Rapportage Informatiebeveiliging Deurne 2017

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeente om hun processen uit te voeren. Gemeenten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven en daarnaast zijn zij verantwoordelijk voor een betrouwbare en continue dienstverlening. Het is daarom belangrijk gemeenten op passende wijze hun informatie beveiligen.
Het begrip 'informatiebeveiliging' heeft betrekking op beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van gegevens. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Gemeenten dienen bij hun informatiebeveiliging te voldoen aan wet- en regelgeving, zoals bijvoorbeeld voor privacy.
Met deze rapportage Informatiebeveiliging Deurne 2017 verantwoordt het college van de gemeente Deurne zich richting gemeenteraad over de status van informatiebeveiliging over 2017.

De gemeente dient jaarlijks verantwoording af te leggen over informatieveiligheid. Voorheen waren er aparte verantwoordingsprocedures voor de volgende registratiesystemen en systemen met privacygevoelige informatie:

- Basisregistratie Personen (BRP).
- Paspoort en Nederlandse Identiteitskaart (PNIK).
- Digitale persoonsidentificatie (DigiD).
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).
- Basisregistratie Adressen en Gebouwen (BAG).
- Basisregistratie Grootschalige Topografie (BGT).

Deze verantwoordingsprocedures bestaan nog steeds. Echter, sinds 2017 verantwoordt de gemeente zich ten aanzien van het informatiebeveiligingsgedeelte voor het eerst met behulp van een nieuwe systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid en is verplicht voor alle gemeenten. Met ENSIA leggen gemeenten in één keer verantwoording af aan toezichthouders over de informatiebeveiliging van bovenstaande systemen en over informatiebeveiligingsnormen, waaraan alle Nederlandse gemeenten zich dienen te houden (verticale verantwoording). Daarnaast dient het college zich voortaan ook naar de gemeenteraad toe te verantwoorden over informatiebeveiliging (horizontale verantwoording).
Deze systematiek maakt de stand van zaken rondom informatieveiligheid meer inzichtelijk.

In deze rapportage gaat het college verder in op:
1. Het informatiebeveiligingsbeleid en doelstellingen.
2. Uitgevoerde acties in 2017.
3. Resultaat informatiebeveiliging over 2017 en vervolgstappen
    a. per registratiesysteem;
    b. gemeentebreed.
4. Beveiligingsincidenten (privacy-datalekken).
5. Het meerjarenperspectief.

1. Informatiebeveiligingsbeleid en doelstellingen

Informatiebeveiligingsbeleid
Een vastgestelde informatiebeveiligingsbeleid is het uitgangspunt voor de inrichting en borging van informatiebeveiliging in de gemeente. In 2013 is tijdens de Buitengewone Algemene Ledenvergadering van de VNG besloten dat iedere gemeente de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt voor haar informatiebeveiligingsbeleid hanteert. De BIG voldoet aan de internationaal geaccepteerde beveiligingsstandaarden ISO 27001/27002 en bevat een normenkader met beveiligingsmaatregelen die een goed basis-beveiligingsniveau voor gemeenten neerlegt.

In 2014 is het informatiebeveiligingsbeleid voor de gemeente Deurne vastgesteld. Het informatiebeveiligingsbeleid hanteert de BIG als uitgangspunt en is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving. Het beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid.

De informatiebeveiligingsbeleid gaat conform de BIG in op de volgende gebieden:

- Beveiligingsbeleid.
- Organisatie van de informatiebeveiliging.
- Beheer van bedrijfsmiddelen.
- Personele beveiliging.
- Fysieke beveiliging en beveiliging van de omgeving.
- Beheer van communicatie- en bedieningsprocessen.
- Toegangsbeveiliging.
- Verwerving, ontwikkeling en onderhoud van Informatiesystemen.
- Beheer van informatiebeveiligingsincidenten.
- Bedrijfscontinuïteitsbeheer.
- Naleving.

In het beleid staan concrete doelstellingen op gebied van organisatorische, technische en fysieke beveiliging. Deze doelstellingen worden in een beveiligingsplan verder uitgewerkt. In 2018 beoordeelt de gemeente het beleid opnieuw en stel zij dit opnieuw vast.

Doelstellingen
De gemeente Deurne stelt als doel om op het gebied van informatiebeveiliging “in control” te zijn en legt daarover jaarlijks verantwoording af. In control betekent in dit verband dat:

- de gemeente weet welke maatregelen genomen zijn;
- er een specifieke planning is van de maatregelen die nog niet genomen zijn;
- dit geheel verankerd is in de Plan Do Check Act-cyclus.

