Berenschot

Quickscan Digitale Veiligheid

Bart Keijzer
Bram Lankreijer

26 maart 2018

Berenschot

Quickscan Digitale Veiligheid

Inhoud **Pagina**

Berenschot

1. Inleiding (doel en aanleiding onderzoek, onderzoeksmethode)

Met de toegenomen digitalisering van onze samenleving vormen cybercrime en andere inbreuken op de informatieveiligheid steeds serieuzere bedreigingen voor publieke organisaties, burgers en bedrijven. Een reeks kleinere en grote incidenten in het recente verleden hebben Nederland en de wereld bewuster gemaakt van de grote gevolgen die dergelijke incidenten kunnen hebben. Het wordt steeds duidelijker dat geen enkel individu of organisatie zich immuun kan wanen voor digitale dreigingen.

Ook voor het Hoogheemraadschap de Stichtse Rijnlanden (vanaf nu HDSR) groeit die afhankelijkheid van informatie en digitalisering. Enerzijds kent het Hoogheemraadschap de operatie, de bediening van gemalen en Riool Water Zuiveringsinstallaties (RWZI's), dat ondersteund wordt door meet- en bedieningssystemen. Anderzijds is HDSR een ambtelijke organisatie, met circa 400 medewerkers en benodigde werkplekken, applicaties en administratieve informatiestromen (inclusief eventuele privacy gevoelige informatie). Beide functies zijn van bedrijfskritisch en zelfs maatschappelijk belang, waarbij de vatbaarheid voor digitale dreiging in toenemende mate een rol speelt op zowel operationeel als bestuurlijk niveau.

Het is voor het algemeen bestuur (AB) belangrijk om zicht te hebben op de wijze waarop HDSR omgaat met informatieveiligheid en de risico's die zij loopt. Om het algemeen bestuur van het HDSR te ondersteunen, heeft de Rekenkamercommissie (RKC) besloten om een onderzoek in te stellen naar het beleid en de uitvoering hiervan, op het gebied van informatiebeveiliging en privacy. Dit onderzoek heeft als doel een bijdrage te leveren aan de kaderstellende en controlerende taak het algemeen bestuur. De RKC heeft voor het onderzoek de volgende centrale onderzoeksvraag geformuleerd:

"Bieden de borging en verantwoording ten aanzien van digitale veiligheid in de wisselwerking tussen het dagelijks bestuur en het algemeen bestuur voldoende inzicht en mitigatie ten aanzien van de digitale bedreigingen?"

Voor beantwoording van deze onderzoeksvraag heeft de RKC onderscheid gemaakt in een aantal subvragen, die in dit document beantwoord worden. In het algemeen: deze quickscan is een afgebakend onderzoek en richt zich op (1) de borging van digitale veiligheid door het dagelijks bestuur en (2) het bewustzijn bij en verantwoording aan het algemeen bestuur. Daarbij vallen de technische borging van digitale veiligheid ende operationele invulling en ambtelijke organisatie van HDSR buiten scope.

Om tot een gedegen antwoord te komen op de voorliggende vraag, hebben de onderzoekers onderscheid gemaakt tussen een aantal stappen. Wij hebben de volgende aanpak ingezet:

1. *Documentstudie.* In de bijlage staan de geraadpleegde stukken. Het was niet eenvoudig om de beschikking of inzicht te krijgen in alle – volgens ons – benodigde documentatie. Dit heeft onder andere te maken met de vertrouwelijkheid van sommige documentatie.

2. *Interviews met Secretaris-directeur, de CISO en de Dijkgraaf (respectievelijk als hoofd van de ambtelijke organisatie, de ambtelijke verantwoordelijke voor informatiebeveiliging en als portefeuillehouder en eindverantwoordelijke binnen het dagelijks bestuur).* Hierbij lag de focus op de ambtelijke organisatie (kaders, risico's et cetera). In het gesprek met de dijkgraaf (als portefeuillehouder binnen het dagelijks bestuur) stond met name de wisselwerking met het algemeen bestuur centraal. Van beide gesprekken is een verslag gemaakt en ter verificatie aangeboden aan de betrokkenen.
3. *Interactieve sessie algemeen bestuur.* In de interactieve sessie, met een afvaardiging van het algemeen bestuur, stond de wisselwerking tussen het algemeen bestuur en het dagelijks bestuur centraal en was er aandacht voor de (benodigde) kennis van de thematiek en grip op dit onderwerp.
4. *Hoor en wederhoor.* De bevindingen worden zowel ambtelijk als bestuurlijk getoetst.

