Uitvoeringsplan Informatiebeveiliging 2024 - 2025 SSC DeSom.

DeSom: Uitvoeringsplan informatiebeveiliging 2023	Risicoprofiel: middel	DOC-23-753472

Doelstelling GR

Het belang van deze regeling is het bewerkstelligen van een kwalitatief hoogwaardige en een doelmatige uitvoering door het SSC van de door de gemeenten opgedragen uitvoerende taken en de ondersteuning in brede zin op het terrein van de ICT en het creëren van de voorwaarden voor een efficiënte bedrijfsvoering en een efficiënte en klantgerichte dienstverlening.

Voorstel zienswijze raad

- Een positieve zienswijze af te geven onder de voorwaarde dat Bedrijfscontinuïteit Management (BCM) onderdeel wordt van het Uitvoeringsplan Informatiebeveiliging 2024-2025 van SSC DeSom.

Argumenten

- Het Uitvoeringsplan Informatiebeveiliging van DeSom bevat een pakket aan technische maatregelen welke de kans en impact van een cyberincident verlagen. Hiermee wordt de (technische) informatieveiligheid van onze informatievoorziening verbeterd;

- Het geeft ook technische invulling aan de bevindingen vanuit het rekenkameronderzoek naar de staat van informatieveiligheid binnen gemeente Medemblik van 29 september 2022 (agendapunt C.4)[1].

Algemene bevindingen

Samen met SSC DeSom is op een constructieve en positieve wijze een pakket aan technische maatregelen samengesteld. Deze technische maatregelen bevorderen de (technische) informatieveiligheid van onze informatievoorziening. De kans en impact van cyberincidenten worden hiermee verlaagd. De bedrijfsvoering, de dienstverlening aan onze inwoners en de gegevens van onze inwoners worden hiermee beter beschermd.

Als gevolg van de onzekere uitkomst van het traject “Stip op de Horizon” is gekozen om de belangrijkste technische maatregelen voor 2024 en 2025 op te nemen in de eerste tranche. De komende jaren worden meerdere tranches aangevraagd, afhankelijk van de uitkomst van het traject “Stip op de Horizon”. Op dit moment is nog niet bekend welke impact dit heeft. Deze extra tranches zullen op basis van risico management worden samengesteld.

SSC DeSom heeft het Uitvoeringsplan Informatiebeveiliging onderbouwd op basis van nieuwe Europese regelgeving, de NIS2-directive. Op het moment van schrijven is nog veel onduidelijk over de werkelijke impact van deze nieuwe wetgeving in Nederland. Deze onderbouwing is onhandig van SSC DeSom.

Het pakket aan technische maatregelen bestaat uit basismaatregelen op het gebied van informatieveiligheid. Hiermee wordt het basisniveau van informatieveiligheid verbeterd waarmee de kans en impact van een cyberincident wordt verlaagd. Hiermee wordt de (technische)

[1] https://medemblik.bestuurlijkeinformatie.nl/Agenda/Index/e940e245-f6c3-4e27-8e8b-2c28039c2358

informatieveiligheid van onze informatievoorziening verbeterd. Om deze reden zijn de technische maatregelen, los van de NIS2-directive, nodig.

Het risico op een cyberincident wordt nooit nul. Het voorbereiden hierop is daarom van essentieel belang middels Bedrijfscontinuïteit Management (BCM). Gemeente Medemblik maakt hier, samen met DeSom-gemeenten en Werksaam WF stappen in om dit samen met SSC DeSom vorm te geven. Het onderwerp Bedrijfscontinuïteit Management is niet opgenomen in het Uitvoeringsplan Informatiebeveiliging 2024-2025 van SSC DeSom, naar onze mening had dit wel gemoeten.

Financiële consequenties

Van gemeente Medemblik wordt in 2024 een extra bijdrage van € 39.000,-- gevraagd. Als gevolg van de structurele financiële aframing daalt de bijdrage voor 2024 met € 8.000,--.

De overall financiële consequenties voor de begroting 2024 tot en met 2028 van SSC DeSom worden weergegeven op p.2 van Uitvoeringsplan Informatiebeveiliging 2024-2025.
Samengevat:

onderdeel	krediet	2024	2025	2026	2027	2028
1. processen, meten en sturen		121.000	48.000	48.000	48.000	48.000
2. segmentering	84.500		20.300	19.600	18.900	18.200
3. ict en basisvoorzieningen	242.000		58.100	56.200	54.300	52.400
overige structurele kosten			181.500	181.500	181.500	181.500
totaal		**121.000**	**307.900**	**305.300**	**302.700**	**300.100**

Het Uitvoeringsplan Informatiebeveiliging 2024-2025 heeft geen financiële consequenties in 2023. Voor 2024 worden in het Uitvoeringsplan Informatiebeveiliging 2024-2025 totaal € 121.000,-- aan extra financiële middelen gevraagd. De extra financiële middelen voor 2025 en verder worden opgenomen in de begrotingen van SSC DeSom en worden in de reguliere P&C-cyclus aan u voorgelegd.

De financiële gevolgen van het Uitvoeringsplan Informatiebeveiliging 2024-2025 zijn door DeSom in kaart gebracht. Deze bestaan uit incidentele en structurele budgetten en twee kredieten die leiden tot afschrijvingslasten. Op basis van het Besluit begroting en verantwoording provincies en gemeente (BBV) en het Activabeleid van DeSom is bepaald welke kosten wel/niet voor activering (krediet) in aanmerking komen. Deze afweging is bepalend voor het (meerjarig) financieel effect op de begroting van DeSom, en dus op de deelnemersbijdrage. Wij hebben onvoldoende inzicht gekregen in de aard van de kosten om de financiële vertaling van DeSom te kunnen toetsen.

Risico's

- Het niet investeren in dit pakket aan technische maatregelen zal leiden tot achterstanden in de modernisering van de techniek. De kans op een cyberincident zal hierdoor toenemen. Met als mogelijks gevolg dat de gemeentelijke bedrijfsvoering en dienstverlening ernstig worden verstoord en gegevens van onze inwoners op straat komen te liggen.

- In het pakket van de technische maatregelen zijn ook verdiepende adviesvragen opgenomen. Deze zullen mogelijk leiden tot extra investeringsaanvragen;

- Het technische pakket aan maatregelen is, naast de verdiepende adviesvragen, nog niet volledig. In de toekomst is het mogelijk dat extra investeringen nodig zijn;

- Het pakket van technische maatregelen draagt bij aan een verlaging van de kans en impact van een cyberincident. Het risico wordt echter nooit nul. Het blijven door ontwikkelen en

investeren, in de breedste zin van het woord, in informatieveiligheid is van belang. Ook het voorbereiden op cyberincident is van belang zodat herstelmaatregelen vooraf geformuleerd kunnen worden om de bedrijfsvoering en dienstverlening zo snel mogelijk weer te herstellen.