Voorstel aan het AB

Van	Dagelijks Bestuur		
Scribent	Ron Piepers	ID-nummer	2019-1134774830-113
Portefeuillehouder	R. Sleijpen		
Onderwerp	BIO en AVG WBL		
Datum vergadering	13 april 2022	Agendapunt nr.	**3.4**

Gevraagde besluiten

1. Beschikbaar stellen van een budget van € 913.500,- op de exploitatie van WBL voor 2022.
2. Informatiebeveiligingsfuncties aan te stellen voor in totaal 2 FTE structureel vanaf 2024 (totale jaarlijkse kosten: € 220.000).

Argumenten

1.1 Exploitatiebudget essentieel voor behalen benodigde niveaus voor informatiebeveiliging en privacy

Het budget is eind 2021 ondergebracht in het MIP. De kosten zijn echter niet activeerbaar (getoetst bij de accountant) en deze zullen derhalve in de exploitatie opgenomen moeten worden. WBL heeft geen financiële ruimte om deze kosten op te vangen. Zonder dit exploitatiebudget kan er niet worden gestart met werving van de benodigde capaciteit en het uitvoeren van de werkzaamheden voor het behalen van de vereiste niveaus voor informatiebeveiliging en privacy en kunnen we niet voldoen aan de vigerende wet- en regelgeving m.b.t. BIO/AVG/ISO en sectorale afspraken (UvW). Het auditrapport van VKA bevat dezelfde conclusies op de gebieden van de te behalen niveaus en de noodzakelijke verbeterpunten.

2.1 Voldoen aan vigerende wet- en regelgeving m.b.t. BIO/AVG/ISO en sectorale afspraken (UvW)

De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging dat wordt gehanteerd binnen de Nederlandse overheid en iedere Nederlandse overheid moet hier wettelijk aan voldoen. Elke overheidslaag mag zijn eigen implementatiepad voor de BIO vastleggen. De waterschappen hebben in de Commissie Bestuurszaken, Communicatie en Financiën (CBCF) van de Unie van Waterschappen (UvW) afgesproken om eind 2021 aan volwassenheidsniveau 3 en eind 2023 aan volwassenheidsniveau 4 van de BIO te voldoen. Dit geldt zowel voor de kantoorautomatisering als de procesautomatisering. Niveau 3 is niet behaald in 2021. In 2022 zal WBL er alles aan doen om niveau 3 te behalen. Samen met WL wordt geëvalueerd wanneer niveau 4 realistisch en haalbaar is. Vervolgens wordt er een bestuursbesluit genomen of de doorgroei naar niveau 4 gaat plaatsvinden.

2.2 Huidige bezetting informatiebeveiligingsfunctie loopt achter de feiten aan waardoor risico's toenemen

Uit een eerdere analyse (Bijlage 1 - Roadmap Informatiebeveiliging en Privacy) blijkt dat er een aanvulling nodig is van 2 FTE's. Om de informatiebeveiligingsfunctie in te richten binnen de staande organisatie, zal in 2022 moeten worden gestart met het werven van een Chief Information Security Officer (CISO) voor 1 FTE en een netwerkbeheerder voor 1 FTE. De huidige rollen voor IT Security Officer (IT-SO), netwerkbeheerder en CISO zijn nu versnipperd ingevuld en krijgen door dedicated rollen de juiste focus.

2.3 Informatiebeveiliging structureel borgen

Vanuit de WBL-informatiebeveiligingsfunctie is de afgelopen periode kritisch gekeken naar de huidige activiteiten op het gebied van informatiebeveiliging en privacy. Hierbij is op basis van de huidige wet- en regelgeving geconstateerd dat een verdere verbeterstap nodig is op het vlak van risicobeheersing. Daarom ligt er een voorstel om de aankomende jaren de huidige activiteiten te intensiveren met als uitgangspunt een opgestelde roadmap (zie bijlage 1). In de uitgevoerde analyse is ook geconstateerd dat WBL projectmatig de

rollen voor privacy en informatiebeveiliging heeft belegd en al veel beleid heeft geschreven. De vereiste formatiecapaciteit en middelen om de WBL-informatiebeveiligingsfunctie structureel te borgen zijn in de huidige opzet nog onvoldoende gewaarborgd.

2.4 Aansluiten bij gangbare inzet voor informatievoorziening bij waterschappen

Er is géén standaard organisatiemodel. Elke organisatie zal eigen keuzes moeten maken voor het inrichten van de informatiebeveiligingsfunctie. Dit wordt in gesprekken met o.a. Waterschap Limburg en Waterschap Rivierenland bevestigd.

Kanttekeningen
1.1 Exploitatiebudget is niet voorzien

Het exploitatiebudget is niet voorzien aangezien het als investeringskrediet is meegenomen in de MIP-sprint 2021. Dit zal leiden tot een negatief resultaat op de exploitatie van 2022. Alle kosten voor 2022 kunnen niet worden opgevangen in de begroting 2022.