Berenschot

2. Bevindingen (beantwoording van de aspectvragen)

In dit hoofdstuk treft u de bevindingen op de aspectvragen. Het geheel van de aspectvragen leidt uiteindelijk tot de beantwoording van de hoofdvraag in hoofdstuk 3.

Aspectvraag 1: Welke beleidsmatige kaders kent HDSR ten aanzien van de digitale veiligheid?

De volgende zaken worden door zowel de ambtelijke organisatie als het dagelijks bestuur benoemd als beleidsmatige kaders:

- **Wettelijke kaders**
  Vanzelfsprekend moet HDSR voldoen aan allerlei wet- en regelgevingen. De belangrijkste hiervan zijn de meldplicht datalekken en de Algemene Verordening Gegevensbescherming (AVG) die vanaf mei 2018 ingaat.
- **Sectorbrede afspraken**
  Door zowel de ambtelijke organisatie, het dagelijks bestuur als het algemeen bestuur worden sectorbrede afspraken (met andere waterschappen) als een belangrijk beleidsmatig kader gezien. Hierbij gaat het met name om de Baseline Informatiebeveiliging Waterschappen (BIWA). HDSR is druk doende met het in praktijk brengen hiervan. Door iedereen wordt het als zeer zinvol ervaren om aan te sluiten bij ontwikkelingen in de sector. Bovendien zijn hierover afspraken gemaakt met het Waterschapshuis, waarbij eind 2017 door een externe partij wordt getoetst bij HDSR hoe de implementatie van de BIWA verloopt.

In het kader van de onderzoeksvraag is het interessant om te vermelden dat er geen extra aanvullende kaders vanuit het algemeen bestuur zijn gesteld. Het algemeen bestuur geeft hierover twee zaken aan:

1. Er is vertrouwen in de sectorbrede richtlijnen, zoals de BIWA die integraal is verwerkt in het informatiebeveiligingsbeleid van HDSR. Hierdoor is het niet noodzakelijk om met aanvullende kaders te komen.
2. Het algemeen bestuur geeft aan over onvoldoende kennis te beschikken om een kaderstellende rol goed te vervullen.

De wettelijke kaders en de sectorbrede afspraken zijn uitgewerkt in een informatiebeveiligingsbeleid voor HDSR. Dit beleid is echter niet in het bestuur vastgesteld.

Aspectvraag 2: Leidt het beleid ten aanzien van digitale veiligheid tot het juiste inzicht om risico's in te schatten en te mitigeren?

Het beleid rondom de digitale veiligheid leidt tot het uitvoeren van een risicoanalyse op het gebied van digitale veiligheid. Voor de ICT-migratie heeft een uitgebreide analyse plaatsgevonden. Deze risico's worden vervolgens weer telkens geactualiseerd op het moment dat er een groot project of

een grote wijziging optreedt. Dit gebeurt met diverse stakeholders uit de organisatie. Aanvullend hierop is er een informatiebeveiligingsbeleid, waarin op basis van de BIWA is geïnventariseerd hoe HDSR er voor staat op de verschillende hoofdstukken van de BIWA. Hierin is per gebied in beeld gebracht welke risico's HDSR loopt, wat daar de kans op is, wat daar de impact van is, welke maatregelen genomen zijn, en welke maatregelen nog genomen moeten worden op basis van deze analyse. Dit document is vertrouwelijk en kon slechtst ter plekke door de onderzoekers ingezien worden. Gezien de vertrouwelijkheid van de risico's is dat begrijpelijk. HDSR is momenteel druk doende met het verbeteren van deze methodiek, door het inrichten van een 'Information Security Management System' (ISMS). Dit wordt door organisaties gebruikt bij het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd kwaliteitsproces rondom informatiebeveiliging. Met het inrichten van ISMS moet het breder in de organisatie gaan leven en het makkelijker worden het te monitoren.

Aanvullend hierop, maar niet voortvloeiend uit een specifiek beleid voor digitale veiligheid voert HDSR jaarlijks een integrale risicoanalyse uit. Deze wordt gehouden in het kader van de reguliere planning & control cyclus, waarbij met name aandacht is voor financiële risico's voor HDSR. Hierin komt volgens de ambtelijke organisatie een breed spectrum van risico's aan bod; van financiële risico's tot fysieke veiligheidsrisico's. Zo wordt de top 10 risico's met het college besproken en verder toegelicht aan het algemeen bestuur. De genoemde risico's worden als vertrouwelijk behandeld en daarmee niet zomaar openbaar gemaakt in stukken.

Uit het gesprek met het dagelijks bestuur bleek dat alleen de risico's uit de reguliere planning & control cyclus met het dagelijks bestuur besproken worden. Er is geen expliciete aandacht voor informatiebeveiligingsrisico's, in zoverre dat deze risico's alleen indien ze in de top 10 van risico's worden voorkomen, onder aandacht van het dagelijks bestuur komen. Het is eenmalig voorgekomen dat een digitale veiligheid gerelateerde ontwikkeling binnen de top 10 is vermeld als potentieel risico, inclusief mitigerende maatregelen. Het ging daarbij om de meldplicht datalekken, die in de vorm van een boete grote financiële impact kan hebben op de organisatie. Als reden voor het ontbreken van andere informatiebeveiligingsrisico's wordt genoemd dat de maatregelen die op het gebied van watersturing zijn genomen om de risico's mitigeren, er voor zorgen dat deze risico's in het primaire proces lager worden ingeschat. Zo is het bijvoorbeeld mogelijk om alle watersturingsinstallaties handmatig over te nemen in het geval van een digitale verstoring. Door deze maatregel is de impact van uitval van digitale sturingssystemen beperkt (tenminste bij korte duur hiervan).

De onderzoekers hebben gedurende het onderzoek op hoofdlijnen inzicht verkregen in de analyse-methodiek en de risico's zelf. Op basis van het inzicht op hoofdlijnen kunnen de onderzoekers stellen dat er op een structurele en zorgvuldige manier naar de informatieveiligheidsrisico's wordt gekeken en daarbij een breed pakket van maatregelen wordt voorgesteld. Het lijkt erop dat de juiste risico's worden ingeschat en gemitigeerd. Daarbij willen we niet zeggen dat HDSR geen risico's loopt, maar dat de risico's wel in beeld zijn en hier acties op ondernomen worden. Op het gebied van informatiebeveiliging loopt HDSR momenteel de grootste risico's op het gebied van datalekken veroorzaakt door onbewust onzorgvuldig gedrag van medewerkers. HDSR is voornemens om op dit gebied meer maatregelen te nemen de komende tijd.

Uit de gesprekken met het dagelijks bestuur en de ambtelijke organisatie bleek wel dat er veel afstemming is tussen de waterschappen. Veiligheidsincidenten worden gezamenlijk gecoördineerd en er vinden maandelijks overleggen plaats tussen de CISO's van de verschillende waterschappen. Ook hier worden de risicoanalyses besproken. HDSR hanteert daarbij een vergelijkbare methodiek als andere waterschappen.

Om te kunnen beoordelen of de door HDSR geïdentificeerde risico's ook de juiste zijn, is door de onderzoekers gekeken hoe deze risico's zich verhouden tot een landelijk beeld. Hierin komen drie relevante zaken terug:

