Rapportage DigiD Assessment - ENSIA 2017 Aansluiting no. 1000081

Bijlage B en C

Reg.nr. Haarlem: 2018/222836

Vragen vooraf

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	Ja
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	1 assessmentplichtige DigiD aansluiting

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	1000081
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	Gemeente Haarlem
Externe infrastructuur-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Nee
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Ja
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Nee

Bijlage B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 1000081 en Gemeente Haarlem.

Gemeente Haarlem biedt functionaliteit aan op de website waarvoor DigiD aansluiting 1000081 voor authenticatie wordt gebruikt. Dit betreft het leveren van diensten waarvoor het noodzakelijk is dat de aanvrager wordt geïdentificeerd en geauthenticeerd.

Deze applicatie betreft een eigen oplossing van de gemeente Haarlem en wordt onderhouden door medewerkers van ICT.

Deze applicatie is extern benaderbaar via de volgende URL(s): www.haarlem.nl . De infrastructuur waar deze applicaties op draaien wordt beheerd door de gemeente Haarlem.

Het object van onderzoek was de webomgeving van DigiD aansluiting. Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze 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.

Bijlage C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van gemeente Haarlem

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 1000081 en Gemeente Haarlem.

Norm	Beschrijving van de norm	Resultaat	Toelichting
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 niet	Hoewel externe contentmanagers onder beleid en processen Haarlem vallen, is in het contract onvoldoende vastgelegd om aan deze norm te voldoen.
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 niet	Voldoet nog niet, verbetering is ingezet. Om volledig te voldoen is een infrastrucuturele wijziging nodig welke in 2018 is gepland.
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 niet	Verdere verbetering is nodig voor wat betreft encryptie van opgeslagen gegevens.
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 een hardeningsrichtlijn beschikbaar.	Voldoet niet	In ‘opzet’ is de hardeningsrichtlijn beschikbaar. Op punten is bij vaststellen ‘bestaan’ geconstateerd dat verbetering nodig is, waarvan de implementatie in gang is gezet.

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 niet	Er is een DMZ maar verdere verbetering is nodig, met name door de productieomgeving volledig te scheiden van andere omgevingen. Deze verbetering is in gang gezet.
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 hardeningrichtlijn 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 niet	Voldeed niet op het moment van de evaluatie, maar is toegevoegd aan de beheertaken. Voldoet inmiddels wel.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet niet	Verbetering is nodig. Bij evaluatie blijkt dat niet altijd het proces wordt gevolgd wanneer een wijziging met spoed wordt uitgevoerd. Juist bij deze gevallen is het proces belangrijk.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	