Jaarverslag informatieveiligheid gemeente Zaanstad

Periode: 2018

Inhoudsopgave

1 Versiebeheer

Versie	Datum	Opstellers	Reden wijziging
0.1	28-1-2019	Agatha Smeeing	Verslaglegging informatiebeveiliging 2018
0.2	12-2-2019	Agatha Smeeing	Tekstuele aanpassingen, aanvulling §6.1, 7.1 en 9 uitgebreid met §6.5 en 10
0.3	11-3-2019	Agatha Smeeing	Feedback Jan Willem van Brummelen verwerkt en §5.1 met schematisch verantwoordingsschema
0.9	28-3-2019	Agatha Smeeing	Gereed voor bespreking wethouder en als bijlage jaarverslag
1.0	08-4-2019	John van der Sluis	Laatste wijzigingen doorgevoerd

2 Verspreiding

Dit jaarverslag wordt vastgesteld door de directie en als bijlage bij de jaarrekening ter kennisname verstuurd aan het college van B&W en de gemeenteraad.

3 Doel en scope

Dit jaarverslag bevat een overzicht van de uitgevoerde activiteiten en gerapporteerde grotere incidenten met betrekking tot het onderwerp informatieveiligheid bij de gemeente Zaanstad over het jaar 2018. De rapportage is in overeenstemming met het door de directie vastgestelde beleidsplan Informatiebeveiliging en privacy 2017– 2019 opgesteld.
Met het van kracht worden van de Algemene Verordening Gegevensbescherming (AVG) (privacywetgeving) per 25 mei 2018 is op projectmatige basis de inrichting van de AVG vorm gegeven binnen de gemeente Zaanstad. Gezien de urgentie en de aandacht voor dit onderwerp is besloten om de jaarverslagen separaat op te stellen in tegenstelling tot eerdere jaren. Neemt niet weg dat een optimale privacybescherming niet zonder informatieveiligheid kan plaatsvinden en de twee onderwerpen wel degelijk nauw met elkaar verbonden zijn en er intensieve samenwerking plaatsvindt.

