Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Raad van State
Afdeling IT-beheer
t.a.v. [redacted] 10,2,e
Postbus 20019
2500 EA Den Haag

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Inlichtingen
[redacted] 10,2,e
T 070[redacted]
[redacted]@minfin.nl

Ons kenmerk
ADR/2015/177

Uw brief (kenmerk)
-

Bijlagen
Geen

Datum: 6 februari 2015
Betreft: Tweede hertoets van de normen met als oordeel "voldoet niet" betreffende de uitgevoerde DigiD ICT-beveiligingsassessment per 27 januari 2014 over aansluiting Digitaal Loket van de Raad van State.

Met het assurancerapport met kenmerk ADR-2014-126, d.d. 27 januari 2014, is invulling gegeven aan het uitvoeren van een onderzoek naar het voldoen aan het normenkader zoals beschreven in de 'Norm ICT-beveiligingsassessments DigiD' van Logius. De daarin gestelde normen die een oordeel "voldoet niet" bevatten zijn voor Logius aanleiding geweest om aan de aansluitende organisaties een verbeterplan en een hertoets van de betreffende normen te verlangen.

De uitkomsten van de hertoets (uitgevoerd door de Auditdienst Rijk) naar de stand per 15 juli 2014 (kenmerk ADR/2014/1044, d.d. 15 juli 2014) zijn voor Logius (brief kenmerk Logius/2015/U003182, d.d. 22 januari 2015) aanleiding geweest om bij de Raad van State aan te dringen om per direct alsnog aan de toetsingcriteria (te weten, de normen B3-15, B7-8 en B7-9 die bij de eerste hertoets niet voldeden) te voldoen.

Op verzoek van de Raad van State is in de week van 2 februari 2015 door de Auditdienst Rijk een tweede hertoets uitgevoerd op voornoemde normen die onderdeel uitmaken van de DigiD ICT-beveiligingsrichtlijn. Hieronder zijn de uitkomsten van deze werkzaamheden per norm nader beschreven en voorzien van een oordeel.

Maatregel nummer:	Omschrijving
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd

Opzet en bestaan	
Korte omschrijving van uitgevoerde werkzaamheden:	Op 2 februari 2015 heeft de ADR een blackbox scan uitgevoerd met de tools AppScan (IBM) en ZAP (OWASP). De scans waren voor wat betreft de scope van het onderzoek gericht op de webapplicatie Digitaal Loket en getoetst tegen de OWASP benchmark voor Application Software. De uitkomsten in de vorm van rapportages zijn gedeeld en beschikbaar gesteld aan de Raad van State. Deze scans zullen bij de DigiD ICT-beveiligingsassessment over het jaar 2014 worden herhaald. De ZAP scan zal zelfstandig door de Raad van State worden herhaald.
Oordeel:	**Voldoet**

Maatregel nummer:	Omschrijving
B7-8	Voer actief controles uit op logging.

Opzet en bestaan	
Korte omschrijving van uitgevoerde werkzaamheden:	Er is logging die actief door de Raad van State wordt gemonitord en bewaakt. Mogelijk voorkomende (beveiligings)incidenten worden opgepakt. De Raad van State heeft haar logstructuur en -beleid t.a.v. de webapplicatie Digitaal Loket nader toegelicht en verklaard. Op 2 en 4 februari hebben ter zake interviews en waarnemingen ter plaatse plaatsgevonden. Uit de interviews is gebleken dat het logbeleid onderdeel gaat uitmaken van het onderhanden zijnde inventariserend onderzoek (van IT-organisatie Fox-IT) met daaruit te actualiseren beveiligingsplan en - beleid. Verder is het de bedoeling om de leerpunten en ervaringen uit de invoering van de Baseline Informatiebeveiliging Rijksdienst (BIR), in relatie tot de log essentialia, daarin te betrekken. Ter plaatse zijn het daadwerkelijke bestaan en de aanwezige structuur van logging afkomstig van de external firewalls, de monitoring & alerting systemen (CheckPoint, Sophos UTM SG 310 en SolarWinds), evenals voor de webapplicatie Digitaal Loket, inhoudelijk beoordeeld en getoetst. Configuratie-instellingen voor het periodiek draaien van diverse

