GEMEENTE MIDDEN-DRENTHE

Postadres	Postbus 24, 9410 AA Beilen
Telefoon	(0593) 53 92 22
Internet	www.middendrenthe.nl
E-mail	gemeente@middendrenthe.nl

Bezoekadres

Beilen	Raadhuisplein 1	
	ma, wo, vr	8.30 – 16.30
	di	8.30 – 14.30
	do	8.30 – 20.00
Smilde	Elzenlaan 10	
	ma	8.30 – 12.00

Aan de raads- en commissieleden
van de gemeente Midden-Drenthe

Datum: 19 mei 2020
Behandeld door: Jacobus Koops
Zaaknummer: 1459976
Onderwerp: Verantwoording DigiD en Suwinet ENSIA 2019

Bijlagen:

Geachte raads- en commissieleden,

Met de bijgevoegde college- en assuranceverklaringen informeren wij u over de status van de informatieveiligheid voor het onderdeel Suwinet en DigiD. Wij zijn verantwoordelijk voor de informatieveiligheid. Vanuit deze verantwoordelijkheid leggen wij, door middel van deze verklaringen, verantwoording af over de kwaliteit- en veiligheid van onze informatievoorziening voor de onderdelen Suwinet en DIGID.

De wijze waarop de verantwoording plaats vindt is op basis van de Eenduidige Normatiek Single Information Audit (voortaan ENSIA genoemd). In deze brief wordt kort toegelicht wat de ENSIA is, hoe de verantwoording eruit ziet, op welke wijze dit proces in 2018 is doorlopen en wat de resultaten hiervan zijn.

Wat is de ENSIA?
ENSIA is een initiatief van de VNG en de ministeries Binnenlandse Zaken en Koninkrijksrelaties, Infrastructuur en Milieu en Sociale Zaken en Werkgelegenheid.
ENSIA is een integrale audit waarbij een aantal audits en zelfcontroles op het terrein van informatievoorziening en –beveiliging gebundeld zijn.
De ENSIA bestaat uit de volgende onderdelen: BAG (Basisadministratie Adressen en Gebouwen), BGT (Basiskaart Grootschalige Topografie), BRP (BasisRegistratie Personen), PUN (PaspoortUitvoeringsregeling Nederland), Suwinet (Inkijksservice Sociaal domein) en DigiD (Digitale Identiteit). Het doel is dat de ENSIA door het toezicht te bundelen zorgt voor een verdere professionalisering van het verantwoordingsproces rondom de informatievoorziening. Daarbij is ook de insteek dat met de bundeling de auditdruk op gemeenten acceptabel blijft.

Verantwoording
In het kader van de ENSIA vindt de verantwoording over de informatieveiligheid plaats langs twee wegen. Allereerst wordt er verticaal verantwoording afgelegd aan de diverse ministeries. Dit gebeurt op basis van de uitgevoerde zelfevaluaties. Tevens legt het college horizontaal verantwoording af aan de raad. Hiervoor wordt aansluiting gezocht bij de reguliere Planning & Control-cyclus van de gemeente. Dat betekent dat in de jaarrekening verantwoording wordt afgelegd over de kwaliteit en veiligheid van de informatievoorziening. Deze verantwoording is opgenomen in de paragraaf bedrijfsvoering in de jaarstukken.

Aanvullend op de verantwoording via de jaarrekening is er over 2019 specifiek verantwoording vereist over een tweetal onderdelen, te weten DigiD en Suwinet. Dit gebeurt nu door de college- en assurance verklaringen over deze twee onderdelen ter informatie aan te bieden aan de raad. Met het assurance rapport wordt door een onafhankelijke geregistreerde IT-auditor onze verklaring onderschreven.

Resultaten DigiD
Zes normen voldoen niet voor het gedeelte DigiD het gaat om de volgende normen;

- Toegang tot beheermechanismen
- Hardening van platformen
- Protectie- en detectiemechanismen
- Vulnerability-assessments
- Penetratietesten
- Signaleringsfuncties

Resultaten Suwinet
Vijf van de normen voldoen niet voor het gedeelte Suwinet het gaat om de volgende normen;

- Beveiligingsfunctie Suwinet
- Taken, verantwoordelijkheden en functiescheiding
- Toegangsmechanisme: Gebruikersidentificatie- en authenticatie
- Evaluatie op aansluitbeleid
- Beoordeling van toegangsrechten

Risico's
Extra risico hebben we hierdoor niet gelopen. Veel procedures worden wel gedaan. Het probleem zit hem in het vastleggen, rapporteren en evalueren wat niet consequent gebeurt i.v.m. capaciteit. De auditor kan dan niet vaststellen dat we volledig aan de norm voldoen. Daarnaast is de zelfevaluatie een groeimodel waarbij de auditor steeds strenger naar de naleving van de normen kijkt. We zijn dit jaar niet meegegroeid maar op het niveau van vorig jaar blijven hangen.

Toelichting op de resultaten
We zijn wel geschrokken door de tegenvallende resultaten in vergelijking met andere jaren. We hebben eerder geconstateerd dat we te weinig investeren in ICT dat wordt nu weer bevestigd. We zijn daarom onmiddellijk gestart met een herstelplan.

Herstelplan
Tijdens de zelfevaluaties is vooral gebleken dat er niet voldoende capaciteit is om de procedures rondom informatiebeveiliging consequent uit te voeren en dit ook te monitoren. We hebben daarvoor de volgende maatregelen genomen;

Over de auditperiode heeft onze medewerker informatiebeveiliging (CISO) te weinig tijd gehad in verband met andere verantwoordelijkheden. We zorgen ervoor dat er voor deze medewerker voldoende tijd beschikbaar is om zijn rol goed te kunnen uitvoeren.
We hebben inmiddels een externe FG (Functionaris Gegevensbescherming) aangesteld om deze medewerker te ondersteunen en te ontlasten. De rol van FG en CISO in één medewerker is praktisch onuitvoerbaar en niet wenselijk.
Om de technische procedures rondom informatiebeveiliging consequent te kunnen uitvoeren gaan we capaciteit vrijmaken bij systeembeheer.
Er zal gemonitord moeten worden door de CISO of de procedures consequent worden uitgevoerd, hiervoor is software aangeschaft.
Daarnaast hebben we extern ingehuurd om de implementatie van deze software te ondersteunen.

Deze maatregelen gelden voor alle processen rondom informatiebeveiliging dus ook voor bovenstaande normen DigiD en Suwinet.

Onze huidige auditor gaat de voortgang van het herstelplan monitoren en eventueel bijsturen waar nodig.

Voor de komende jaren gaan we meer middelen beschikbaar maken voor ICT en Informatiebeveiliging.

Informatie
Voor meer informatie kunt u contact opnemen met Jacobus Koops, medewerker zaaksysteem/informatiebeveiliging, te bereiken op via telefoonnummer (0593) 53 92 36.

Met vriendelijke groet,
burgemeester en wethouders van Midden-Drenthe,

de secretaris, de burgemeester.