Hoogheemraadschap van
Rijnland

18.164571

Rapportage follow-up Rekenkamercommissie rapport informatiebeveiliging

De Rekenkamercommissie heeft de rapportage van de landelijke Taskforce Bestuur & Informatieveiligheid Dienstverlening (BID) van november 2014 als uitgangspunt genomen. Deze adviezen beschrijven de inrichting van de informatiebeveiliging op hoog niveau. Vervolgens heeft de rekenkamercommissie ingezoomd op een aantal specifieke onderwerpen. Een technische test door een ethisch hacker van de RKC heeft kwetsbaarheden aan het licht gebracht, aanvullend hierop organiseert Rijnland zelf her-testen door ethische hackers. In deze rapportage wordt op hetzelfde niveau als in de rapportage van de rekenkamercommissie de actuele stand van zaken weergegeven. In de toelichting onder 2.5 worden bijzonderheden aangegeven over de aanpak van de kwetsbaarheden, inclusief de leerpunten uit de her-testen.

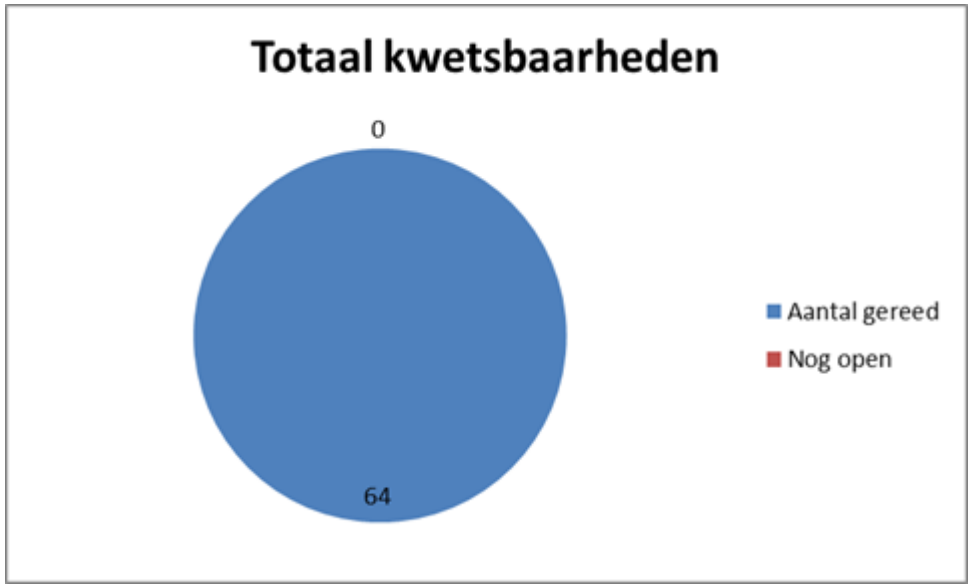
Adviezen BID

	0
	1
	7

Specifieke onderwerpen

	1
	2
	11

Herstel kwetsbaarheden



Status van de reparatie van de door de RKC aangetroffen kwetsbaarheden is inmiddels 100%.

Archimedesweg 1
postbus 156
2300 AD Leiden

KvK nr: 51137747

telefoon: (071) 30 63 063
internet: www.rijnland.net
e-mail: post@rijnland.net

BTW nr: NL813766928B01

Hoogheemraadschap van Rijnland

Datum rapportage: 12 december 2018

Uitleg kleuren in deze rapportage:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Hoogheemraadschap van Rijnland