2.1 Datalekken onmogelijk volledig te voorkomen

Ondanks de verbetering die bereikt wordt op het gebied van informatiebeveiliging na het uitvoeren van de projectmatige aanpak voor de uitvoering, is de mogelijkheid dat er datalekken ontstaan nog altijd aanwezig. De kans dat het gebeurt, is wel kleiner geworden door de getroffen maatregelen.

2.2 Behalen van de beoogde niveaus is onzeker

Ondanks de verbetering die bereikt wordt op het gebied van informatiebeveiliging na het uitvoeren van projectmatige aanpak, is het niet zeker dat het beoogde niveau wordt bereikt. Hoewel de maatregelen zullen aansluiten bij het gewenste niveau, is de uitvoering ervan en de controle erop afhankelijk van meerdere bedrijfsfuncties in de WBL-organisatie.

2.3 en 2.4 Mensen duurzaam binden vraagt mogelijk extra middelen in de toekomst

In een tijd waarin informatiebeveiliging en privacy hot items zijn en prominent in het nieuws omdat er veel incidenten – zowel landelijk als wereldwijd – zijn, is de vraag naar mensen navenant en wordt het moeilijker mensen te binden en vast te houden binnen de salarisschalen die standaard zijn binnen de overheid. Mogelijk zal in de toekomst meer rekening gehouden moeten worden met marktconforme salarissen om de expertise binnen te houden of zal extra exploitatiebudget nodig zijn om expertise in te huren.

Doelstelling
Voldoen aan geldende wet- en regelgeving op het gebied van informatiebeveiliging en privacy voor geheel WBL en het voorkomen van informatiebeveiligingsrisico's.

Strategische doelen in relatie tot:
- Schoon en ecologisch gezond water: indien WBL te maken krijgt met een groot security-incident waarbij de toegang tot onze informatiesystemen niet of niet meer volledig mogelijk is, kan het primaire proces niet of niet optimaal verlopen. Hierdoor is er een verhoogd risico op het optreden van grote schade aan het milieu;
- Vergroten duurzaamheid: niet van toepassing;
- Vergroten maatschappelijke waarde: door invulling van de informatiebeveiligingsfunctie verkleinen we de kans op een security-incident en de negatieve invloed op onze dienstverlening aan klanten die daardoor ontstaat.

Organisatie
Ten behoeve van de invulling van de informatiebeveiligingsfunctie van WBL op te pakken en te beheren conform de eisen van BIO en AVG, binnen WBL betekent dit dat er 2 FTE's beschikbaar moet zijn, verdeeld over de rollen CISO (1 FTE), Privacy Officer (PO) en IT-SO (samen 1 FTE). De formatie-uitbreiding is een randvoorwaarde om de informatiebeveiliging in onze organisatie te waarborgen en te voldoen aan het kwaliteitsniveau dat voor 2021 en 2022 geldt overeenkomstig de uitgangspunten van de Unie van Waterschappen. In vergelijking tot het Waterschap Limburg en andere waterschappen is bij het WBL op het gebied van de informatiebeveiligingsfunctie en privacy sprake van een onderbezetting. Daarnaast noodzaakt de toename van het normenkader, de richtlijnen, audits en pentesten met betrekking tot de informatiebeveiliging tot een formatie-uitbreiding, zodat de informatiebeveiliging in onze organisatie op het vereiste volwassenheidsniveau 3 (eind 2022) en volwassenheidsniveau 4 (eind 2023) kan worden gerealiseerd en gewaarborgd. Op alle mogelijke gebieden wordt de samenwerking met Waterschap Limburg opgezocht om synergie te behalen en het benodigde werk aan WBL-zijde zo ver als mogelijk te minimaliseren. Dit kan echter momenteel niet in cijfers worden uitgedrukt, aangezien het een minimale tijdswinst oplevert waar dit het (her)gebruik van WL-documentatie betreft. Op deze manier hoeven slechts delen van de documentatie aangepast te worden en niet de volledige inhoud.

Ondernemingsraad
Niet van toepassing

Juridische aspecten
Voldoen aan vigerende wet- en regelgeving m.b.t. BIO/AVG/ISO en sectorale afspraken (UvW)

Financiële consequenties
1. Structureel vanaf 2024:
   Loonkosten CISO € 105.000 per jaar (loonschaal 11).
   Loonkosten Netwerkbeheerder € 95.000 per jaar (loonschaal 10).
   Aanvullende IT-kosten per medewerker per jaar € 10.000.
   Totale jaarlijkse structurele kosten bedragen hier € 220.000.