1. Het landelijk beeld (bijvoorbeeld vanuit het Cybersecuritybeeld van het Nationale Cybersecurity Centrum) is dat ICT steeds een grotere rol speelt in ons dagelijks werk. ICT wordt op meer en meer plaatsen toegepast, waarbij de directe invloed op de fysieke omgeving groeit, terwijl analoge alternatieven verdwijnen. Daarom groeit het belang van het garanderen van betrouwbare ICT-systemen. Dit is herkenbaar voor HDSR. In het gesprek met de ambtelijke organisatie en het dagelijks bestuur bleek ook dat de kwetsbaarheid van aansturingssoftware van gemalen, sluizen en zuiveringsinstallaties herkend en erkend wordt en dat bij een waterschap van oudsher het belang om bijvoorbeeld gemalen nog analoog te kunnen bedienen aanwezig was. Dit risico is bij HDSR duidelijk in beeld, en in samenspraak met het primair proces worden de juiste maatregelen genomen, doordat alle watersturingsproces handmatig over te nemen zijn.
2. In het landelijk beeld wordt ook aandacht besteed aan de actoren die belangen kunnen aantasten, bijvoorbeeld cybercriminaliteit. Zo verleggen criminelen hun focus meer en meer naar organisaties die van belang zijn voor continuïteit van de maatschappij (zoals waterschappen of vliegvelden). Ook worden statelijke actoren steeds actiever in het saboteren van vitale processen. Terroristen uiten tevens een dergelijke dreiging, maar hebben zich nog niet gemanifesteerd. Dit geldt ook voor HDSR; het heeft nog niet te maken gehad met dergelijke incidenten. Zowel de ambtelijke organisatie als het dagelijks bestuur menen dat het niet aannemelijk is dat HDSR ten prooi valt aan deze nieuwe vorm van criminaliteit. Mochten deze actoren zich toch richten op de systemen voor watersturing, dan geldt (zoals bij punt 1 vermeld) dat er voldoende maatregelen zijn genomen om de impact hiervan te beperken.
3. Tenslotte geeft het Cybersecuritybeeld aan dat interne actoren een stabiele en beperkte dreiging zijn voor ICT-belangen. Met name industriële controlesystemen worden vaker doelwit van ransomware, en Internet-of-Things (IoT) brengt nieuwe kwetsbaarheden met zich mee. Bovendien kunnen storingen zonder moedwillige dader grote gevolgen hebben. Ook dit wordt herkend en erkend bij HDSR; de mens en organisatie zijn een cruciale factor in de veiligheid van informatie, en in de risicoanalyse worden onbewuste datalekken ook als belangrijkste risico erkend. HDSR organiseert dan ook verschillende bewustwordingssessies om medewerkers bewust te maken van de gevolgen van hun handelen. Men constateert een stijgende lijn hierin, maar beseft tegelijkertijd dat er nog regelmatig fouten worden gemaakt op dit gebied.

Aspectvraag 3: In welke mate vindt expliciet verantwoording aan het algemeen bestuur plaats ten aanzien van digitale veiligheid en digitale dreigingen?

De onderzoekers hebben zich hierbij drie vragen gesteld:

1. Wordt dit onderwerp besproken in verantwoordingsdocumenten als jaarverslagen?
2. Wordt dit onderwerp besproken tijdens vergaderingen van het algemeen bestuur? Zo ja, hoe vaak en op welke manier?
3. Hoe wordt de verantwoordelijk beleefd door het algemeen bestuur?

1. Wordt dit onderwerp besproken in verantwoordingsdocumenten als jaarverslagen?

Met betrekking tot de vraag of het onderwerp digitale veiligheid en/of dreigingen besproken wordt in verantwoordingsdocumenten, is er gekeken naar de bestuursrapportages en jaarverslagen vanaf 2013, waarin verantwoording wordt afgelegd. Deze documentstudie geeft het beeld dat na 2013 het onderwerp digitale veiligheid en/of dreigingen langzaam een plek in de documenten van het dagelijks bestuur verwerft. In de verantwoording over 2013 komt dit onderwerp niet voor, maar in bestuursrapportages en jaarverslagen over 2014 en 2015 wordt de maatregel Informatieveiligheid behandeld. Hierbij wordt kort en bondig toegelicht dat aan de hand van de BIWA een nulmeting is uitgevoerd en dat op basis van de resultaten een maatregelenpakket is samengesteld. In het bestuursverslag 2016 worden de genomen maatregelen rondom digitalisering en informatie-veiligheid compact, maar concreet toegelicht. Een voorbeeld hiervan is de uiteenzetting van de verschillende aspecten van de vernieuwde technische infrastructuur. Hieruit ontstaat het beeld dat het onderwerp digitale veiligheid en/of dreigingen vanaf de verantwoording over 2014 jaarlijks wordt besproken in de verantwoordingsdocumenten. De mate waarin dit gebeurt neemt langzaam toe. In eerste instantie betrof het een beknopte mededeling dat maatregelen rondom informatieveiligheid getroffen worden, maar dit is in de recentere verantwoordingen gegroeid tot een compacte beschrijving en uitleg van de maatregelen die genomen zijn of worden genomen.