2.1 Opvolging adviezen Taskforce BID

Deelvragen	Status RKC	Status 2018 Q1	Status 2018 Q2	Status 2018 Q3	Toelichting
Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget					Het informatiebeveiligingsbeleid is actueel. In april 2018 is het Informatiebeveiligingsplan 2018-1019 bekrachtigd in de I-raad (werkversie) is inmiddels in het Dt vastgesteld.
Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten					Het DT heeft in januari 2018 besloten een specifiek budget voor informatiebeveiliging te alloceren. Is geregeld voor 2018. Dit is inmiddels in de MJP-voorbereiding opgenomen tbv opname in de begroting 2019 e.v.
De implementatie van de Baseline Informatiebeveiliging Waterschappen (BIWA)					De landelijke audit van het Waterschapshuis heeft laten zien dat van de 44 BIWA doelstellingen Rijnland op 25 grotendeels voldoet en op 19 deels voldoet. Op geen enkele doelstelling is het oordeel “voldoet beperkt”. In het Informatiebeveiligingsplan zijn veel actie’s opgenomen die de mate van voldoen aan de BIWA zullen vergroten. Rijnland bevindt zich met de uitslag met Schieland en de Krimpenerwaard inmiddels bij de twee hoogst scorende waterschappen. Gestuurd wordt om eind 2019 volledig te voldoen, mede via een pdca-cyclus en bijbehorende borging via de opzet- en inrichting van een Information Security Management System (ISMS). Overigens zal de BIWA in 2019 worden opgevolgd door de BIO (Baseline Informatieveiligheid Overheden).
Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere Planning & Control-cyclus					De PDCA-cyclus voor informatiebeveiliging functioneert en sluit aan op de reguliere P&C-cyclus. Om in control te komen hiervan is het ISO (Information Security Office) bezig met de opzet & inrichting van het ISMS (Information Security Management Systeem) en het borgen hiervan in de bedrijfsvoering. . Er is een vooronderzoek gestart om duidelijk in beeld te hebben welke applicatie/systeem het meest geschikt is.

Deelvragen	Status RKC	Status 2018 Q1	Status 2018 Q2	Status 2018 Q3	Toelichting
Het meten van informatieveiligheid aan de hand van indicatoren					De i-raad monitort de informatieveiligheid per kwartaal aan de hand van 42 KPI's. Indien nodig schaalt de i-raad op naar de directie.
Het aanleveren van de meting naar de koepel (UvW) ten behoeve van een beeld over de overheidslaag					Naast de initiële meting is eind 2017 een landelijke BIWA-audit georganiseerd door Het Waterschapshuis. Rijnland heeft hier alle gegevens voor aangeleverd.
Het treffen van voorbereidingen voor een audit op informatieveiligheid					Ten behoeve van de landelijke BIWA-audit zijn vele bewijsstukken verzameld en aangeleverd. In 2018 wordt een interne audit gehouden. Hieraan gerelateerd worden ook technische testen uitgevoerd, zie hiervoor ook paragraaf 2.4.
Het inrichten van incidentregistratie en incidentrapportages					De incidentregistratie van informatiebeveiligingsincidenten is uitgewerkt, ingericht en geïntegreerd in het reguliere systeem voor incidentregistratie. In de i-raad wordt de rapportage besproken.

2.2 Bevindingen RKC: Beleid en organisatie

Deelvragen	Status RKC	Status 2018Q1	Status 2018Q2	Status 2018 Q3	Toelichting
Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap?					Het informatiebeveiligingsbeleid is actueel, in april 2018 is een nieuw informatiebeveiligingsplan bekrachtigd en vastgesteld in het Dt.
Wie zijn er als verantwoordelijken aangesteld?					De verschillende rollen op het gebied van informatiebeveiliging zijn ingevuld. Januari 2018 is een nieuwe security officer benoemd. Er is ter versterking van de

Deelvragen	Status RKC	Status 2018Q1	Status 2018Q2	Status 2018 Q3	Toelichting
					informatiebeveiligingsorganisatie een nieuwe rol gedefinieerd: Operational Security Officer, is aangesteld per 1 mei 2018
Is er aandacht voor bewustwording?					Er is op verschillende fronten aandacht voor bewustwording. Dit onderwerp is nooit klaar, medewerkers en bestuursleden moeten meegroeien in hun weerbaarheid met de toenemende dreigingen vanuit de wereld om ons heen. Inmiddels de actie actie om in het voorjaar 2018 de 10 gouden regels structureel onder de aandacht te brengen afgerond. Deze 10 gouden regels liggen aan de basis van de nog vast te stellen ‘Gedragscode omgaan informatie en ICT’. In nauw samenspraak met Privacy en Communicatie wordt een communicatieplan bewustwording samengesteld.