	rapportagevormen met verschillen in periodiciteit zijn waargenomen. De bewaartermijn voor de logging van de external firewall is, daarbij vooruitlopend op de uitkomsten van het te actualiseren logbeleid (zie hierna inventariserend onderzoek door Fox-IT), per direct door de Raad van State verhoogd van 30 naar 155 dagen. De overige bewaartermijnen van logfiles, in relatie tot de webapplicatie Digitaal Loket, gaven geen directe aanleiding tot passende maatregelen. Voorts zijn door de Raad van State voor dit onderzoek standaardrapportages beschikbaar gesteld, afkomstig van de monitoring & alerting systemen. Ook zijn op verzoek enkele selectieve tests op realtime logfiles, in relatie tot de webapplicatie Digitaal Loket, uitgevoerd teneinde de werking van de filtering op 'critical occurences' vast te stellen. Vastgesteld is dat de Raad van State (na de eerste hertoets) verbeteringen heeft doorgevoerd in samenhang met de logging en de wijze waarop dit thans via dashboards (ondermeer met behulp van de nieuwe network monitoring software SolarWinds) op actieve wijze wordt gemonitord en bewaakt.
Oordeel:	**Voldoet**

Maatregel nummer:	**Omschrijving**
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.

	Opzet en bestaan
Korte omschrijving van uitgevoerde werkzaamheden:	Organisatorische invulling t.a.v. de informatiebeveiliging bij de Raad van State: ➢ De Raad van State beschikt over een afzonderlijke functionaris die zich bezighoudt met (informatie) beveiliging in brede zin. Deze functionaris ressorteert onder de Directie Bedrijfsondersteuning van de Raad van State. De context tot de ICT-voorziening, in het bijzonder tot de webapplicatie Digitaal Loket, in relatie tot de daaraan gestelde aansluitingscriteria

	DigiD-beveiligingsassessment zijn hem bekend. ➢ Binnen de IT-afdeling, behorend tot de eenheid Plaatsvervangend Secretaris, zijn het Hoofd IT-beheer en een technisch beheerder benoemd die verantwoordelijk respectievelijk uitvoerings-verantwoordelijk zijn voor de beveiliging en derhalve voor het afhandelen van (beveiligings)incidenten, indien personen kwaadwillend misbruik willen plegen of hebben gepleegd ten aanzien van de ICT-voorzieningen en de infrastructuur van de Raad van State. ➢ Elke donderdag wordt door beide functionarissen van de eenheid Plaatsvervangend Secretaris, op basis van de uitkomsten van een scala aan monitorings- en alerting rapportages, de severity en mogelijke impact van de gedetecteerde gebeurtenissen ('occurences') afkomstig van de externe kopppelvlakken (firewalls) en de antivirus systemen, inhoudelijk besproken en gedeeld. De rapportages afkomstig van de monitoring & alerting systemen worden op de management-server 1 jaar bewaard. ➢ Indien nodig vinden, naar aanleiding van het wekelijks overleg, bijstellingen van de ingeregelde filtering van de ICT-monitorings en alerting systemen plaats en zal daartoe een service request of wijzigingsverzoek in de daartoe ingerichte helpdesk tool TopDesk worden ingebracht. ➢ Voor aanpassingen in de technische configuratie en voor specifieke technische ondersteuning beschikt de Raad van State over een volwaardig servicecontract met een externe ICT-dienstverlener. De externe ICT-dienstverlener voert in opdracht van de Raad van State werkzaamheden uit aan ondermeer de firewalls evenals aan de overige netwerk ICT-componenten die onderdeel uitmaken van de infrastructuur van de Raad van State.
Oordeel:	**Voldoet**

Bronnen (namen van documenten, bestanden, screen prints, enz.)
1a. Rapportage AppScan (IBM)
1b. Rapportage ZAP (OWASP)
1c. Diverse printscreens log- en rapportagestructuur
1d. Printscreen Outlook (schedule wekelijks (beveiligings)incidentenoverleg
1e. Configuratie evidence (crontab) firewalls CheckPoint

In deze gerichte follow-up audit zijn de opzet en het bestaan van de normen B3-15, B7-8 en B7-9 naar de stand per 5 februari 2015 voldoende bevonden.

In de DigiD ICT-beveiligingsassessment over het jaar 2014 zullen de opzet en het bestaan voor deze normen worden geëvalueerd.

Datum:	6 februari 2015
Naam:	[redacted]
Organisatie:	Auditdienst Rijk – Ministerie van Financiën
Handtekening:	[redacted] 6/2/2015

10,2,e

10,2,e