Rapportage Informatiebeveiliging Eemsmond 2017

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten 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 dat 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 Eemsmond 2017 verantwoordt het college van de gemeente Eemsmond zich aan de 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 vastgesteld 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 2017 is het informatiebeveiligingsbeleid voor de gemeente Eemsmond 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.

Het 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 het gebied van organisatorische, technische en fysieke beveiliging. Deze doelstellingen worden in beveiligingsplannen verder uitgewerkt. In 2018 wordt een informatiebeveiligingsbeleid voor Het Hogeland opgezet en stellen de gemeenten dit vast.

Doelstellingen
De gemeente Eemsmond 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 samen met de BMWE-gemeenten 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 hebben de BMWE-gemeenten in 2017 een Chief Information Security Officer (CISO) en een medewerker informatiebeveiliging benoemd. Deze functionarissen zorgen voor een samenhangend pakket van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de gemeenten Bedum, De Marne, Winsum en Eemsmond te waarborgen. Daarnaast is in 2017 voor de BMWE-gemeenten een Functionaris Gegevensbescherming/Privacy Officer aangesteld die zorg draagt dat de gemeente privacy borgt in de organisatie.

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

iBewustzijn
In 2017 is BMWE-breed een informatiebeveiligingsbewustzijnsplan voor medewerkers opgesteld. De gemeenten Bedum, De Marne en Winsum hebben in 2017 een nulmeting uit laten voeren waarbij de kennis en het gedrag van medewerkers is gemeten ten aanzien van informatiebeveiliging. Daarnaast zijn voor deze gemeenten in 2018 workshops gehouden. Gemeente Eemsmond heeft dit traject in 2016 al doorlopen, maar sluit in 2018 aan bij online cursussen op het gebied van informatiebeveiliging. Deze en andere

bewustzijnsacties hebben tot doel de kennis en de houding van medewerkers ten aanzien van informatiebeveiliging te verbeteren.

3. Resultaat over 2017 en vervolgstappen

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

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

Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteitskaart (PNIK)
Bij deze zelfevaluaties ligt de focus op kwaliteit en daarmee integriteit (juistheid, volledigheid) van informatie en op de vertrouwelijkheid van de informatie. Uit de uitgevoerde zelfevaluatie heeft de gemeente Eemsmond voor BRP een score behaald van 92,6% en voor PNIK 90,5%. De norm voor beide is 90%.

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. De focus ligt hier op de beveiliging van het DigiD-systeem waarmee vertrouwelijkheid gewaarborgd wordt. Begin 2017 heeft Eemsmond voor DigiD een nieuwe aansluiting geactiveerd. Na deze activering heeft de gemeente zich al moeten verantwoorden over de aansluiting. De gemeente hoeft zich niet nogmaals over 2017 te verantwoorden en een hernieuwde, externe audit is daarom niet benodigd.

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De focus ligt hier op de vertrouwelijkheid van persoonsgegevens. Voor Suwinet heeft een auditor geconstateerd dat gemeente Eemsmond en daarbij horend Werkplein Ability (gemeenschappelijke regeling die de Participatiewet uitvoert voor BMWE-gemeenten) voldoen aan de gestelde normen.

Zoals beschreven voldoen de gemeenten aan de gestelde normen, echter heeft de auditor wel aanbevelingen beschreven in de assurance-rapportage. Deze aanbevelingen worden door de gemeenten opgepakt samen met de acties richting Het Hogeland.

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)
Basisregistratie Adressen en Gebouwen (BAG) 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. De focus ligt hier op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.
Eemsmond heeft met een zelfevaluatie de borging van de processen, tijdigheid, volledigheid en juistheid getoetst. Over 2017 is het optioneel om als gemeente verantwoording af te leggen richting de toezichthouder het Ministerie van Infrastructuur en Waterstaat. De gemeente heeft ervoor gekozen wel de zelfevaluatie uit te voeren, maar heeft zich niet verantwoord richting de toezichthouder. Vanaf 2018 is verantwoording verplicht. Zij heeft op de vragenlijst 120 punten gescoord, op een totaalscore van 200 punten. Dit is dus een 60% score. Vanuit het ministerie is de ‘lat’ gesteld op 75% van de totaalscore. Verbeteracties zijn deels getroffen. Daarnaast worden verbeteracties uitgevoerd met het samengaan met de andere gemeenten.
Het niet halen van de norm heeft vooral te maken met de overgang van de samenwerking in DEAL verband naar het op de markt zetten van de werkzaamheden naar VGI-support. Aan de zijde van Eemsmond was en is geen BAG-beheerder of BAG-medewerker aanwezig. Voor het jaar 2018 worden de tekortkomingen binnen BMWE-verband opgelost. Een belangrijke verbetermaatregel is de ‘oprichting’ van het gegevenshuis voor de nieuw te vormen gemeente Het Hogeland.