De gemeente prioriteert op basis van risicoanalyse welke maatregelen (eerst) getroffen moeten worden en hanteert hierbij het ‘pas toe of leg uit’ principe.

2. Uitgevoerde acties in 2017

Informatiebeveiligings- & privacy-functionaris aangesteld
Om stappen te zetten op het gebied van informatiebeveiliging heeft de gemeente in 2017 een Chief Information Security Officer (CISO) benoemd. Deze functionaris zorgt voor een samenhangend pakket van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de gemeente te waarborgen. Daarnaast is in 2017 ter ondersteuning van de Functionaris Gegevensbescherming een Privacy Officer aangesteld die zorgt voor borging van privacy in de organisatie.

AVG & ENSIA
Naar aanleiding van Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 door de Autoriteit Persoonsgegevens gehandhaafd wordt, en de komst van ENSIA is de gemeente eind 2017 gestart om zowel privacy-activiteiten als informatiebeveiliging projectmatig op een hoger niveau te brengen en daarna structureel te borgen in de organisatie.

3. Resultaat over 2017 en vervolgstappen

Zoals eerder vermeld, dient de gemeente zich te verantwoorden over BRP, PUN, DigiD, Suwinet, BAG, en BGT. Dit vindt plaats door een zelfevaluatie (BRP, PNIK, BAG en BGT) of door een audit (DigiD en Suwinet). Verder toetst de gemeente haar informatieveiligheid in algemene zin via een zelfevaluatie (BIG).

De resultaten en de vervolgstappen hiervan zien er als volgt uit:

Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteitskaart (PNIK)
Uit de uitgevoerde zelfevaluatie heeft de gemeente Deurne voor BRP een score behaald van 85,2% en voor PNIK 87,7%. De norm voor beide is 90%.
De lagere score voor BRP en PNIK is een landelijke trend. Dit wordt veroorzaakt doordat vragen die in voorgaande jaren specifiek op dit domein te beantwoorden waren, nu ineens als gemeentebrede norm gelden. Nog niet al deze normen zijn gemeentebreed al doorgevoerd. Dit betekent dat meer vragen een negatieve score opleveren. De VNG geeft aan dat voor 2018 de ENSIA-vragen beter op BRP en PNIK zullen worden afgesteld, waardoor scores voor BRP en PNIK een betere afspiegeling zijn van de werkelijke status.

Gaat alles dan al goed? Nee, er is altijd ruimte voor verbetering. De verbeteracties voor dit domein zijn opgenomen in "actieplan basisregistratie Personen en reisdocumenten 2018" en maken onderdeel uit van de focuslijst 2018-2019 (zie volgende pagina). Het merendeel van de acties wordt nog in 2018 uitgevoerd.

Digitale persoonsidentificatie (DigiD) en Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
DigiD staat voor Digitale identiteit waarmee de burger kan inloggen op de websites van de overheid en in de zorg. Begin 2017 heeft Deurne voor DigiD een nieuwe aansluiting geactiveerd. Na deze activering heeft de gemeente zich al moeten verantwoorden over de aansluiting. Het was daarom niet nodig een voor 2017 een (hernieuwde, externe) audit uit te voeren.

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen.
Voor Suwinet heeft een externe auditor geconstateerd dat gemeente Deurne en daarbij horend Senzer (gemeenschappelijke regeling die de Participatiewet uitvoert voor o.a. Deurne) niet voldoen aan 10 van de 12 gestelde normen. Dit wordt veroorzaakt door het ontbreken van een informatiebeveiligingsbeleid specifiek voor Suwinet. Hierop is direct actie ondernomen en Senzer geeft aan dat deze per 1-10-2018 is opgesteld. Deurne adviseert in dit traject en ziet toe op tijdige oplevering en uitvoering van het beleid.

Het college dient over de audits van DigiD en Suwinet formeel een collegeverklaring af te leggen aan de gemeenteraad en toezichthouders. Daarom is deze collegeverklaring integraal opgenomen aan het einde van de rapportage.

Basisregistratie Adressen en Gebouwen (BAG)
BAG (Basisregistratie Adressen en Gebouwen) is onderdeel van het stelsel van basisregistraties in Nederland. Gemeenten zijn bronhouders van de BAG. Dat betekent dat de gemeente verantwoordelijk is voor het beheer en de kwaliteit van de gegevens van de adressen en gebouwen binnen de gemeentegrenzen.

