ENSIA rapportage informatiebeveiliging & privacy 2019

1. Inleiding

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten eenvoudiger te maken. Uitgangspunt van ENSIA is *de single information audit*. Dit betekent dat we maar één keer per jaar een zelfevaluatie op het gebied van informatiebeveiliging uitvoeren. Diverse bewijsstukken moeten daarbij vastgelegd worden en er vindt gedeeltelijk controle plaats door een externe IT auditor. Deze informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting ministeries.

ENSIA richt zich op de volgende onderdelen:

1. Basisregistraties waar de gemeente bronhouder van is:
   - Basisregistratie Personen (BRP);
   - Basisregistratie Adressen en Gebouwen (BAG);
   - Basisregistratie Grootschalige Topografie (BGT);
   - Basisregistratie Ondergrond (BRO).

2. Kritische processen:
   - Suwinet;
   - Paspoorten, ID-kaarten en rijbewijzen;
   - DigiD (2 aansluitingen).

3. Baseline Informatiebeveiliging Gemeenten (BIG)

2. Aan wie leggen we verantwoording af?

Horizontaal:
- Gemeenteraad.

Verticaal:
- Ministerie van Sociale zaken (BKWI inzake Suwinet);
- Ministerie BZK (RviG inzake paspoorten, ID-kaarten en rijbewijzen);
- Ministerie BZK (Logius inzake DigiD-aansluitingen);
- Ministerie BZK (Inzake de BRP);
- Ministerie BZK (BAG, BGT en BRO).

3. Stappen in het verticale verantwoordingsproces

- Uitvoeren zelfevaluaties.
- Opstellen collegeverklaring: de collegeverklaring is opgesteld op basis van bevindingen uit onze zelfevaluatie op Suwinet en DigiD. Hierin verklaart het college dat de zelfevaluatie naar eer en geweten ingevuld is en dat eventuele tekortkomingen in verbeterplannen zijn opgenomen.
- Een externe IT auditor toetst deze collegeverklaring en neemt de bevindingen op in een assurancerapport. Met de vastgestelde collegeverklaring en het assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

4. Samenvattend beeld collegeverklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Twenterand op 31 december 2019 voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen. Het gaat concreet om 2 DigiD aansluitingen (iBurgerzaken en de website) en de aansluiting op Suwinet. We voldoen aan alle normen, waardoor een verbeterplan niet nodig is. Hieronder volgt een samenvattend beeld:

Onderdeel	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1003081	Ja	Niet van toepassing
DigiD 1001861	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

5. Informatiebeveiliging en privacy 2019

De doelstelling van informatiebeveiliging is als volgt: het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie(systemen) van onze gemeente. Dit onderwerp wordt steeds belangrijker omdat we informatiegestuurd en datagedreven werken. Zonder een adequate beveiliging van onze 'kroonjuwelen' kunnen we als Twenterand niet functioneren: persoonsgegevens, financiële- en medische gegevens, vertrouwelijke plannen en kritieke systemen. Hoe we onze informatiebeveiliging organiseren is niet geheel vrijblijvend. Alle gemeenten in Nederland hebben zich namelijk geconformeerd aan een norm voor informatiebeveiliging: de Baseline Informatiebeveiliging Gemeenten (BIG). Vanaf 2020 geldt overigens een nieuwe norm: de Baseline Informatiebeveiliging Overheid (BIO).

In 2019 zijn in het kader van de BIG verschillende activiteiten uitgevoerd. Denk bijvoorbeeld aan het invoeren van gepersonaliseerde toegangspasjes. In het gemeentehuis dienen alle medewerkers de pasjes zichtbaar te dragen. Daarbij is er ook een nieuwe bezoekersregeling doorgevoerd. Hiermee proberen we het risico op onbevoegde toegang door derden zo klein mogelijk te houden.
Ook is in 2019 gestart met het verbeteren van het autorisatiemanagement. Het doel hiervan is om ervoor te zorgen dat medewerkers zo veel mogelijk alleen de informatie kunnen inzien en gebruiken die ze nodig hebben om hun taak goed uit te voeren. Dit is een langdurig traject en wordt in 2020 voorgezet.
In het kader van beveiligingsbewustzijn is in 2019 gestart met het Nanolearning programma. Dit is een e-learning programma waarbij alle medewerkers elke 3 weken een korte les over informatiebeveiliging of privacy per e-mail toegestuurd krijgen. Door dit onderwerp regelmatig aan bod te laten komen tillen we de alertheid van de gehele organisatie omtrent beveiligingsrisico's steeds naar een hoger niveau.
Verder bereiden we ons voor op de nieuwe norm: de BIO. Hiervoor hebben we bijvoorbeeld meegedaan aan de aanbesteding GGI-veilig.

6. Beveiligingsincidenten en datalekken in 2019

100% beveiligen van informatie bestaat niet. Het is daarom van belang dat we goed omgaan met beveiligingsincidenten. Als er bij een beveiligingsincident persoonsgegevens betrokken zijn spreken we van een datalek. Een 'ernstig' datalek dienen we te melden bij de Autoriteit Persoonsgegevens en/of aan de betrokkenen wie het betreft. Een datalek kan als ernstig worden gekwalificeerd indien er persoonsgegevens van gevoelige aard zijn gelekt (denk aan Burgerservicenummers en gezondheidsgegevens). Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Dit wordt altijd per incident onderzocht.

We onderschrijven het belang van een adequate behandeling van incidenten en de response daarop om daarmee de gevolgen voor de bedrijfsvoering te minimaliseren. Dit begint bij het registeren van alle incidenten die plaatsvinden. Elke medewerker dient alert te zijn op bedreigingen en kwetsbaarheden met betrekking tot informatiebeveiliging en privacy en is verplicht om elk beveiligingsincident intern te melden dat hij/zij ontdekt of vermoedt.

In 2019 zijn er zoals verwacht meer incidenten intern gemeld dan een jaar eerder. Dit omdat er meer aandacht is geweest voor het onderwerp informatiebeveiliging en privacy, waardoor beveiligingsincidenten beter worden herkend.
In totaal zijn er 17 beveiligingsincidenten intern gemeld en geregistreerd. 9 van de 17 gevallen zijn gekwalificeerd als datalek. Het ging onder andere om e-mails die per ongeluk naar de verkeerde ontvanger zijn verstuurd, meldingen van ontvangen phishing e-mails of om post dat geopend retour is gekomen.
Alle gemelde incidenten zijn onderzocht, gedocumenteerd en waar nodig, conform beleid en de AVG, gemeld aan de Autoriteit Persoonsgegevens.

7. Informatiebeveiliging en privacy 2020

In 2020 zal met name de nieuwe norm (BIO) ons bezig houden. Dit betekent onder andere dat het informatiebeveiligingsbeleid geactualiseerd zal worden en dat we ons zullen aansluiten bij het project 'Verhogen Digitale Weerbaarheid' van de VNG. Van belang is om te beseffen dat we nooit klaar zullen zijn met informatiebeveiliging en privacy. We zullen altijd geconfronteerd worden met een veranderende maatschappij en daarmee veranderende risico's. Continue aandacht blijft noodzakelijk.