2. Wordt dit onderwerp besproken tijdens vergaderingen van het algemeen bestuur? Zo ja, hoe vaak en op welke manier?

In de beantwoording is gekeken naar de verslaglegging van de vergaderingen van het algemeen bestuur. Het onderwerp maakt geen structureel onderdeel uit van de agenda en komt met name op basis van vraag en aanbod ter sprake. Wel zit er een lijn in de ontwikkeling hiervan. In 2014 lijkt het onderwerp nauwelijks tot niet ter sprake te komen, maar in 2015 worden vooral in de commissies enkele vragen gesteld met betrekking tot dit onderwerp. In 2016 komt het onderwerp meer en meer ter sprake. Het dagelijks bestuur voorziet al in meer informatie op digitalisering en informatie-veiligheid, wat vervolgens leidt tot meer vragen uit het algemeen bestuur over dit onderwerp. In de vergaderingen in 2017 neemt de informatievoorziening rondom digitale veiligheid en dreigingen vanuit het dagelijks bestuur verder toe.

3. Hoe beleeft het algemeen bestuur de expliciete verantwoording?

Leden van het algemeen bestuur gaven aan dat ze onvoldoende frequent op de hoogte worden gebracht door het dagelijkse bestuur, aangaande deze thematiek. De verslaglegging kenmerkt zich met name als reactief, beantwoording van vragen uit het algemeen bestuur. De documentatie bevestigt dit beeld. Deze zorg is immers, zo blijkt uit algemene beschouwingen van het algemeen bestuur in zomer van 2016, al eerder uitgesproken. Daarnaast wordt de verantwoording ook inhoudelijk als onvoldoende beoordeeld, door het algemeen bestuur. Het betreft vaak slechts informatie over voortgang (op procesniveau), waardoor het algemeen bestuur geen zicht heeft op waar HDSR inhoudelijk staat, en er op moet vertrouwen dat het de juiste richting op gaat. Zij geven aan behoefte te hebben aan een proactieve berichtgeving door het dagelijks bestuur, met meer inhoudelijke duiding. Dat kan in de vorm van een periodieke en feitelijke rapportage van (mitigerende) maatregelen en incidenten, waarmee het algemeen bestuur voldoende op de hoogte blijft. Deze taak ligt in lijn met de afspraken binnen het informatiebeveiligingsbeleid, zoals is opgesteld in 2017 en is belegd bij het dagelijks bestuur. Het algemeen bestuur begrijpt dat het een vorm moet zijn waarin niet op details wordt verantwoord, maar die wel tot voldoende inzicht leidt. De huidige verantwoording zorgt voor weinig vertrouwen van het algemeen bestuur ten aanzien van de grip op digitale veiligheid door HDSR.

Aspectvraag 4: In hoeverre is het algemeen bestuur in staat om te beoordelen of de digitale veiligheid binnen het Hoogheemraadschap De Stichtse Rijnlanden voldoende is geborgd om de primaire taakstelling en verantwoordelijkheden te verzekeren?

In deze vraag staan twee zaken centraal; de informatie die men ontvangt en de kennis die het algemeen bestuur heeft om dit te kunnen beoordelen. Zoals bij aspectvraag 3 al werd geconstateerd ontvangt het algemeen bestuur momenteel niet de juiste informatie, op het juiste moment om een goed oordeel te kunnen geven. De antwoorden op vragen vanuit het algemeen bestuur leiden niet tot betere inzichten bij het algemeen bestuur. Het algemeen bestuur geeft aan over onvoldoende kennis te beschikken voor de beoordeling van de inhoud op dit onderwerp. Echter, het algemeen bestuur vraagt zich af in welke mate men over kennis zou moeten beschikken; het gaat hier om een controlerende taak, waarbij geen dieptekennis nodig is op dit onderwerp. Dit maakt het belang voor proactieve verantwoording op het juiste abstractieniveau, in de taal van de bestuurders, duidelijk. Vergelijkende onderzoeken met andere waterschappen zouden volgens het algemeen bestuur kunnen bijdragen aan het kunnen beoordelen van de borging van de risico’s op het gebied van digitale veiligheid.