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 hier ligt de focus dus op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.
Ook voor de BGT heeft Eemsmond een zelfevaluatie uitgevoerd op het gebied van borging van processen, tijdigheid, volledigheid en juistheid. Over 2017 is het optioneel om als gemeente verantwoording af te leggen richting de toezichthouder Ministerie van Infrastructuur en Waterstaat. De gemeente heeft ervoor gekozen wel de zelfevaluatie uit te voeren, maar zich niet te verantwoorden richting de toezichthouder. Vanaf 2018 is verantwoording verplicht.
De gemeente Eemsmond heeft op de vragenlijst 70 punten gescoord, op een totaalscore van 150 punten. Dit komt neer op een scoringspercentage van 47%. Vanuit het ministerie is de 'lat' gesteld op 75% van de totaalscore. Verbeteracties zijn deels getroffen. Daarnaast worden verbeteracties uitgevoerd met het samengaan met de andere gemeenten.
Ook hierbij speelt de overgang van DEAL naar VGI-support een grote rol in het niet halen van de norm. In dit geval ontbreekt vooral de live-koppeling tussen het beheersysteem en de BGT-registratie. Door het ontbreken van deze koppeling en het ontbreken van een verantwoordelijke applicatiebeheerder van het beheersysteem worden wijzigingen door werkzaamheden niet verwerkt in de BGT. Hierdoor zijn de onderdelen tijdigheid, volledigheid en juistheid zwaar onder druk komen te staan. Ook dit wordt in 2018 opgelost binnen het proces van het op te richten gegevenshuis.

Informatieveiligheid gemeentebreed - Baseline Informatiebeveiliging Gemeenten (BIG)
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 BIG.

De conclusie uit de zelfevaluatie is dat Eemsmond eind 2017 nog niet voldoet aan haar eigen informatiebeveiligingsbeleid, waar de BIG aan ten grondslag ligt.

Eemsmond scoort goed op het gebied van betrokkenheid van haar medewerkers ten aanzien van informatiebeveiliging. Op de volgende gebieden heeft de gemeente wel maatregelen getroffen, maar is een hoger volwassenheidsniveau nodig om te komen tot een voldoende basisniveau van informatieveiligheid:

- Governance, rollen en verantwoordelijkheden ten aanzien van informatieveiligheid
- Borging van beveiliging door middel van Plan-Do-Check-Act-cyclus
- Kennis, houding en gedrag ten aanzien van informatiebeveiliging
- Autorisatiemanagement
- Wijzigingsbeheer op IT-gebied
- Incidentenbeheer
- Fysieke beveiliging
- Bedrijfscontinuïteitsmanagement
- Systeem- en netwerkbeveiliging

Wat is er inmiddels gedaan?
In 2017 heeft de gemeente besloten om informatieveiligheid op een hoger niveau te brengen en om het vervolgens structureel te borgen in de organisatie. Hiervoor is in 2017 de Beveiligingscommissie Eemsmond opgericht. In deze commissie zitten medewerkers van verscheidene vakafdelingen. De Beveiligingscommissie heeft op gemeentelijk niveau de status inzichtelijk gemaakt betreffende de zelfevaluatie informatiebeveiliging (ENSIA). Tevens heeft de Beveiligingscommissie maatregelen benoemd ter verbetering van informatie-beveiliging.

Vanaf 1 januari 2018 is de Beveiligingscommissie overgegaan in de gemeenteoverschrijdende BMWE-Veiligheidscommissie. De commissie richt zich op het in kaart brengen van:

- De status van informatiebeveiliging.
- Benoemen van beveiligingsmaatregelen.
- Prioritering en planning van beveiligingsmaatregelen op basis van risicoanalyse.