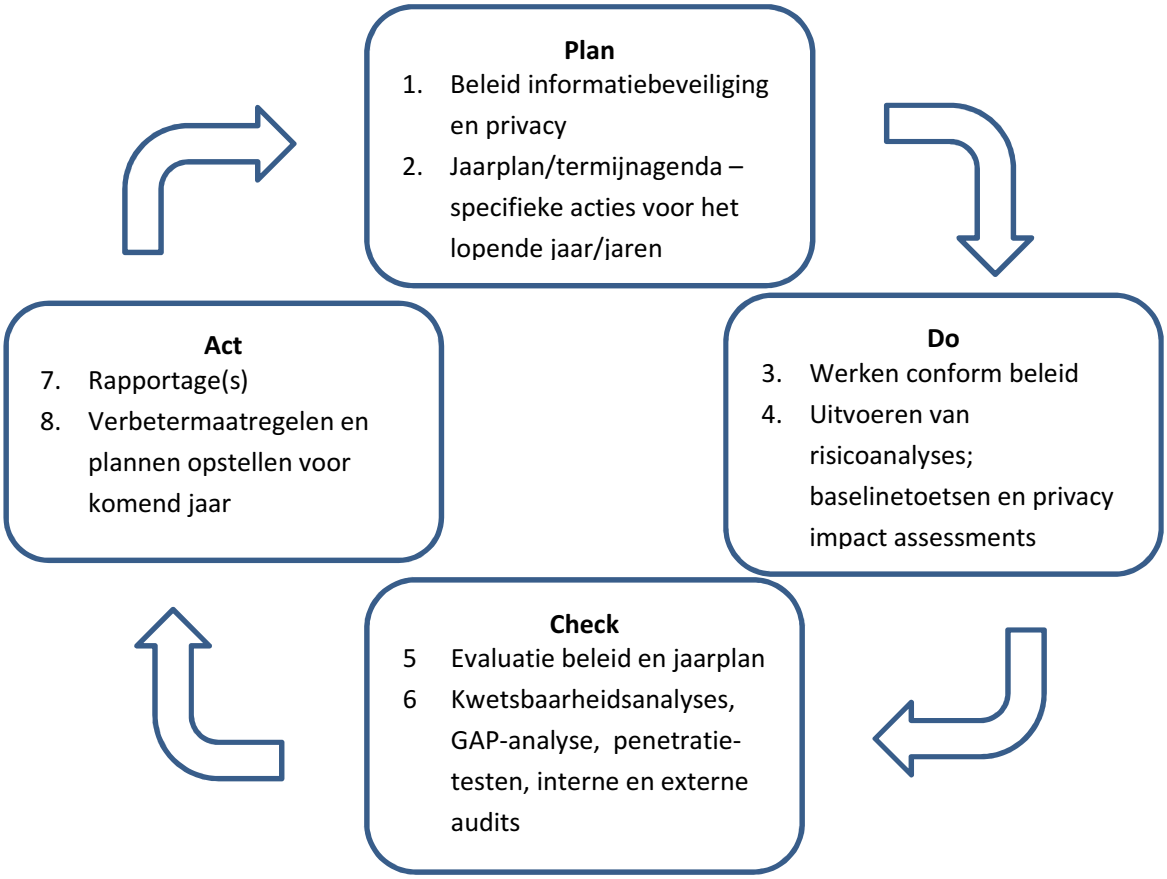
4 Personele bezetting

In 2018 is er gekeken naar de governance op het gebied van informatieveiligheid en privacybescherming. Dit heeft er toe geleid dat er op de begroting ruimte is gemaakt voor uitbreiding van capaciteit op deze vakgebieden. Er is gekozen voor de positionering van de coördinator informatieveiligheid (CISO) en de Functionaris Gegevensbescherming (FG) bij Auditing en Onderzoek met ingang van 1 januari 2019, de FG is per 1 januari 2019 overgegaan, de CISO volgt later. Binnen de afdeling Informatie, Beheer en Techniek (IBT) wordt een team gevormd met Informatiebeveiligers en Privacy officers, het IBPO-team. In het laatste kwartaal van 2018 is 1 van de functies vervuld door een interne medewerker met als aandachtsgebied privacy. De verdere invulling van het team vindt plaats in de eerste helft van 2019.

5 Informatieveiligheid

Informatieveiligheid is het treffen en onderhouden van een samenhangend pakket van organisatorische, procedurele en technische maatregelen gericht op het waarborgen van de betrouwbaarheid van de informatievoorziening.

Informatieveiligheid is geen eenmalige activiteit maar een continu verbeterproces. Gemeente Zaanstad kiest bij het implementeren, uitvoeren en onderhouden van informatiebeveiliging dan ook voor een aanpak op basis van een kwaliteitscyclus (Plan-Do-Check-Act of PDCA-cyclus) waardoor de voortdurende verbetering van de betrouwbaarheid van de informatievoorziening wordt geborgd.



6 Verantwoording en zelfevaluaties

6.1 Verantwoording

De horizontale verantwoording over informatieveiligheid en privacybescherming aan het College van B&W en het gemeentebestuur vindt door middel van dit jaarverslag plaats.

Daarnaast heeft de gemeente in 2018 volgens de methodiek ENSIA gerapporteerd. De antwoorden van de ENSIA zelfevaluatie, de daaruit verkregen Collegeverklaring en de door een onafhankelijke auditor opgestelde Assurance verklaring voor de DigiD koppelingen en Suwinet, worden gebruikt voor de verticale verantwoording aan de stelselhouders op het gebied van informatieveiligheid.

ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid, dat is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

ENSIA helpt gemeenten om in één keer slim verantwoording af te leggen over informatieveiligheid. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is samengevoegd en gestroomlijnd.

De samenvoeging en stroomlijning betekenen in essentie niet dat de verantwoording efficiënter en effectiever verloopt. De borging van de PDCA cyclus en de vastlegging van bewijsmateriaal gebeurt nu te veel op ad-hoc basis, vraagstelling is voor meerdere interpretaties vatbaar en eenduidige registratie ontbreekt. Daarnaast is de invoering in de verplichte ENSIA tool handwerk. In de loop van 2019 wordt binnen Zaanstad gewerkt aan de structurele borging van de PDCA cyclus voor informatieveiligheid en de vastlegging van het bewijsmateriaal. Daarnaast neemt Zaanstad deel aan de pilot van VNG Realisatie om de verantwoording over de Baseline Informatiebeveiliging Overheid (BIO) conform de ENSIA methodiek voor te bereiden voor 2020 en daarmee een bijdrage te leveren aan de kwaliteit van de vragenlijsten en rapporten.