Deurne heeft met een zelfevaluatie de borging van de processen, tijdigheid, volledigheid en juistheid getoetst. Zij heeft op de vragenlijst 200 punten gescoord, op een totaalscore van 200 punten. Dit is dus een 100% score. Vanuit het ministerie is de 'lat' gesteld op 75% van de totaalscore.

Basisregistratie Grootschalige Topografie (BGT)
Basisregistratie Grootschalige Topografie (BGT) is een gedetailleerde digitale kaart van heel Nederland. Daarin staan onder andere gebouwen, wegen, water, spoorlijnen en groen. Door de gegevens in de BGT eenduidig op te slaan, zijn ze herbruikbaar voor alle overheidsorganisaties die deze gegevens nodig hebben. Gemeenten zijn bronhouder van deze basisregistratie en moeten er dus voor zorgen dat de gegevens van de BGT kloppen.

Ook voor de BGT heeft Deurne een zelfevaluatie gedaan op het gebied van borging processen, tijdigheid, volledigheid en juistheid. De gemeente Deurne heeft op de vragenlijst 130 punten gescoord, op een totaalscore van 150 punten. Dit komt neer op een scoringspercentage van 86,6%. Vanuit het ministerie is de 'lat' gesteld op 75% van de totaalscore. Een goede score met ruimte voor verbetering. Hiertoe wordt het delegatie- en mandaatbesluit aangepast en het proces van uitwisseling van informatie met de BAG en Beheer Openbare Ruimte (BOR) verbeterd.

Informatieveiligheid gemeentebreed
Informatiebeveiliging is van belang voor meer dan alleen de voorgaande specifieke registraties en systemen. Dit geldt ook voor andere processen in de gemeente, vandaar dat binnen ENSIA ook gemeentebreed met een

zelfevaluatie getoetst wordt of de gemeente voldoet aan de normen uit de Baseline Informatiebeveiliging Gemeenten (BIG).

De conclusie uit de zelfevaluatie is dat Deurne eind 2017 nog niet volledig voldoet aan haar eigen informatiebeveiligingsbeleid.

Welke stappen zijn er het laatste jaar gezet?
Eind 2017 heeft het college besloten om Privacy en Informatieveiligheid eerst projectmatig op een hoger niveau te brengen en vervolgens om het structureel te borgen in de organisatie. Dit heeft tot onderstaande resultaten geleid:

- Het laatste half jaar is de bezetting van coördinerende functies op orde
- Er is groeiende aandacht voor en betrokkenheid bij het onderwerp bij medewerkers, MT en B&W
- Beheer van de basisregistraties is goed op orde
- Risico-analyse heeft plaatsgevonden op basis van de ENSIA zelfevaluatie 2017. Hieruit komt een lijst met mogelijke verbeterpunten
- Er is een werkgroep gestart met een twintigtal betrokken medewerkers uit alle geledingen van de organisatie. Zij kijken samen naar verbetermogelijkheden en werken aan betrokkenheid bij het thema

Focus maatregelen 2018-2019
De verbeterpunten op basis van de risico-analyse kunnen niet allemaal gelijktijdig worden opgelost. De komende periode ligt de focus op onderstaande punten:

1. Rollen en verantwoordelijkheden ten aanzien van Informatieveiligheid duiden en vastleggen
2. Bewustwording; kennis verhogen, houding en gedrag van medewerkers verbeteren
3. Autorisatiemanagement (wie mag wat waarin?) aanscherpen
4. Proces veranderingen in ICT-omgeving beter borgen
5. Proces afhandelen ICT-incidenten transparanter maken
6. Bedrijfscontinuïteit; noodscenario's en uitwijkplannen aanscherpen
7. Systeem- en netwerkbeveiliging doorontwikkelen
8. Borging van acties in PDCA-cyclus

Volgend jaar komt er een nieuwe lijst met focuspunten op basis van de ENSIA zelfevaluatie 2018.

4. Beveiligingsincidenten (privacy-datalekken) 2017

Gepubliceerde vergunningen met persoonsgegevens
In 2017 heeft de gemeente een incident geconstateerd waarbij sprake is van een datalek. Hierbij zijn ongewenst en onbedoeld bepaalde persoonsgegevens gepubliceerd. De gemeente heeft het datalek gemeld aan de Autoriteit Persoonsgegevens. De gemeente heeft van de leverancier geëist de software aan te passen. Daarnaast vindt in het proces extra visuele controle plaats op onbedoelde publicatie van persoonsgegevens.

Laptop gestolen
In 2017 is een laptop van een medewerker gestolen. De gegevens op de laptop waren versleuteld, waardoor onbevoegden geen mogelijkheid hebben gehad om gevoelige gegevens te achterhalen. Het incident is wel gemeld bij de Autoriteit Persoonsgegevens.

