2021: eDiensten Mijn inkomen & Mijn regie geslaagd voor DigiD-audit

De eDiensten zijn de afgelopen periode (**Q3 en Q4 2021**) door een externe partij beoordeeld op de normen die Logius stelt aan het gebruik van DigiD.

Dit beveiligingsassessment keert jaarlijks terug. Alle eDiensten zijn met vlag en wimpel geslaagd en daarmee weer als veilige en betrouwbare oplossingen bestempeld.

Datum rapportage externe partij: **28 oktober 2021.** De TPM-verklaringen zijn door Centric aan de klanten verstuurd die gebruik maken van deze oplossing.

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
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
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	Voldoet

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
	protectiemechanismen.	
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 assessments (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