

Bijlage bij het Assurancerapport inzake DigiD – Gemeente Lansingerland (Zaaksysteem)

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
B0-5	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgesteld en op het juiste (organisatorische) niveau vastgesteld.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken. Via inspectie van documentatie vastgesteld dat een getekend contract inzake het beheer en hosting van de DigiD webapplicatie aanwezig is. Via inspectie van het contract, SLA en bewerkersovereenkomst met Zaaksysteem.nl vastgesteld dat de volgende onderwerpen zijn benoemd: • een beschrijving van de diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden • informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten en datalekken; • het jaarlijks uitvoeren van audits bij de leverancier(s) • Service Level Reporting; • de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen / data van de gebruikersorganisatie mag hebben; Bewerkersovereenkomst Lansingerland en Mintlab; • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers. • Service Level Reporting verloopt via een dashboard	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
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 de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken. Via inspectie van documentatie vastgesteld dat de procedure voor het toekennen, wijzigen, intrekken en periodiek controleren van toegangsrechten is beschreven. Via inspectie van documentatie vastgesteld dat een wachtwoordbeleid is beschreven. Via inspectie van systeeminstellingen vastgesteld dat het wachtwoord op netwerkniveau aan specifieke eisen dient te voldoen. Via inspectie van uitdienstgetreden medewerkers vastgesteld dat het account verwijderd was. Via inspectie van indienstgetreden medewerkers vastgesteld dat de toegang tot het Zaaksysteem verleend is die ook aangevraagd was. Via interview vastgesteld dat geen movers aanwezig waren. Via inspectie van documentatie vastgesteld dat periodieke controle op verleende toegangsrechten in het Zaaksysteem heeft plaatsgevonden. Via reperformance vastgesteld dat met enkele standaard wachtwoorden geen toegang werd verkregen tot het ingebouwde admin account in het Zaaksysteem.	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
		Via inspectie van accounts in het Zaaksysteem vastgesteld dat geen niet-persoonsgebonden accounts aanwezig waren.	
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken. Via inspectie van documentatie vastgesteld dat de procedure voor het toekennen, wijzigen, intrekken en periodiek controleren van toegangsrechten is beschreven. Via inspectie van documentatie vastgesteld dat summier een beschrijving van taken, verantwoordelijkheden en bevoegdheden van de functioneel applicatiebeheerrol aanwezig is. Via inspectie van documentatie vastgesteld dat periodieke controle op verleende toegangsrechten in het Zaaksysteem heeft plaatsgevonden. Via inspectie van documentatie vastgesteld dat een autorisatiematrix voor Zaaksysteem is opgesteld. Via inspectie van de autorisatiematrix en de beheerrollen in Zaaksysteem vastgesteld dat de beheerrollen zoals beschreven in de autorisatiematrix in Zaaksysteem zijn toegekend.	Voldoet Wij bevelen aan een uitgebreide beschrijving van taken, verantwoordelijkheden en bevoegdheden van de functioneel applicatiebeheerrol op te stellen.

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken. Via inspectie van documentatie vastgesteld dat dataclassificatie voor het Zaaksysteem heeft plaatsgevonden en is opgenomen in het register van verwerkingen voor de AVG.	Voldoet
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
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.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	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.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	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.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken. Via inspectie van documentatie vastgesteld dat de procedure voor wijzigingsbeheer van het Zaaksysteem is beschreven. Via inspectie van URL's vastgesteld dat de productie omgeving gescheiden is van de acceptatie en	Voldoet Lansingerland geeft aan dat geen wijzigingen door Lansingerland zijn aangevraagd derhalve hebben we het bestaan niet kunnen vaststellen.

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
		ontwikkelomgeving.	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.	Vanuit de TPM rapportage van Zaaksysteem.nl met kenmerk MMC/DIGID/LSL28112017 , gedateerd 17 november 2017, zijn geen afwijkingen op deze norm gebleken.	Voldoet