Berenschot

3. Conclusies (beantwoording van de hoofdvraag)

De bevindingen van het onderzoek op de verschillende aspectvragen leidt tot conclusies op de verschillende aspecten, waarmee vervolgens weer de hoofdvraag beantwoordt wordt. Vandaar dat hieronder eerst nog kort de beantwoording van de aspectvragen terugkomt:

1. *Welke beleidsmatige kaders kent Hoogheemraadschap De Stichtse Rijnlanden ten aanzien van digitale veiligheid?*

   HDSR hanteert met name wetgeving en sectorbrede afspraken als beleidsmatige kaders voor digitale veiligheid. Zowel het dagelijks bestuur als het algemeen bestuur heeft voldoende vertrouwen in reeds bestaande sectorspecifieke (zoals de BIWA) en wettelijke kaders en ziet geen noodzaak in het stellen van aanvullende kaders. Deze beleidsmatige kaders zijn uitgewerkt in een informatiebeveiligingsbeleid, welke echter niet door het bestuur is vastgesteld.

2. *Leidt het beleid ten aanzien van digitale veiligheid tot het juiste inzicht om risico's in te schatten en te mitigeren?*

   HDSR voert structureel en zorgvuldig een risicoanalyse uit op de informatiebeveiligingsrisico's en neemt hierbij maatregelen. Er wordt nog gewerkt aan het verder verbeteren van deze methodiek. Daarnaast worden de belangrijkste risico's ook meegenomen in de integrale risicoanalyse van HDSR, als onderdeel van de planning & control cyclus. Het omgaan met risico's hoort bij de aard van een waterschap en maatregelen die in het primair proces zijn genomen en gericht zijn op de continuïteit en betrouwbaarheid van het primaire proces lijken afdoende te zijn om de continuïteit te borgen. Door deze maatregelen worden de digitale risico's in het primaire proces niet structureel tot de belangrijkste risico's gerekend. De belangrijkste risico's die HDSR op dit moment loopt zijn de risico's op datalekken door onbewust onzorgvuldig gedrag van medewerkers.

3. *In welke mate vindt expliciet verantwoording aan het algemeen bestuur plaats ten aanzien van digitale veiligheid en digitale bedreigingen?*

   Verantwoording op dit thema gebeurt in de ogen van het algemeen bestuur niet structureel en niet proactief, zo blijkt uit de sessie met een afvaardiging van het algemeen bestuur. Dat heeft tot resultaat dat het algemeen bestuur niet het gevoel heeft dat HDSR als organisatie grip heeft op haar digitale veiligheid. Het algemeen bestuur heeft behoefte aan betere informatie om haar controlerende taak te kunnen vervullen.

4. *In hoeverre is het algemeen bestuur in staat om te beoordelen of de digitale veiligheid binnen het Hoogheemraadschap De Stichtse Rijnlanden voldoende is geborgd om de primaire taakstelling en verantwoordelijkheden te verzekeren?*

   In het algemeen bestuur is beperkt kennis aanwezig over digitale veiligheid en is daardoor beperkt in staat de eigen informatiebehoefte te formuleren. Echter, die erkenning laat onverlet dat de (niet als adequaat ervaren) verslaglegging door het dagelijks bestuur weinig vertrouwen

biedt voor de mate van grip op het onderwerp. Kortom, met name door gebrekkige informatie is het algemeen bestuur slecht in staat de digitale veiligheid van HDSR te beoordelen.