Deelvragen	Status RKC	Status 2018Q1	Status 2018Q2	Status 2018 Q3	Toelichting

2.3 Bevindingen RKC: Risicoanalyse

Welke risico's accepteert het college en welke niet?					De objectgerichte risico-analyse is gestart met de eerste drie objecten (Ultimo/Airwatch/InProces).Het uitvoeren van een objectgerichte risico-analyse is veel werk door de grote hoeveelheid objecten en er wordt gezocht naar een efficiënte methode. Bespreking in het college is voorzien in 2019. De 1e pilot fase is opgeleverd en het vervolg (2e fase) reeds ingepland. In december 2018 wordt de 2e fase opgeleverd
Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident?					Deze vraag is nog niet eenduidig te beantwoorden, dit kan op basis van de uitkomsten van de risico-analyse,
Is de privacy van de burgers, bedrijven en overige belanghebbenden gegarandeerd? Ook in relatie tot verbonden partijen?					Er is een FG aangesteld. Het privacybeleid is vastgesteld.. Geïnventariseerd is in welke systemen persoonsgegevens worden verwerkt. De nog te nemen maatregelen zijn bekend. De Implementatie van een aantal maatregelen loopt nog door na 25 mei, maar Rijnland voldoet tijdig aan de formele eisen van de AVG. De BSGR heeft een eigen verantwoordelijkheid en heeft eveneens FG aangesteld en een beleid vastgesteld.

Hoogheemraadschap van Rijnland

2.4 Bevindingen RKC: Cyclus van informatieveiligheid

Deelvragen	Status RKC	Status 2018Q1	Status 2018Q2	Status 2018 Q3	Toelichting
Functioneert de cyclus van informatieveiligheid binnen het waterschap?					De PDCA-cyclus van informatiebeveiliging functioneert. De verbeterpunten uit 2017 zijn meegenomen in het informatiebeveiligingsplan 2018.
Vindt er een jaarlijkse toetsing plaats om na te gaan of het waterschap in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessment?					Rijnland heeft meegedaan in de landelijke audit die Het Waterschapshuis heeft georganiseerd. In 2018 is een interne audit voorzien. Daarnaast laat Rijnland de infrastructuur jaarlijks testen door een ethische hacker. In dat kader is ook een hertest uitgevoerd door dezelfde ethische hacker die de rekenkamercommissie heeft ingehuurd. Met de opzet- en inrichting van het ISMS wordt dit geborgd in de PDCA cyclus.
Wat zijn de resultaten van deze toetsing?					De landelijke audit van het Waterschapshuis heeft laten zien dat van de 44 BIWA doelstellingen Rijnland op 25 grotendeels voldoet en op 19 deels voldoet. Op geen enkele doelstelling is het oordeel “voldoet beperkt.
Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?					De adviezen uit de audit 2017 zijn meegenomen in het informatiebeveiligingsplan 2018.

2.5 Bevindingen RKC: Beveiligingsincidenten

Deelvragen	Status RKC	Status 2018Q1	Status 2018Q2	Status 2018 Q3	Toelichting
Zijn er binnen het waterschap procedures opgesteld voor incidenten?					De incidentregistratie van informatiebeveiligingsincidenten is uitgewerkt, ingericht en geïntegreerd in het reguliere systeem voor incidentregistratie. In de i-raad wordt de rapportage besproken. Indien nodig wordt opgeschaald naar de directie.
Welke risico's loopt Rijnland in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt?					Van de kwetsbaarheden die de rekenkamercommissie heeft gesignaleerd is 100% volledig opgelost (eerste kwartaal was dat 89%). De organisatie heeft een hertest laten uitvoeren en zal verder jaarlijks een technische test laten doen door een ethische hacker. Bevindingen die voortkomen uit de hertest zijn geprioriteerd en worden aangepakt.
Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest?					De nieuwe incidentregistratie is december 2017 gestart Voor 2018 staat per eind november de teller op 33 geregistreerde incidenten. De incidenten worden via een oplosgroep afgehandeld en er worden maatregelen ingezet om dergelijke incidenten in de toekomst te voorkomen. De interne bewustwordingsactie heeft tot meer meldingen geleid en dat is juist goed.
Meldt Rijnland die incidenten bij de autoriteiten?					In 2018 is één incident gemeld bij de Autoriteit persoonsgegevens of andere autoriteiten. Tevens is Rijnland aangesloten op het CERT watermanagement, het samenwerkingsverband van de waterschappen met Rijkswaterstaat voor snelle respons op dreigende incidenten (buiten het domein persoonsgegevens).