De basis hiervoor zijn het informatiebeveiligingsbeleid, de BIG-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA). Zij houdt hierbij rekening met de transformatie naar Het Hogeland. Op basis van risicoanalyse en aansluitend bij de huidige veranderingen beslist de gemeente samen met de herindelingsgemeenten welke verbeteracties in 2018 worden uitgevoerd en welke acties pas na de herindeling worden uitgevoerd.

4. Beveiligingsincidenten (privacy-datalekken) 2017

In 2017 hebben drie bekende datalekken plaatsgevonden. Daarnaast heeft zich één fysiek incident voorgedaan.

Datalek Persoonsgegevens gepubliceerd in Staatscourant
In de bijlagen van 14 publicaties van verkeersbesluiten in de Staatscourant, staan de persoonsgegevens van de politiefunctionaris die advies hieromtrent heeft uitgebracht. De publicaties zijn verwijderd uit de Staatscourant. De betrokken politiefunctionaris is geïnformeerd.

Post gemeente Eemsmond
PostNL had verzuimd de post te bezorgen. Tussen de post zitten allerlei documenten met persoonsgegevens waaronder ook vele met bijzondere persoonsgegevens (bijv. gezondheidsgegevens). Er is adequaat gereageerd door een groep personen te clusteren om te onderzoeken of er sprake was van een datalek. Er is contact opgenomen met PostNL, intussen was de post al na bezorgd. Er is aan PostNL gevraagd of zij konden uitsluiten dat de post op een andere plek is geweest die niet onder hun toezicht viel. Dit konden ze garanderen waarna de gemeente de zaak heeft afgesloten.

Datalek verwijsindex jongeren
De 23 Groninger gemeenten hebben een samenwerkingsverband waarbinnen zij een lokale verwijsindex Zorg voor Jeugd hebben opgetuigd. Tot deze verwijsindex hebben peuterspeelzalen en kinderdagverblijven onterecht toegang tot persoonsgegevens gehad. Als maatregel is de toegang tot de verwijsindex beperkt tot de vastgestelde groep organisaties. Gemeente Eemsmond heeft naar aanleiding hiervan een melding van een datalek gedaan bij de Autoriteit Persoonsgegevens. Betrokkenen in de gemeente Eemsmond zijn hierover ingelicht en het datalek is conform de geldende wetgeving afgehandeld.

Bedreiging met bijl
Begin 2017 heeft een bezoeker gedreigd de glazen toegangsdeur achter de balie met een meegebrachte hakbijl in te slaan wanneer hij niet persoonlijk werd geholpen. De politie heeft de hakbijl in beslag genomen. Het incident is hiermee afgehandeld.

5. Meerjarenperspectief

De gemeente richt zich de komende jaren op het verbeteren en borgen van de informatieveiligheid door BIG-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA) in te richten, te ondersteunen en te bewaken. Op basis van risico, (lopende) projecten en beschikbare tijd en middelen worden maatregelen ingepland over meerdere jaren. Daar waar mogelijk en noodzakelijk worden maatregelen in 2018 al getroffen en wordt aangesloten bij de al in gang gezette veranderingen.

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 en dient ook niet nagestreefd te worden. De kosten van beveiliging moeten in verhouding zijn tot de risico's. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's.

Collegeverklaring ENSIA over informatiebeveiliging DigiD en SUWInet

Hier vindt u de collegeverklaring van de gemeente Eemsmond over DigiD en Suwinet. Een onafhankelijke auditor (BKBO) heeft deze verklaring getoetst.

gemeente EEMSMOND

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Eemsmond 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.

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 DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0 (de Norm v2.0) en 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 die toezien op de veiligheid van DigiD en Suwinet. De departementen en de gemeenteraad die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD en Suwinet geïnformeerd over de afwijkingen van de normen.

26-04-18

BK BO
BKBO
Voorstraat 20
5251 CP VLIJMEN
M 06-28978955

gemeente
EEMSMOND

Verklaring college

Het college verklaart dat bij gemeente Eemsmond op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Uithuizen, 24-04-2018

College van B en W Eemsmond

26-04-18

BKBO
Voorstraat 20
5251 CP VLIJMEN
M 06-28978955