6.2 Zelfevaluatie ENSIA

Proceseigenaren van de (deel)processen DigiD-aansluitingen (Webformulieren, Parkeren en Mijn Inkomen), Suwinet, BRP, PUN, BAG, BGT, ICT, inkoop, facilitair en personeel hebben de vragen in de zelfevaluatie ENSIA voor hun processen beantwoord. Een deel van de zelfevaluatie vragen waren van toepassing op meerdere processen. De verschillende antwoorden zijn in de ENSIA projectgroep met de proceseigenaren behandeld. De gemeente heeft de zelfevaluatie over verantwoordingsjaar 2018 tijdig ingeleverd.

6.3 Zelfevaluatie BRP en Waardedocumenten

De zelfevaluatie BRP en waardedocumenten (PUN) is wat betreft de informatiebeveiligingsvragen opgenomen in ENSIA, naast de kwaliteitsmonitor van het ministerie. De antwoorden uit beide rapportages zijn samengevoegd in de managementrapportage BRP 2018 en managementrapportage PNIK 2018, deze is begin maart ter informatie aan het College verstrekt.

6.4 ICT-assessments DigiD

Sinds 2013 moeten alle organisaties die DigiD gebruiken aan bepaalde beveiligingsrichtlijnen voldoen. Jaarlijks wordt daarvoor voor elke DigiD-aansluiting een verplichte audit uitgevoerd. In Zaanstad betreft dit in 2018 een DigiD-audit voor de volgende aansluitingen:

- Webformulieren
  Het betreft hier aanvraagformulieren voor afdeling Burgerzaken en het opvragen van WOZ-taxatieverslagen.
- Parkeren
  Hierbij gaat het om het aanvragen van een parkeervergunning.
- Mijn inkomen
  Hierbij gaat het om het inzien van de status van uitkeringen en het doorgeven van wijzigingen.

In 2018 zijn voor 2 DigiD-assessments die in het verantwoordingsjaar 2017 niet aan alle normen voldeden, verbeteringen doorgevoerd. De verbeteringen zijn door een onafhankelijk auditor getoetst en akkoord bevonden.

6.5 Suwinet

De zelfevaluatie van Suwinet maakt onderdeel uit van ENSIA. Naar aanleiding van de bevindingen waarbij niet aan alle gestelde normen werd voldaan, is een verbeterplan opgesteld. De verbeteringen zijn meegenomen in de zelfevaluatie over verantwoordingsjaar 2018 en worden de eerste helft van 2019 getoetst door een onafhankelijk auditor.

7 Implementatie Baseline Informatiebeveiliging

Naar aanleiding van de resultaten uit de zelfevaluatie over 2017 is er in 2018 expliciet aandacht besteed aan de voorbereidingen voor de structurele borging van de beveiligingsmaatregelen, actualiseren van bestaand beleid voor onder anderen wachtwoord gebruik en gebruik van mobiele apparatuur. In 2018 is er veel aandacht geweest voor de beveiliging van processen en projecten, niet alleen door het nemen van passende maatregelen maar ook door het (technisch) toetsen of deze maatregelen werken zoals bedacht.

7.1 Risico gebaseerd maatregelen nemen

Om passende organisatorische en technische maatregelen te kunnen nemen binnen de processen en bijbehorende informatiesystemen wordt gekeken naar de risico's die het proces op het gebied van informatieveiligheid loopt. De Baseline Informatiebeveiliging Gemeenten (BIG) wordt per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO)[1]. Deze baseline is nog meer gebaseerd op het nemen van maatregelen vanuit risicoperspectief. Vooruitlopend op deze BIO heeft de gemeente haar risicoanalyse methodiek aangepast en worden nieuwe projecten en gewijzigde processen door middel van deze methodiek getoetst op aanwezige risico's en daarbij aansluitend passende maatregelen genomen.
In zijn algemeenheid genomen kan de bewustwording bij proceseigenaren dat ze verantwoordelijk zijn voor informatieveiligheid binnen hun processen binnen de gemeente nog verder worden verhoogd.

7.2 Beveiliging van industriële automatiseringssystemen

Onder leiding van een externe projectleider wordt in het project informatiebeveiliging industriële automatisering aandacht besteed aan de huidige stand van zaken van de informatiebeveiliging van de brugbediening en de riolen en gemalen, de mogelijke verbeteringen en de borging van de informatieveiligheid. Ook dit project wordt op basis van risico-inventarisatie uitgevoerd. Het doel van de inventarisatie is om te kunnen verantwoorden dat er alles aan gedaan is om incidenten bij industriële automatiseringssystemen te herkennen, te voorkomen en te beheersen. Per definitie is elk informatiesysteem te hacken, er blijft altijd een restrisico bestaan.