2. Specificatie benodigd exploitatiebudget (projectmatige aanpak gedurende 2 jaar: 2022 en 2023 plus de exploitatiekosten vanaf 2024 en elk volgend jaar continuerend)

		Projectmatige aanpak (investeringskrediet ter hoogte van € 1.160.000,- is reeds meegenomen in MIP Sprint 2021)		**Exploitatiekosten na afsluiting projectmatige aanpak**		
Projectmatige aanpak (2 jaar)		**2022**	**2023**	**2024**	**2025**	**2026**
	Inhuur CISO en Netwerkbeheerder (full time), structureel vanaf 2024	€400.000	€ 400.000	€ 220.000	€ 220.000	€ 220.000
	IEC 62443 invoeren en borgen	€246.500	€ 246.500	-	-	-
	Implementatie BIO incl. borging in de organisatie	€267.000	€ 200.000	-	-	-
Exploitatie op KA-securitygebied						
	Inhuur VKA-consultant 1 dag per week	-	-	€ 41.600	€ 41.600	€ 41.600
	Inhuur Functionaris Gegevensbescherming (per jaar)	-	-	€ 9.500	€ 9.500	€ 9.500
	Budget t.b.v. verbeterpunten die nog openstaan. Deze acties zijn structureel vertaald naar jaarplannen en worden opgepakt aan de hand van de toegekende prioriteit. Dit is een dynamische lijst van taken die alleen maar groeit door het toenemende aantal richtlijnen en normenkaders waaraan we moeten voldoen. Verder komen er uit elke audit en pentesten verbeterpunten die ook weer opgenomen worden in de jaarplannen	-	-	€ 80.000	€ 80.000	€ 80.000
Exploitatie op PA-securitygebied						
	Awareness programma	-	-	€ 4.500	€ 4.500	€ 4.500
	Beleid en procedures - controle CMDB, CSMS en 3 jaarlijkse audit (om de 3 jaar € 55.000 i.p.v. € 20.000)*)	-	-	€ 20.000	€ 20.000	€ 55.000
	Continuïteitsmanagement - Beheer disaster recovery	-	-	€ 10.000	€ 10.000	€ 10.000
	Techniek - Pentest en netwerkmonitoring	-	-	€ 80.000	€ 80.000	€ 80.000
	Extra uren beheer PA-omgeving (CroonWolter&Dros)	-	-	€ 102.000	€ 102.000	€ 102.000
Subtotaal		**€ 913.500**	**€ 846.500**	**€ 567.600**	**€ 567.600**	**€ 602.600**
Totaal		**€ 1.760.000**		-	-	-

*) Ieder 3de jaar komt er €35.000 op het exploitatiebudget extra voor het uitvoeren van benodigde audits.

Opmerkingen:

- De inhuur gedurende 2 jaar van de CISO en de Netwerkbeheerder worden vanaf 2024 en verder loonkosten (structureel);
- Het investeringskrediet gereserveerd in de MIP Sprint 2021 ter hoogte van € 1.160.000,- kan niet worden gebruikt aangezien voor deze projectmatige uitvoering een exploitatiebudget noodzakelijk is. De kosten voor de uitvoering zijn echter niet activeerbaar (getoetst bij de accountant) en zullen derhalve in de exploitatie opgenomen moeten worden.

Financiële samenvatting:

- Voor 2022 is het budget ter hoogte van € 913.500,- benodigd;
- Het bedrag ter hoogte van € 846.500,- wordt meegenomen in de begroting van 2023;
- De exploitatiekosten vanaf 2024 bedragen jaarlijks € 567.600,- (elk 3e jaar € 602.600,-);
- Vanaf 2024 bedragen de structurele (/loon-) kosten voor CISO en Netwerkbeheerder (incl. aanvullende IT-kosten) € 220.000,- per jaar. Deze zijn in de tabel op de vorige pagina reeds meegenomen.

Risico's:

Bij het niet toekennen van het exploitatiebudget onderkennen we de volgende risico's:

- Imagoschade bij negatieve publiciteit bij niet voldoen aan vigerende wet- en regelgeving m.b.t. BIO/AVG/ISO en sectorale afspraken (UvW) en verliezen ISO27001 certificaat;
- Inbreuk op informatiesystemen, waardoor niet beschikbaar zijn van ICT en mogelijk verlies van data, mogelijke cyberaanvallen (voorbeeld VDL).

N.B. De in dit voorstel beschreven aanpak wordt bevestigd in de externe audit, getiteld 'Waterschapsbedrijf Limburg - Auditrapport Integrale BIO/AVG audit', dd. 23 februari 2022, uitgevoerd door Verdonck, Klooster & Associates (VKA).

Bijlage

1. Bijlage 1 - Roadmap WBL- 03082021- V0.5.pdf.

De directeur, De voorzitter,

ing. E.M. Pelzer MMO drs. ing. P.F.C.W. van der Broeck

Vastgesteld door het Algemeen Bestuur d.d. ……

De directeur, De voorzitter,

ing. E.M. Pelzer MMO drs. ing. P.F.C.W. van der Broeck