.	De gebruikersorganisatie dient maatregelen te treffen en in te richten met betrekking tot toegangsbeveiliging en -beheer. Hierbij valt te denken aan het gebruikers-beheer van joiners/movers/leavers, beheeraccounts, gedeelde accounts en periodieke review.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	De gebruikersorganisatie dient op basis van een risicoanalyse een gegevensclassificatie uit te voeren conform de WBP. Op basis van de classificatie dient de gebruikersorganisatie gevoelige gegevens (zoals BSN en persoonsgegevens) die in de DMZ worden opgeslagen te versleutelen; gevoelige gegevens in de backoffice blijven buiten beschouwing.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	De gebruikersorganisatie dient maatregelen te ontwerpen en in te richten met betrekking tot wijzigingsbeheer. Hierbij valt te denken aan het indienen van wijzigingsverzoeken.