Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

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

Directie Informatievoorziening en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum 29 oktober 2018
Onderwerp Plan van aanpak 'Verbetering centrale sturing en beheersing informatiebeveiliging JenV'

Ons kenmerk
2386711

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

In het verantwoordingsdebat van 13 juni 2018 heeft uw Kamer gesproken over het rapport Verantwoordingsonderzoek 2017 van de Algemene Rekenkamer (ARK). De ARK heeft geconstateerd dat op het gebied van informatiebeveiliging (IB) door mijn ministerie stappen zijn gezet en de centrale sturing en beheersing zijn verstevigd, maar dat er nog verbeteringen mogelijk zijn. Met name op het gebied van risico- en incidentmanagement waren de verbeteringen nog onvoldoende gevorderd om de onvolkomenheid voor informatiebeveiliging op te heffen. De ARK heeft deze onvolkomenheid gebaseerd op het onderzoek van de Auditdienst Rijk (ADR) naar de volwassenheid van de centrale beheersing van de informatiebeveiliging.

Tijdens het debat heb ik u een Plan van Aanpak toegezegd waarin ik beschrijf hoe de centrale sturing en beheersing van de informatiebeveiliging van mijn ministerie op een hoger niveau wordt gebracht. Hierbij bied ik uw Kamer het plan van aanpak "Verbetering centrale sturing en beheersing informatiebeveiliging Justitie en Veiligheid" aan.

Achtereenvolgens ga ik in op de hoofdlijnen van het plan van aanpak alsook de speerpunten voor de komende jaren. Tot slot zal ik kort beschrijven wat in 2018 ten aanzien van de centrale sturing en beheersing van de informatiebeveiliging is gerealiseerd of al wordt uitgevoerd.

Directie Informatievoorziening en Inkoop

Datum
21 augustus 2018

Ons kenmerk
2386711

Hoofdlijnen van plan van aanpak

Het uitgangspunt voor mijn plan van aanpak is gebaseerd op het door de ADR gebruikte model van de Nederlandse Beroepsorganisatie van Accountants (NBA) model[1] om de volwassenheid van de centrale sturing en beheersing van informatiebeveiliging te meten bij het Rijk. Het model gaat uit van verschillende domeinen van centrale beheersing van IB waaronder het bv. hebben van een IB strategie, IB kaders, een toereikende organisatie en aanwezigheid service level management in relatie tot leveranciers. In 2017 heeft mijn ministerie op een vijfpuntsschaal een *gemiddeld* volwassenheidsniveau van 2.9 gescoord. De ambitie is om in 2021 te groeien naar een gemiddeld volwassenheidniveau van 4.2. Dat zal een behoorlijke inspanning vergen. Met name op het gebied van risico- en incidentmanagement (volwassenheidsniveau score resp. 2.3 en 2 in 2017) constateer ik dat nog verdere groei in volwassenheid noodzakelijk is. Dat verhoogd de weerbaarheid van mijn ministerie op het gebied van IB.

Het plan van aanpak is op hoofdlijnen de komende jaren dan ook gericht op het verhogen van die weerbaarheid en het op gang brengen van preventieve alsook repressieve maatregelen en activiteiten daartoe. Naast technische maatregelen is de factor mens een cruciale factor bij informatiebeveiliging. Preventieve maatregelen worden dan ook gezocht in het continu bewust maken van medewerkers hoe om te gaan met waardevolle informatie. De repressieve maatregelen zijn onder andere gericht op het verkorten van hersteltijd bij incidenten om schade zo veel mogelijk te beperken.

Speerpunten voor de komende jaren zijn het verbeteren van de governance ten aanzien van de informatiebeveiliging, het versterken van risicomanagement en het verbeteren van incidentmanagement.

Om decentraal een nog beter gevalideerd beeld te krijgen van de volwassenheid van beheersing op de IB zal toepassing van het volwassenheidsmodel (NBA) de komende jaren worden uitgebreid naar de taakorganisaties.

Realisatie van maatregelen in 2018

Ten aanzien van de reeds gerealiseerde maatregelen wil ik graag ter illustratie, niet limitatief, een aantal reeds gerealiseerde en/of in gang gezette acties benoemen.

Om het incident- en risicomanagement te verstevigen is op het niveau van JenV inmiddels een incident- en escalatieprocedure IB ontwikkeld en in de (Brede) Bestuursraad vastgesteld. De incident- en escalatieprocedure geeft inzicht in taken, verantwoordelijkheden en bevoegdheden van diverse actoren bij het zich voordoen van een ernstig IB incident en de opschaling ervan. In het najaar van 2018 wordt een simulatie uitgevoerd met alle betrokken partijen, met als doel de werking ervan in de praktijk te toetsen. Ook is de circulaire "Meldplicht Datalekken" op het nieuwe besturingsmodel geactualiseerd en vastgesteld.

[1] De handreiking bij het NBA model is te vinden op de NBAsite: https://www.nba.nl

Directie Informatievoorziening en Inkoop

Datum
21 augustus 2018

Ons kenmerk
2386711

Bij het ministerie van JenV zijn de primaire processen sterk afhankelijk van ICT en veel van de verwerkte gegevens zijn gevoelig van aard. Als laatste wil ik dan ook graag benoemen dat een meerjarig project is gestart voor het verhogen van de weerbaarheid van medewerkers en leidinggevende in het verwerken en omgaan met waardevolle informatie. Het betreft hier data waarvan J&V vindt dat deze informatie op het hoogste niveau van weerbaarheid moet zijn georganiseerd om het hoofd te bieden aan dreiging van corruptie, verlies of diefstal door onder andere criminelen en statelijke actoren.

Ik verwijs ik u voor een meer getailleerde toelichting op mijn meerjarige ambitie op het gebied van Informatiebeveiliging naar het bijgevoegde plan van aanpak "Verbetering centrale sturing en beheersing informatiebeveiliging Justitie en Veiligheid".

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus