Aan algemeen bestuur 7 februari 2022

Informatienota

Datum	1 februari 2022	Portefeuillehouder	mr. S.H.M. Ornstein MCPm
Documentnummer		Programma	Bestuur en belasting
Projectnummer		Afdeling	BDI
Bijlage(n)		Opsteller	R. de Klerk/A. Schaake

Onderwerp Informatieveiligheid en cybersecurity

Kennisnemen van

1. Landelijke afspraken over informatieveiligheid, cybersecurity en de controle daarop
2. De governance op het gebied van informatiebeveiliging
3. De digitalisering en de aanpak van risico's

Inleiding

De commissie heeft naar aanleiding van de behandeling van de i-visie vragen gesteld over cybersecurity, verplicht jaarlijks auditen en terugkeermogelijkheden naar volledige handbediening van installaties.

Kernboodschap

1. Landelijke afspraken over informatieveiligheid, cybersecurity en de controle daarop

De gezamenlijke waterschappen hebben afspraken gemaakt over de ambities en doelen van informatiebeveiliging en privacy. Die afspraken staan in de baseline 'Basis op Orde' van de Unie van Waterschappen en het Programmaplan informatieveiligheid en privacy 2020-2024 van het Waterschapshuis dat is vastgesteld door het Uitvoeringsorgaan.

De volgende ambities zijn in de baseline 'Basis op Orde' en het Programmaplan afgesproken:

- Vanaf 1 januari 2022 zijn de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) in opzet en bestaan aantoonbaar geïntegreerd in de bedrijfsvoering van de waterschappen.
- Vanaf 1 januari 2025 is de werking van de BIO- en AVG-implementatie in de bedrijfsvoering van de waterschappen aantoonbaar op volwassenheidsniveau 4.

De waterschappen hebben de coördinatie en controle collectief ingeregeld met objectieve richtlijnen en monitoring. Dit betekent dat alle waterschappen iedere 4 jaar een onafhankelijke audit op informatiebeveiliging en privacy, conform sectorale afspraken, laten uitvoeren. Deze audits worden centraal vanuit het Waterschapshuis georganiseerd.
De nadruk in de landelijke afspraken ligt op het beheersen van risico's en de invoering van BIO- en privacy maatregelen op basis van een planning en control cyclus.
Omdat informatiebeveiliging een continu proces is, zijn in 2021 bij Vallei en Veluwe risicoanalyses uitgevoerd en maatregelen gepland voor 2022. We voldoen daarmee aan de landelijke afspraken qua voortgang. Dit beeld wordt ondersteund door het slagen voor andere onafhankelijke veiligheid audits, zoals de jaarlijkse verplichte DigiD audit voor de digitale dienstverlening van het waterschap.

2. Governance informatiebeveiliging

De eindverantwoordelijkheid voor informatiebeveiliging ligt op het niveau van Dagelijks Bestuur. De uitvoering en monitoring is een ambtelijke aangelegenheid en is in de staande organisatie belegd. Dit betekent dat de verantwoordelijkheid voor het uitvoeren van risicoanalyses en het nemen van passende maatregelen, de verantwoordelijkheid van het lijnmanagement is. Afdelingen zijn zelf verantwoordelijk voor de start van de informatiebeveiliging P&C cyclus en dat het proces binnen de kaders tot stand komt. De Chief Information Security Officer begeleidt en adviseert in het proces, spreekt eenieder aan op zijn rol en escaleert zo nodig. De informatiebeveiliging P&C cyclus volgt hierbij de reguliere P&C cyclus.

Naast de P&C cyclus bestaat de rapportage structuur uit een opschaling gekoppeld aan de ernst van het risico dat gelopen wordt. In geval van acute dreigingen wordt altijd proactief de Chief Information Officer (CIO) geïnformeerd. Het gaat daarbij om het informeren van de CIO voor het geval er vragen vanuit andere DT leden of bestuur gesteld worden. Indien een dreiging opgeschaald moet worden, omdat het risico daadwerkelijk optreedt, wordt de CIO geïnformeerd over de acties die genomen gaan

worden. Deze acties worden dan opgepakt conform het opschalingsmechanisme zoals verderop geschetst is bij calamiteitenbestrijding.

De kaders voor informatiebeveiliging liggen vast in het informatiebeveiligingsbeleid. Het vaststellen van dit beleid ligt op DT-niveau. Aangezien D&H eindverantwoordelijk is, wordt het vastgestelde beleidsstuk met hen gedeeld. De CISO bewaakt de in het beleid beschreven werkwijzen en begeleidt de lijn in het toepassen van de kaders.

Naast de CISO is er een CI-office [1] die over de gehele informatievoorziening ontwikkeling besluitvormend is. De CISO rapporteert elk kwartaal aan het CI-office. Op basis van deze rapportages vindt de afstemming met de algehele informatievoorziening ontwikkeling (i-visie) plaats.