7.3 Sintstad

Ter voorbereiding op de intocht van Sinterklaas in Zaanstad is er uitgebreid aandacht geweest voor de digitale veiligheid van de betrokken informatiesystemen. Zo is de website Sintstad.zaanstad.nl vooraf technisch getest op mogelijk misbruik/manipulatie van de informatie op de website en is er tijdens de intocht de website vanuit informatieveiligheid extra gemonitord.

7.4 Beveiligde e-mail

Met de komst van de AVG is er meer aandacht voor het beveiligd uitwisselen van informatie met (keten)partners. In het kader daarvan is er een project opgestart die naast de bestaande middelen zoals in gebruik binnen de gemeente Zaanstad ook met zorgaanbieders op een gebruikersvriendelijke manier op een veilige manier e-mails uitgewisseld kunnen worden. In de eerste helft van 2019 wordt deze methodiek in productie genomen.

[1] De Baseline informatiebeveiliging overheid (BIO) gaat gelden voor alle overheidsinstellingen. 2019 is een overgangsjaar voor de implementatie van de BIO.

7.5 Contracten

Bij het afsluiten van nieuwe contracten worden de eisen voor informatieveiligheid beter meegenomen aan het begin van de gesprekken met leveranciers en worden deze maatregelen in de contracten of bijbehorende verwerkersovereenkomsten vastgelegd. Om te voorkomen dat er nieuwe gaten (achterdeuren) ontstaan in de beveiliging, dient voorkomen te worden dat er zonder advisering op het gebied van informatieveiligheid een contract wordt afgesloten. Er is een toename van de behoefte aan advisering op dit gebied zichtbaar.

7.6 Project Identity en Accessmanagement

Eén van de doelstellingen van het project Identity en Accessmanagement is de informatieveiligheid en privacybescherming verbeteren. Het verbeteren van het toekennen, wijzigen en intrekken van rechten tijdens het in-, door- en uitstroomproces draagt bij aan het beheer van toegangsrechten van gebruikers (§11.2 uit de tactische BIG). De coördinator informatieveiligheid draagt hieraan bij voor de invulling van de kaders op het gebied van informatieveiligheid.

8 Bewustwording

Medewerkers worden gezien als de sterkste schakel in de informatiebeveiligingsketen. Indien andere maatregelen falen, zijn de medewerkers de laatste en daarmee belangrijkste schakel in de informatiebeveiligingsketen. Om medewerkers deze belangrijke schakel te kunnen laten zijn, is continu bewustwording van belang.

8.1 Nieuwe medewerkers

Nieuwe medewerkers worden uitgenodigd om deel te nemen aan de introductietraining informatieveiligheid en privacybescherming. In een uur tijd worden ze op een interactieve manier meegenomen in het hoe, wat, waarom van informatieveiligheid en privacybescherming. De training wordt verzorgd door de FG en de CISO. De opkomst bij de introductietraining ligt rond de 15%. Vanuit management verdient het meer aandacht dat de aanwezigheid bij deze trainingen wordt groot.

8.2 Informatievoorziening

Informatieveiligheid en privacybescherming hebben een eigen pagina op het intranet waar naast werk gerelateerde berichten op het gebied van informatieveiligheid en privacybescherming ook berichten geplaatst worden die buiten werk om heel relevant kunnen zijn. Informatieveiligheid stopt tenslotte niet op het moment dat je je werkplek verlaat, in de huidige tijd is de scheidslijn tussen privé en zakelijk lang niet meer zo duidelijk.

In de pantry’s zijn het afgelopen jaar posters opgehangen om aandacht te vragen voor het onderwerp cybersecurity en is het onderwerp in diverse afdelingsoverleggen aanbod gekomen.

Een gemeentebrede bewustwordingscampagne op het gebied van informatieveiligheid heeft niet plaats gevonden mede ook door de brede aandacht die in 2018 aan de invoering van de AVG is besteed, waarbij ook onderwerp van de AVG informatieveiligheid zeker aanbod is gekomen.

8.3 College

In de introductieperiode van het nieuwe College zijn de wethouders door middel van een presentatie over informatieveiligheid op de hoogte gebracht over dit onderwerp in relatie tot hun portefeuilles en zijn ze meegenomen in de verantwoordingsmethodiek.

9 Interne audits informatieveiligheid

9.1 Technische security scans

Om te waarborgen dat de genomen maatregelen ook naar behoren werken zijn er door externe specialisten technische securitytoetsen uitgevoerd op onder andere:

- applicaties die de gemeente Zaanstad zelf heeft laten ontwikkelen;
- applicaties die gehost worden bij externe leveranciers;
- applicaties met een DigiD aansluiting;
- gemeentelijke infrastructuur.

