ICT normenkader DigiD

* B.05 In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgesteld en op het juiste (organisatorische) niveau vastgesteld.
* 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.
* U/WA.02 Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
* U/WA.03 De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
* U/WA.04 De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
* U/WA.05 De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
* U/PW.02 De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
* U/PW.03 De webserver is ingericht volgens een configuratie-baseline.
* 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.
* U/PW.07 Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
* 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.
* U/NW.04 De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.
* U/NW.05 Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
* U/NW.06 Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.
* C.03 Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
* C.04 Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
* C.06 In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
* C.08 Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
* C.09 Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geinstalleerd in de ICTvoorzieningen.