THIRD PARTY MEDEDELING 2015

LEVERANCIER:

LIAAN CONSULT B.V.

APPLICATIE:

E-DIENSTVERLENING

VERSIE 6.1

KENMERK: **1603R.AH46**
DATUM: **30 MAART 2016**

INHOUDSOPGAVE

Deze rapportage bevat 8 pagina's

Cliënten van Liaan Consult B.V.

ControlSolutions International B.V.
Het Poortgebouw
Beechavenue 54-80
1119 PW SCHIPHOL-RIJK
Tel.: +31 (0)20 658 6175
Fax : +31 (0)20 658 6111
http://www.controlsolutions.nl/
info@controlsolutions.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. 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 zoals gespecificeerd in hoofdstuk 3 Object van onderzoek.

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

Hoofdstuk 4 'Verantwoordelijkheid gebruikersorganisatie' verwijst naar de behoefte aan aanvullende interne beheersmaatregelen van de gebruikersorganisaties. De geschiktheid van de opzet, het bestaan of de werking 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.

1.2 Verantwoordelijkheden 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 beheersmaatregelen 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 zoals gespecificeerd in hoofdstuk 3 Object van onderzoek.

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 ons oordeel 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-aansluiting.

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 Oordeel

Ons oordeel is 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 30 maart 2016. 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".

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.	Voldoet
B0-6	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	Voldoet
B0-7	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagementproces doorgevoerd.	Voldoet
B0-8	Penetratietests worden periodiek uitgevoerd.	Voldoet
B0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	Voldoet
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/ toegangsbeheer.	Voldoet
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	Niet van toepassing
B0-14	Leg afspraken met leveranciers vast in een overeenkomst.	Niet van toepassing
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.	Voldoet

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B1-2	Beheer- en productieverkeer zijn van elkaar gescheiden.	Voldoet
B1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.	Voldoet
B2-1	Maak gebruik van veilige beheermechanismen.	Voldoet
B3-1	De webapplicatie valideert de inhoud van een HTTP-request voor deze wordt gebruikt.	Voldoet
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthentiseerd is en de juiste autorisaties heeft.	Voldoet
B3-3	De webapplicatie normaliseert invoerdata voor validatie.	Voldoet
B3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer.	Voldoet
B3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de web applicatie alleen geparametriseerde queries.	Voldoet
B3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	Voldoet
B3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	Voldoet
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	Voldoet
B3-16	Zet de cookie attributen ‘HttpOnly’ en ‘Secure’.	Voldoet
B5-1	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	Voldoet
B5-2	Maak gebruik van versleutelde (HTTPS) verbindingen.	Voldoet
B5-3	Sla gevoelige gegevens – voor zover betrekking hebbend op Digid – versleuteld of gehashed op.	Voldoet
B5-4	Versleutel cookies.	Voldoet
B7-1	Maak gebruik van Intrusion Detection Systemen (IDS).	Voldoet
B7-8	Voer actief controles uit op logging.	Voldoet
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en respons inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	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-aansluiting.

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.

Schiphol-Rijk, 30 maart 2016

ControlSolutions International BV
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 van cliënten van Liaan Consult B.V.

Liaan Consult B.V. biedt de volgende functionaliteit aan waarvoor de betrokken 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 6.1. Deze applicatie betreft standaard software en wordt onderhouden door Liaan Consult 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

In het kader van de ICT-beveiligingsassessment DigiD is Liaan Consult B.V. een service-organisatie. Bij de opzet en implementatie van interne beheersmaatregelen nemen wij voor een aantal beveiligingsrichtlijnen van de 'Norm ICT-beveiligingsassessment DigiD' aan, dat interne beheersmaatregelen door gebruikersorganisaties zullen worden geïmplementeerd om te voldoen aan de 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.

Nr	Beschrijving van de beveiligingsrichtlijn	Beheersactiviteit gebruikersorganisatie
B0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	De gebruikersorganisatie dient maatregelen te ontwerpen en in te richten met betrekking tot wijzigingsbeheer. Hierbij valt te denken aan indienen van wijzigingsverzoeken en uitvoeren van acceptatietests.
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging / toegangsbeheer.	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.
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	De gebruikersorganisatie dient zelf te waarborgen dat niet gebruikte websites en informatie worden verwijderd.
B0-14	Leg afspraken met leveranciers vast in een overeenkomst.	De gebruikersorganisatie dient zelf de afspraken met leveranciers vast te leggen in overeenkomsten.
B2-1	Maak gebruik van veilige beheermechanismen.	De gebruikersorganisatie dient gebruik te maken van veilige beheermechanismen. Hierbij valt te denken aan strong authentication, wachtwoordinstellingen en gebruik van een pincode-functionaliteit.
B5-3	Sla gevoelige gegevens – voor zover betrekking hebbend op DigiD – versleuteld of gehashed op.	De gebruikersorganisatie dient een gegevens-classificatie uit te voeren op de gegevens die via de DigiD-koppeling worden ontsloten.
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en respons inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	De gebruikersorganisatie dient haar eigen informatiebeveiliging te waarborgen. Hierbij valt te denken aan een informatiebeveiligingsbeleid in brede context en specifiek het proces ten aanzien van preventie, detectie en respons inzake informatiebeveiliging.