5. Meerjarenperspectief

De gemeente richt zich de komende jaren op het structureel verbeteren en borgen van informatieveiligheid in de organisatie. De coördinerende rol hiervoor ligt bij de CISO, de doorgevoerde maatregelen worden geborgd in de betreffende vakafdeling. De basis hiervoor vormen de BIG-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA). Op basis van risico, impact en beschikbare capaciteit en middelen worden maatregelen ingepland over meerdere jaren. Daar waar mogelijk of noodzakelijk worden maatregelen in 2018 al getroffen. Om efficiënt met middelen en capaciteit om te gaan wordt zoveel mogelijk aangesloten bij lopende projecten. Ieder jaar wordt een overzicht van genomen maatregelen en nog te nemen maatregelen meegenomen in het verantwoordingsproces.

Tot slot

Bij informatie is het van belang dat deze op een passende wijze wordt beveiligd. Zoals in de inleiding gesteld: hoe waardevoller en gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. 100% beveiliging bestaat echter niet; dagelijks worden er nieuwe kwetsbaarheden ontdekt in software, maken mensen regelmatig bewust of onbewust fouten in hun handelen of ontwikkelen criminelen nieuwe manieren om in te breken. Bedreigingen en risico's blijven zich door ontwikkelen, te treffen beveiligingsmaatregelen worden daarop continu aangepast. Daarnaast is het belangrijk dat de werkomgeving voor de medewerkers van de gemeente Deurne ook werkbaar blijft, zowel fysiek als digitaal. Je plaatst immers niet 10 sloten op de voordeur.

Kortom: bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen en werkbaarheid. Het is hierbij van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen maatregelen. Deze transparantie, dáár zorgt ENSIA voor.

Collegeverklaring ENSIA over informatiebeveiliging DigiD en SUWInet

Hier vindt u de collegeverklaring van de gemeente Deurne over DigiD en Suwinet. Een onafhankelijke auditor heeft deze verklaring getoetst.

Gemeente Deurne

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet
Ons kenmerk: (00635716)

Het college van burgemeester en wethouders van de gemeente Deurne legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om de verantwoording over Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet) te bundelen in één systematiek dat onder meer uitgaat van de Baseline Informatiebeveiliging Gemeenten (BIG). Naast deze verklaring is de zelfevaluatie van de BIG eveneens een onderdeel van de ENSIA systematiek.
ENSIA sluit aan op de gemeentelijke planning en control cyclus voor informatiebeveiliging. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Uitvoering
Voor de uitvoering van Suwinet geldt het volgende. Onder verantwoordelijkheid van de gemeente is de uitvoering van de regelingen op het gebied van werk en inkomen uitbesteed aan de Gemeenschappelijke Regeling (GR) Atlant de Peel (Senzer). Om de werkwijze van Senzer te beoordelen is een TPM (Third Party Memorandum) opgesteld door een externe auditor. De conclusies uit dit TPM zijn mede verwerkt in deze verklaring.

Reikwijdte verklaring
Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit Suwinet, voor wat betreft DigiD hebben we vastgesteld dat er geen via de ENSIA verantwoordingsmethodiek te verantwoorden aansluiting is. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01). De normen staan op het openbare deel van de websites van het ministerie van BZK en het BKWI. De verklaring omvat niet de werking van de maatregelen over 2017.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen (SZW) die toezien op de veiligheid van Suwinet. De departementen en de gemeenteraad die toezien op de veiligheid van Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor Suwinet geïnformeerd over de afwijkingen van de normen.

25-04-2018

BKBO
Voorstraat 20
5251 CP Vl
M 06-28

Verklaring college

Het college verklaart dat bij gemeente Deurne op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan 2 van de 12 geselecteerde normen inzake Suwinet, met uitzondering van de hierna vermelde normen:

B.01, B.04, B.05, C.01, C.04 C.05, C.06, C.07, U.02 en U.11.
De met de uitzonderingen samenhangende beoogde (aanvullende) beheersmaatregelen ten aanzien van Senzer zijn in verbeterplannen opgenomen. De door de auditor geadviseerde verbetermaatregelen ten aanzien van de gemeente worden tussen 1 mei en 1 oktober 2018 opgepakt en uitgevoerd.

Deurne, 24 april 2018

burgemeester en wethouders van Deurne

R.B.M. Halffman
gemeentesecretaris

H.J. Mak
burgemeester

25-04-2018

BKBO
Voorstraat 20
5251 CP VLIJMEN
M 06-28978955