9.2 Kwetsbaarhedenscans

De informatiebeveiligingsdienst voor gemeenten (IBD) doet via e-mail melding van dreigingen en kwetsbaarheden in applicaties die door de gemeente worden gebruikt. De gemeente Zaanstad neemt elke melding op in het servicedesksysteem, waarna de ICT-medewerkers een afweging maken van de relevantie voor Zaanstad, de impact, het risico en zo-nodig een herstelmaatregel plannen.
Daarnaast wordt ook de infrastructuur preventief gescand op kwetsbaarheden.

10 Informatiebeveiligingsincidenten

Er hebben zich in 2018 geen grote informatiebeveiligingsincidenten voorgedaan. De incidenten die zich voordeden waren beperkt in omvang wat schade betreft en snel te herstellen. Het ontstaan van datalekken heeft een relatie met informatiebeveiligingsincidenten, bijvoorbeeld het versturen naar de verkeerde afzender of verlies van apparatuur kan een datalek zijn.

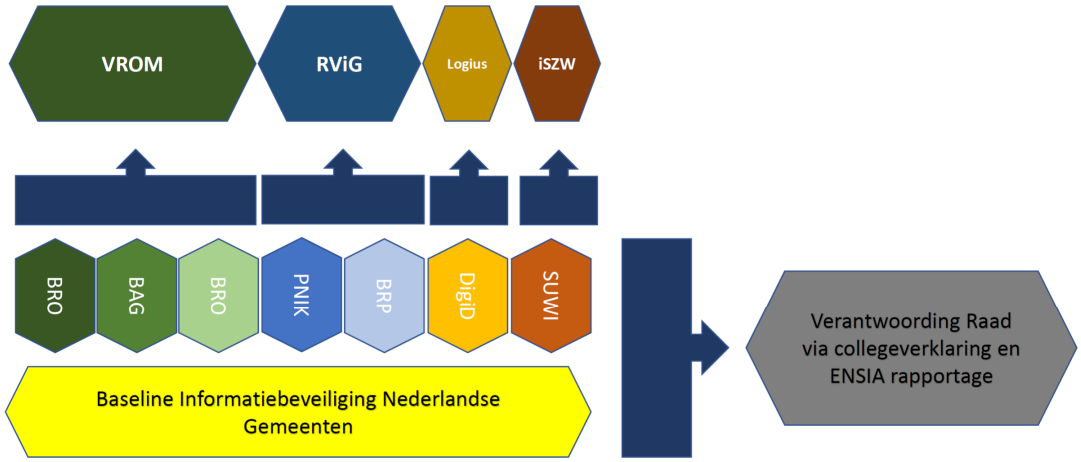
Naar aanleiding van meldingen van onder andere de Informatiebeveiligingsdienst voor gemeenten (IBD) van incidenten is extra gemonitord op het netwerk. De huidige organisatorische en technische beveiligingsmaatregelen hebben deze incidenten kunnen afvangen voor de gemeente zodat de gemeente hier geen schade van ondervonden heeft.

11 Bijlage 1 Managementsamenvatting zelfevaluatie ENSIA 2018

Dit rapport geeft de uitkomsten weer van de gemeentebrede (horizontaal) uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2018. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG)[2]. Of we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie die is uitgevoerd in de periode 1 juli t/m 18 december 2018. Als gemeente Zaanstad rapporteren we op één moment in het jaar over de status van onze informatieveiligheid. De methodiek heet ENSIA en staat voor Eenduidig Normatiek Single Information Audit.

Vanuit deze horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders afgeleid, de zogenaamde verticale verantwoording. Zo zijn de informatieveiligheidsvragen over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) uit ENSIA automatisch overgeheveld en ingevoegd bij de kwaliteitsmonitor voor verantwoording aan Rijksdienst voor Identiteitsgegevens (RvIG). En voor de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootschalige Topografie (BGT) verantwoording worden data automatisch naar het Ministerie van I&W [3] opgeleverd vanuit ENSIA.

Voor het jaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en deze is getoetst door de interne EDP auditor met dossierreview door de EDP auditor van de gemeente Haarlem. Met de vastgestelde Collegeverklaring en het Assurance rapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.



