Gemeente
EDAM
VOLENDAM

Oplegnotitie
Informatiebeveiligingsbeleid

Waarom deze oplegnotitie

Als bijlage wordt u het Informatiebeveiligingsbeleid aangeboden. Dit is een uitgebreid document. Als het mogelijk was het beleid eenvoudig te beschrijven was dat zeker gedaan. Maar omdat het een uitgebreide en complexe materie betreft is dat bijna niet mogelijk. Daar komt bij dat dit nieuwe beleid eigenlijk een uitbreiding is van het vorige waardoor het een flink document blijft.
Tijdens de themaraad op 22 juni 2017 is dit stuk aan u gepresenteerd. Ook zijn er toen praktische voorbeelden van informatiebeveiliging en gevolgen weergegeven. In deze notitie wordt u in het kort nog een keer geïnformeerd over de belangrijkste punten. Uiteraard staat het u uiteraard volledig vrij het gehele document nog eens rustig door te lezen.

Het beleid van 2013 en nu

Het eerste beleid is in 2013 geïmplementeerd en door B&W bekrachtigd. Het beleid is toen 'utopisch' beschreven. Uitgaande van de meest ideale stip op de horizon in een wereld zoals die zou moeten zijn. De gemeente Edam-Volendam had toen te weinig tijd, middelen en menskracht om informatiebeveiliging de nodige aandacht te geven. Ondanks dat heeft men toch de urgentie van het onderwerp ingezien en is er een start gemaakt met het serieus vorm geven van informatiebeveiliging.
Dat is de reden dat in het vorige beleid in elke laatste paragraaf van elk hoofdstuk beschreven is wat er **wel** was gedaan. Het beoogde doel was de ideale wereld zo dicht mogelijk te benaderen. En dat is eigenlijk nu nog steeds zo. Informatiebeveiliging is geen tijdelijk project, maar een onderwerp dat continu de aandacht moet hebben.

Dit is er o.a. van af 2013 gerealiseerd:

- Nulmeting en de productie van nodige documentatie zoals BIG's, IB beleid, IB plan, Incidentmanagement, PIA en andere diverse documenten met maatregelen;
- Bewustwordingscampagne 'Blijf denken, werk veilig…!' . Op alle niveaus. Door het geven van presentaties voor iedereen, aandacht middels posters, e-learning, publicatie op intranet, implementatie van beveiligingsrichtlijnen voor iedereen, persoonlijke begeleiding/ondersteuning enz.;
- Creëren van commitment;
- Start van borging van informatiebeveiliging in de belangrijke processen;
- Toepassen van informatiebeveiliging op ontwikkelingen die de gemeente zijn opgelegd;
- Nemen van maatregelen als gevolg van de normen uit de BIG;
- Implementeren van Informatie Security Management Systeem;
- Uitvoeren van diverse audits (Digid, Suwinet, BRP/PUN, BAG/BGT zie ook ENSIA);
- Uitvoeren van pentesten;
- Registratie van incidenten;
- Starten met dataclassificatie.

Nu, na vier jaar, is het beleid geëvalueerd. De conclusie is dus dat het beleid zoals eerder in deze notitie al is aangegeven ongewijzigd blijft, maar als het ware wordt verlengd.

In elk hoofdstuk is de laatste paragraaf aangevuld met wat de afgelopen drie jaar gerealiseerd is. Daaruit blijkt dat we de komende drie jaar, naast het continueren van wat we al deden, toch nog veel moeten doen!
Daarom zal er de komende drie jaar ook ingezet gaan worden op:

- Het uitvoeren van technische handelingen voor de medewerkers ter uitvoering van hun werkzaamheden, zoals veilig mailen, veilig inloggen en encrypten van bestanden;
- Het uitbreiden van Cybersecurity => andere technische maatregelen;
- Het voorbereiden op incidenten => crisisgame op alle niveaus;
- Het uitvoeren van audits op bedrijven die 'onze' gegevens verwerken;
- Het opzetten privacy management;
- Het voorzetten van gegevensmanagement;
- Bewustwording van de accountability => aantoonbaar maken.

Bewustwording houdt aandacht

Uit alles komt naar voren dat het lastig is het beleid goed uit te voeren. Dit heeft o.a. te maken met de fusie en hoe collega's, op alle niveaus, met dit onderwerp omgaan. Daarom zal de focus ook blijven liggen op bewustwording. Naast de kracht van de herhaling gaan er ook nieuwe onderwerpen aan de orde komen. Uit praktijk blijkt dat bewustwording van de collega's groeit, maar nog lang niet voldoende is. Het gevoel van urgentie is soms nog ver te zoeken. De vraag is of de organisatie er 'rijp' voor is. Afspraken worden wel gemaakt, maar leiden niet tot de noodzakelijke uitvoer. Het ontbreekt aan goede communicatie tussen secties/deskundigen en MT. En juist hiervan is de informatiebeveiliging adviseur/de CISO van afhankelijk. Dit probleem is diverse malen besproken met leidinggevende en gerapporteerd aan de directie en de portefeuillehouder. Langzaam maar zeker komt hier wel enige progressie in. We hopen deze weg voort te zetten.