De beantwoording van deze aspectvragen leidt tot beantwoording van de hoofdvraag: "*Bieden de borging en verantwoording ten aanzien van digitale veiligheid in de wisselwerking tussen dagelijks bestuur en algemeen bestuur voldoende inzicht en mitigatie ten aanzien van digitale bedreigingen?"*

In het algemeen is er beperkte wisselwerking tussen het algemeen bestuur en het dagelijks bestuur wat betreft de digitale veiligheid van HDSR. Het onderwerp staat beperkt op de bestuurlijke agenda en wordt veelal reactief behandeld door het dagelijks bestuur. Deze gebrekkige wisselwerking bemoeilijkt de controlerende functie van het algemeen bestuur op dit dossier. Daarbij, het feit dat de expliciete verantwoording als onvoldoende wordt ervaren door het algemeen bestuur werkt niet stimulerend voor het vertrouwen in de mitigatie ten aanzien van digitale dreigingen door HDSR. De borging en verantwoording vinden met name plaats in de ambtelijke organisatie, waar met name kennis over de digitale veiligheid aanwezig is, specifiek bij CISO. Hier wordt zowel door de ambtelijke organisatie als door het bestuur sterk op geleund. De onderzoekers constateren dat HDSR structureel en zorgvuldig risicoanalyses uitvoert op het gebied van informatiebeveiliging en daarbij concreet de te nemen maatregelen benoemt. Hierbij baseert HDSR zich met name op wettelijke kaders en sectorale afspraken zoals het BIWA-normenkader. Het inzicht in de digitale dreigingen en maatregelen beperkt zich echter wel tot de ambtelijke organisatie.

NB: Of deze constateringen an sich een kwetsbaarheid vormen voor de kwaliteit van de informatiebeveiliging is interessant maar valt nu niet te zeggen. Die vraag bevindt zich overigens niet binnen de scope van dit onderzoek. Daarbij kan het ter onderbouwing van het lage vertrouwen, van belang zijn ook de bredere context te kennen en daarmee nader in te gaan op het algemene vertrouwen en de verslaglegging tussen het algemeen bestuur en het dagelijks bestuur

Berenschot

4. Tips en aanbevelingen voor het algemeen bestuur

Op basis van de bevindingen en de conclusies zijn er een aantal concrete tips en aanbevelingen geformuleerd voor het algemeen bestuur.

1. *Beleidsmatige kaders*

    - HDSR gebruikt met name de landelijke normen uit de BIWA als beleidskader. Het is verstandig om standaarden uit het veld te gebruiken, echter er kunnen goede redenen zijn (op basis van een risicoanalyse) om van de BIWA af te wijken. Denk bijvoorbeeld aan een waterschap dat de ict-dienstverlening voor meerdere waterschappen uitvoert; de impact van uitval van ict-dienstverlening is daarmee groter. Het kan zijn dat daarom meer maatregelen wenselijk zijn. Vandaar dat de stelling om de BIWA te volgen dus een stevigere onderbouwing behoeft.
    - Het algemeen bestuur geeft aan over onvoldoende kennis te beschikken om een kaderstellende rol goed te vervullen. Dat is ook niet vreemd gezien de complexiteit van het onderwerp. Uiteraard is het Algemeen Bestuur van HDSR niet het enige bestuur dat met dit vraagstuk speelt. Je zou kunnen leren van andere besturen (bijvoorbeeld van waterschappen) om zo beter invulling te kunnen geven aan de kaderstellende taak.
    - HDSR beschikt over een informatiebeveiligingsbeleid, echter deze is niet door het bestuur vastgesteld. Om het vertrouwen van het bestuur op dit onderwerp te verstevigen zou het goed zijn om het beleid (of de hoofdlijnen hiervan) door het bestuur te laten vaststellen.

2. *Inzicht in risico's*

    - De ambtelijke organisatie is continu bezig met het verbeteren van de risicoanalyse methodiek. Het is raadzaam om deze ontwikkeling door te zetten, zeker gezien het toenemende belang van ict in de processen van het hoogheemraadschap.
    - HDSR werkt met twee verschillende risicoanalyse methodieken: een losse voor digitale veiligheid en een organisatiebrede analyse. De twee analyses staan niet helemaal los van elkaar, maar de relatie tussen beide analyses zou nog verstevigd kunnen worden. Daarnaast wordt de risicoanalyse op het gebied van digitale veiligheid niet breed gedeeld in de verantwoordingsketen. Het is aan te bevelen om ook het bestuur hierin met regelmaat mee te nemen, al is het op wat abstracter niveau in verband met geheimhouding.

