

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Ministerie van
Binnenlandse Zaken en
Koninkrijksrelaties**

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Kenmerk
2019-0000173413

Uw kenmerk

Datum 16 april 2019

Betreft Voortgang informatiebeveiliging SSO Caribisch Nederland

Hierbij informeer ik uw Kamer over de voortgang van de verbetering van de Informatiebeveiliging van de Rijksdienst Caribisch Nederland.

Verantwoordingonderzoek 2017 Algemene Rekenkamer

De Algemene Rekenkamer besloot in april 2018, op grond van artikel 7.21, lid 1 van de Comptabiliteitswet 2016, bezwaar te maken tegen de informatiebeveiliging van de Rijksdienst Caribisch Nederland (RCN). De informatiebeveiligingsfunctie is naast andere bedrijfsvoeringsfuncties ondergebracht bij de Shared Service Organisatie Caribisch Nederland (SSO-CN). In de periode 2014-2017 was naar het oordeel van de Algemene Rekenkamer weinig vooruitgang in de uitvoering geboekt en belangrijke beveiligingsrisico's bleven onvoldoende afgedekt door passende beheersmaatregelen. In het Verantwoordingsonderzoek 2017 stelde de Algemene Rekenkamer een ernstige onvolkomenheid vast in de informatiebeveiliging van de RCN.

Op 30 april 2018 ontving de Algemene Rekenkamer het verbeterplan Informatiebeveiliging RCN. Dat plan toonde naar het oordeel van de Algemene Rekenkamer aan dat de minister van Binnenlandse Zaken en Koninkrijksrelaties met veel inzet aan de slag is gegaan om concrete maatregelen te treffen, gericht op de aanpak van de ernstige onvolkomenheid in de informatiebeveiliging. Gezien de genomen maatregelen en het verbeterplan besloot de Algemene Rekenkamer het bezwaar bij deze ernstige onvolkomenheid niet te handhaven. In de loop van 2018 zijn er forse stappen gemaakt in het op orde brengen van de informatiebeveiliging.

Stand van zaken verbetermaatregelen

De Auditdienst Rijk (ADR) is door de Chief Information Officer van BZK (CIO-BZK) gevraagd onderzoek te doen naar de daadwerkelijke implementatie van de meest urgente verbetermaatregelen, gericht op de externe- en interne dreigingen in de netwerkinfrastructuur van SSO-CN. Daarnaast vroeg de CIO-BZK de ADR te onderzoeken of de verbetermaatregelen voor de middellange- en lange termijn zijn afgerond, dan wel door SSO-CN concreet onderhanden zijn. Het doel van de middellange- en lange termijn verbetermaatregelen is om de resterende risico's in de informatiebeveiliging weg te nemen en zorg te dragen voor inbedding van de verbetermaatregelen in de te actualiseren Plan-Do-Check-Act (PDCA-cyclus) van SSO-CN.

Het onderzoek van de ADR liet een positieve ontwikkeling zien. De ADR heeft gevalideerd dat de korte termijn verbetermaatregelen uit het verbeterplan van de SSO-CN met de meeste urgentie in de netwerkinfrastructuur van SSO CN zijn geïmplementeerd en dat daarmee de eerder gesignaleerde risico's zijn teruggebracht. De implementatie van de middellange en lange termijn maatregelen is afgerond, dan wel belegd in de lijnorganisatie van SSO-CN. Veel verbetermaatregelen hadden betrekking op het in orde brengen van (technische) beveiligingsmaatregelen in IT-componenten van SSO-CN en zijn feitelijk te beschouwen als 'hygiëne-factoren' in een te ontwerpen beveiligingsarchitectuur. De resultaten van het ADR-onderzoek bevestigen dat de geplande verbeteringen op koers liggen.

Vervolgstappen

Naast de door de ADR en Algemene Rekenkamer gesignaleerde tekortkomingen heb ik vastgesteld dat een verbetering van de interne controlesystematiek noodzakelijk is om de aangebrachte verbeteringen te borgen en hierop in 2019 verder te sturen. Nog te realiseren verbeteringen zijn opgenomen en beschreven in de begroting van SSO-CN voor 2019 en worden met prioriteit opgepakt. Behalve borging van de standaard dienstverlening, ziet dit op het toekomstbestendig maken van de informatiebeveiliging. Met name door een verbeterde PDCA-cyclus, kan en zal er adequater worden gestuurd op aanpak van eventuele risico's en tekortkomingen.

Een belangrijk aandachtspunt bij SSO CN is de beschikbaarheid van voldoende senior ICT-expertise, zodanig dat de ICT-dienstverlening blijvend op niveau is en er tijdig en adequaat kan worden geanticipeerd op behoeften van afnemers en ontwikkelingen in het vakgebied, waaronder informatiebeveiliging. Beschikbaarheid van die expertise is momenteel niet structureel voorhanden en legt een hypotheek op de capaciteit en het functioneren van de beheerorganisatie. Om daaraan het hoofd te bieden, wordt die capaciteit nu met regelmaat –tijdelijk- aangevuld met externe expertise, die ook binnen de markt, zeker de lokale en regionale markt, schaars is. Een structurele oplossing, die de gehele ICT-dienstverlening van SSO-CN en de doelmatigheid daarvan ten goede komt, acht ik wenselijk. Om die reden laat ik momenteel verkennen op welke wijzen daar invulling aan gegeven kan worden.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

drs. R.W. Knops