3. De digitalisering en de aanpak van risico's

De afgelopen jaren zijn ambities en doelen hoger en installaties ingewikkelder geworden. Hierdoor is de aansturing van installaties en processen steeds verder geautomatiseerd. Ook is door het automatiseren van processen en installaties de afgelopen jaren efficiëntie voordeel behaald. Deze ontwikkelingen zijn niet uniek en ook in de hele maatschappij zichtbaar. Het terugkeren naar geheel handmatige sturing is daarmee vaak niet meer mogelijk. Wij beschikken daarom over opties om op terug te vallen bij optredende stroomuitval of verstoring van de digitale aansturing. Installaties kunnen bij stroomuitval werken op noodstroomvoorzieningen of soms op mechanische aandrijving. Bij verstoring van de aanstuursoftware draaien de installaties door op basisinstellingen die in de installatieonderdelen zelf zijn vastgelegd.

Daarnaast heeft het waterschap de volgende basisset aan maatregelen:

- *Computer Emergency Response Team - WaterManagement.*
  Het waterschap is aangesloten bij het CERT-WM. Dit is een landelijke samenwerking van de waterschappen met het beveiligingscentrum van Rijkswaterstaat. Het CERT-WM monitort actief alle kwetsbaarheden in de software van ons waterschap. Bij eventuele kwetsbaarheden in systemen van waterschap Vallei en Veluwe worden we direct gewaarschuwd, inclusief een risico inschatting en potentiële oplossingen.

[1] CI-office: Strategisch overleg m.b.t. informatievoorzieningsontwikkelingen bestaande uit een DT lid in de rol van Chief information officer (CIO), programmamanager digitale transformatie, manager BDI, teamleider informatiemanagement, strategisch adviseur informatiemanagement. Periodiek aangevuld met de chief information security officer (CISO), Functionaris Gegevensbescherming en Privacy Officer.

- *Actieve monitoring ICT-infrastructuur van het waterschap.*
  Vallei en Veluwe zet marktpartijen als ethische hackers in die gespecialiseerd zijn in het 7x24 testen en monitoren van de beveiliging van ICT-infrastructuur. Bij afwijkend gedrag en kwetsbaarheden in de beveiliging, informeren ze direct het ICT-team. Zij ondersteunen daarbij actief bij het opzetten en/of uitvoeren van oplosscenario's.

- *Continue informatiedeling binnen de watersector*
  Er is continu contact via beveiligde kanalen tussen alle adviseurs informatiebeveiliging (CISO's) van waterschappen m.b.t. informatiebeveiliging.

- *Patchen en updaten.*
  Het waterschap zorgt ervoor dat software bijgewerkt wordt en daarmee actueel is. Dit doen wij door te patchen en te updaten. Dit betekent dat eventuele kwetsbaarheden in systemen zo snel mogelijk worden gedicht.

- *Pentesten*
  Regelmatig schakelt het waterschap ethische hackers in om systemen die aan het internet zijn gekoppeld te toetsen op kwetsbaarheden. Eventuele gedetecteerde kwetsbaarheden worden direct aangepakt en opgelost.

- *Oefenen, trainen en opleiden.*
  Informatiebeveiliging wordt versterkt door continu verbeteren en leren. Op 13 en 14 oktober 2021 heeft waterschap Vallei en Veluwe samen met andere waterschappen en andere netwerkpartners meegedaan aan de oefening Stroomversnelling met als thema cybersecurity. Dit jaar worden de leerpunten opgepakt. Deze oefeningen vinden regelmatig plaats.
  Daarnaast volgen alle medewerkers modules op het digitale leerplatform informatiebeveiliging en privacy over het herkennen van risico's en het handelingsperspectief.
  De ICT-beveiliging specialisten, de CISO, de Functionaris Gegevensbescherming en de Privacy Officer volgen regelmatig opleidingen op hun vakgebied om bij te blijven.

- *Back-up en herstel van data en software.*
  De data en software van het waterschap worden veiliggesteld op een veilige (offline) locatie, zodat deze na een eventuele aanval van bijvoorbeeld een hacker of ransomware, terug kan worden gezet. Regelmatig wordt het terugzetten van data en software getest.

- *Meerlagen beveiliging door netwerksegmentering*
  Maatregelen zijn verdeeld over meerdere lagen. Naast firewalls, antivirus systemen en inbraakdetectiesystemen, is de ICT-infrastructuur ook opgedeeld in meerdere beveiligingslagen of netwerksegmenten.

- *Applicatie rationalisatie*
  Ook het terugdringen of zo klein mogelijk houden van het aantal systemen draagt bij aan informatiebeveiliging. Hoe kleiner het palet aan systemen, hoe minder systemen beschermd hoeven te worden.

- *Calamiteitenbestrijding*
  In het geval dat ondanks onze preventieve en detectie maatregelen toch een ICT-calamiteit ontstaat, wordt op basis van een vastgelegde procedure opgeschaald naar de reguliere calamiteitenorganisatie. Hiermee wordt ervoor gezorgd dat werkwijzen en procedures, ook bij ICT-calamiteiten, voor iedereen gelijk en bekend zijn. Per ICT-calamiteit worden repressieve maatregelen bepaald, oplosscenario's uitgewerkt en toegepast.

Ondertekening

ir. M.J. Diependaal
directeur