3. *Verantwoording ten aanzien van digitale veiligheid en digitale bedreigingen*

    - Maak afspraken tussen Dagelijks Bestuur en Algemeen Bestuur over een periodieke verslaglegging. Besteed daarbij aandacht aan de wensen over inhoud en vorm van het

Algemeen bestuur ten aanzien van die rapportage. Dat helpt het AB met haar controlerende taak, wat weer bijdraagt aan het vertrouwen in het Dagelijks bestuur en de ambtelijke organisatie op dit onderwerp.

- In de ambtelijke organisatie wordt sterk geleund op het werk van de CISO; het zou voor de borging van dit belangrijke onderwerp goed zijn als:
    - verantwoordelijkheden breder in de organisatie belegd worden. Dit begint met bewustwording bij iedereen dat digitale veiligheid een integraal onderdeel van de dagelijkse werkzaamheden is. Maar ook dat het aan alle leidinggevenden is om ook op het hierbij behorende gedrag te sturen in de praktijk
    - er in de verticale verantwoordingslijnen minder sterk geleund wordt op één functionaris.
- Over het algemeen was het lastig om inzicht te krijgen in de benodigde documenten. Van de ene kant is dit begrijpelijk omdat het over een gevoelig onderwerp gaat, waar soms geheimhouding van toepassing is. Maar van de andere kant sluit dit ook aan bij het beeld van het algemeen bestuur dat het lastig is om goed inzicht te krijgen in de risico's die het hoogheemraadschap loopt, en hoe deze gemitigeerd zijn. De bereidheid van de ambtelijke organisatie om te communiceren over dit onderwerp heeft direct effect op het vertrouwen van het algemeen bestuur. Het is dus belangrijk dat er een juiste vorm van transparantie is om te zorgen dat het algemeen bestuur zich betrokken voelt bij dit onderwerp en daarmee ook het vertrouwen heeft in de borging hiervan.

4. *In hoeverre is het algemeen bestuur in staat om te beoordelen of de digitale veiligheid binnen het Hoogheemraadschap De Stichtse Rijnlanden voldoende is geborgd om de primaire taakstelling en verantwoordelijkheden te verzekeren?*

    - Door gebrek aan kennis van het algemeen bestuur op dit onderwerp vindt men het lastig om goed te kunnen oordelen hierover. Vergelijkend onderzoek met bijvoorbeeld andere waterschappen zou hen daarbij kunnen helpen. Het zou daarom handig zijn als het Dagelijks bestuur dit soort onderzoeken (bijvoorbeeld vanuit het waterschapshuis) kan delen met het algemeen bestuur. Hierbij is het wel belangrijk om te melden dat alhoewel dit leidt tot inzicht, niet per definitie tot het goede inzicht hoeft te leiden; immers het hoogheemraadschap kan op sommige gebieden een andere risicoprofiel hebben waardoor men eigenlijk tot andere maatregelen zou moeten komen dan collega waterschappen. Bovendien zegt de stand van zaken bij andere waterschappen niet veel over of je voldoet aan alle wettelijke eisen, bijvoorbeeld in het geval dat alle waterschappen hier aan voldoen. Met andere woorden; vergelijkend onderzoek leidt tot inzicht, maar niet tot het volledige beeld.
    - Naast rapportage zien we het gebrek aan kennis over het onderwerp en eventuele bewustwording van die eerder genoemde risico's op bestuurlijk niveau. Voor de toenemende urgentie van een goede informatiebeveiliging, zowel maatschappelijk als voor

de organisatie zelf, zien we het als essentieel dat deze basiskennis ook op bestuurlijk niveau wordt opgebouwd. Denk daarbij aan kennis over de beleidkaders en de ontwikkelingen op landelijk en regionaal niveau, zodat bijvoorbeeld, als het Nationaal Cyber Security Centrum een bepaalde ontwikkeling rapporteert, het algemeen bestuur in staat is om dit te vertalen naar de situatie waar zij verantwoordelijk voor is.

.