Informatiestrategie 2017-2022

Met het uitvoeren van het beleid wordt tevens de verbinding gelegd met de informatiestrategie 2017-2022. De overlap en samenwerking is groot, maar moet wel gescheiden blijven. Op deze wijze wordt aan het 'vier-ogen principe' uitvoering gegeven maar wordt in de praktijk beperkt. De vraag is of plaatsing van informatiebeveiliging onder de afdeling Interne Dienstverlening, waar ook Informatievoorziening onder valt, de juiste keuze is.
Daar waar informatie**voorziening** zich richt op het vormgeven van dienstverlening, bedrijfsvoering en informatievoorziening, zal informatie**beveiliging** er op toe zien dat gegevens tijdig (wendbaar), veilig (vertrouwen), en integer (leiderschap) in de bedrijfshuishouding bewegen. Beschikbaarheid, integriteit en vertrouwelijk zijn hierbij de pijlers. Deze worden dan ook in proce**s**sen verwerkt (verbinden) zoals de Baselinetoets en de Data Privacy Impact Assessments (DPIA). Naast het informatiebeveiligingsbeleid wordt een informatiebeveiligingsplan gemaakt. Dit plan zal bestaan uit de resultaten van de ENSIA audit (zie voor uitleg hieronder). Een plan met bevindingen, risico's en uitgewerkte kostenindicaties. De bedragen die in de begroting voor informatiebeveiliging zijn genoemd worden gebruikt om bovengenoemde punten te realiseren.

De BIG

Naast het informatiebeveiligingsbeleid zijn de Baseline Informatiebeveiliging Nederlandse Gemeente (BIG), het Strategisch Kader (SK) en het Tactisch Kader (TK) bekrachtigd door B&W. Dit is landelijke regelgeving en komt voort uit de VNG resolutie van november 2013. In deze resolutie hebben alle gemeenten afgesproken informatiebeveiliging naar een hoger niveau te tillen door o.a. de BIG's te introduceren.

De BIG SK geeft de afspraken aan die op strategische niveau zijn gemaakt. Deze afspraken gelden nog steeds. Afspraken zoals:

- De opdracht, doel;
- Het Strategisch normenkader;
- Scope;
- Uitgangspunten;
- Visie;
- Plaatsbepaling en Reikwijdte;
- Beleid;
- Verantwoordelijkheden.

In de BIG TK staan de ongeveer 340 normen die afkomstig zijn van de wereldbekende 'ISO certificering'. Deze zijn gebaseerd op 'pas toe en leg uit' principe. Daar waar ontwikkelingen organisatiebreed uitgevoerd moeten worden is afgesproken hiervoor de nodige maatregelen te treffen. Kortom 'informatiebeveiliging by design'. De BIG SK en BIG TK overlappen en verbinden het beleid. Het informatiebeveiligingsplan heeft een overlap en verbintenis met ENSIA.

ENSIA

Staat voor: Eenduidige Normatiek Singel Information Audit en is in juni 2017 gestart. Dit is in feite een audit/zelfevaluatie op de BIG die elk jaar wordt uitgevoerd. Er zijn nu een aantal audits die we jaarlijks uit moeten voeren. Deze zijn de BRP/PUN zelfevaluatie, Suwinet, DigiD en BAG/BGT audit. Hierin worden vaak dezelfde vragen gesteld. Deze vragen worden dus vier á vijf keer gesteld. Vragen die ook als normen in de BIG zijn opgenomen. Dus is het handiger de vragen één keer te stellen. Hiermee is de 'BIG audit/zelfevaluatie' ontstaan. In praktijk houdt dit in dat we ongeveer 160 vragen uit de BIG over de DigiD en Suwinet moeten beantwoorden en moeten bewijzen dat we hier als organisatie goed mee bezig zijn. Met andere woorden: zijn wij betrouwbaar? Dit wordt door een externe auditor geauditeerd die hierover een verklaring af zal geven.

Met ENSIA wordt eveneens een horizontale als verticale verantwoording afgelegd. Dus rapportages voor B&W en de Gemeenteraad, maar ook naar verantwoordelijke binnen de betrokken Ministeries. Elk jaar wordt door ENSIA duidelijk in een wat wij als gemeente moeten doen om de informatiebeveiliging te complementeren. Dit wordt verwerkt is het informatiebeveiligingsplan. Een plan met bevindingen, risico's en kostenindicaties.

Als we niet de ENSIA audit halen, heeft dit indirecte gevolgen voor onze dienstverlening. Het kan zijn dat we afgesloten worden van Suwinet. Antwoorden op vragen en bewijzen die we nu uit Suwinet halen zullen de burgers dan zelf moeten geven en/of worden aangeleverd. Dit geldt ook voor DigiD audit. Als en we niet 'slagen' voor deze audit kunnen we worden afgesloten van de DigiD koppeling. Het gebruik van DigiD op onze website vervalt waardoor gegevensuitwisseling niet meer veilig is. Dit geldt dan tevens voor de WOZ zaken en digitale aanvragen bij Burgerzaken via internet.

Wilt u meer informatie over ENSIA? In dit animatiefilmpje wordt ENSIA helder uitgelegd: https://youtu.be/cc98ZlPldhQ

Privacy

Tot slot privacy. Privacy is een belangrijk onderdeel van informatiebeveiliging. Door de Algemene Verordening Gegevensbescherming (AVG; de Europese Regelgeving), die op 25 mei 2018 in werking treedt,

krijgt de privacy nog meer aandacht. Door de AVG komen er veel (verplichte) taken op de gemeente af. Dit heeft gevolgen voor personele bezetting. Daar waar nu door één medewerker de informatiebeveiliging en privacy wordt uitgevoerd, moeten in de toekomst taken gescheiden gaan worden. De AVG verplicht de gemeente taken uit te voeren, maar ook deze te controleren. Dus moet er iemand zijn die voor uitvoer verantwoordelijk is, maar ook iemand die de controle doet. En dan blijft ook nog iemand verantwoordelijk voor de uitvoer van de informatiebeveiliging.

Kortom er ligt de komende jaren een flinke taak op ons te wachten. Maar met voldoende commitment en gevoel voor urgentie gaat het ons lukken om de utopie tot realiteit te maken.