Voor de verslaglegging is deze rapportage opgesteld conform de BIG hoofdstukindeling. In elk hoofdstuk is een korte samenvatting over de achtergrond van het hoofdstuk opgenomen en zijn de resultaten uit de zelfevaluatie uitgewerkt. Naast het gemeentebrede beeld zijn de resultaten voor de IT auditvragen vanuit Suwinet en de DigiD zelfevaluatie opgenomen.

[2] Gemeenten hebben met het aannemen van de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” in november 2013 deze Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) als hét gemeentelijk basisnormenkader voor informatieveiligheid omarmd.

[3] De BAG en BGT kennen elk in ENSIA ook een domeinspecifieke vragenlijst en een specifieke rapportage. Deze wordt separaat voorgelegd aan het College ter vaststelling en aangeboden aan het Ministerie van I&W.

11.1 Uitkomsten Baseline Informatieveiligheid Gemeenten

Op hoofdlijnen zijn de uitkomsten van de BIG zelfevaluatie conform onderstaande status omschrijving opgenomen in deze managementsamenvatting en worden ze in de vertrouwelijke interne verantwoordingsrapportage ENSIA specifieker uitgewerkt.

De status wordt als volgt weer gegeven:

Symbool	Omschrijving
☺	Voldoet aan de norm
😐	Voldoet gedeeltelijk aan de norm
☹	Voldoet niet aan de norm

De normen zijn in de BIG op heel abstract niveau beschreven en zijn voor meerdere interpretaties vatbaar. Door net als vorig jaar deze diepgaande zelfevaluatie uit te voeren, waarbij gekeken wordt naar de aantoonbaarheid van de maatregel (opzet en bestaan), is een goed overzicht verkregen waar verbeteringen in de organisatie nodig zijn. Veel maatregelen worden in de praktijk uitgevoerd maar ontbreekt de formele vastlegging van de procedure/werkinstructie. Constatering is wel dat door de beperkte beschikbare capaciteit van het informatiebeveiligingsteam door extra werk als gevolg van de ENSIA de uitvoering van het jaarplan 2018 onvoldoende gevorderd is waardoor de bevindingen in deze rapportage veel overeenkomsten vertonen met de rapportage uit 2017.

Voor het eerst dit jaar waren er in de BIG ENSIA vragenlijst ook vragen met betrekking tot de AVG opgenomen. De beantwoording en de verslaglegging daarvan vindt plaats door de Functionaris Gegevensbescherming in het jaarverslag Privacy 2018.
In de ENSIA vragenlijst zijn een aantal vragen uit 2017 komen te vervallen en is de vraagstelling van diverse vragen aangepast waardoor er niet direct een 1 op 1 vergelijking te maken is met de bevindingen over 2017.

Vanaf januari 2020 wordt er een nieuw normenkader voor informatiebeveiliging voor gemeenten van kracht, de Baseline Informatiebeveiliging Overheid (BIO). In 2019 zal er gestart worden met de implementatie van de BIO. Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.

De implementatie van de BIO sluit aan bij de verbeteringen die naar voren zijn gekomen uit de zelfevaluatie 2018. De nadruk komt in 2019 te liggen op het implementeren van het Information Security Management Systeem (ISMS) zodat de monitoring om de voortgang van de verbeteringen beter plaats kan vinden en er gewerkt wordt met de Plan, Do, Check, Act cyclus op de normen. De normen waar we nu wel (grotendeels) aan voldoen, moeten frequent onderworpen worden aan de controle cyclus om te bepalen of ze nog steeds voldoen en passend zijn bij de risico's. Het beleggen van de verantwoordelijkheden voor informatieveiligheid op het juiste niveau in de organisatie, treffen van maatregelen op basis van risico-inschatting en de menselijke aspecten voor informatiebeveiliging zijn verbeteringen die opgenomen worden in het jaarplan 2019.
Daarnaast is het classificeren van processen en de daarbij behorende informatie van belang evenals aandacht voor het optimaliseren van de techniek naar de actuele dreigingen en borging van de bedrijfscontinuïteit.

Big Hoofdstuk	Omschrijving	Status	Prioriteit
3	Implementatie van de Tactische Baseline (oa ISMS)	☹	1
4	Risicobeoordeling en risicoafweging bij samenwerkingsverbanden	😐	2
5	Beveiligingsbeleid	🙂	1/2
6	Organisatie van de informatiebeveiliging	☹	1
7	Beheer van Bedrijfsmiddelen	☹	1
8	Personele beveiliging	😐	2/4
9	Fysieke beveiliging	☺	
10	Beheer van communicatie en bedieningsprocessen	😐	1/2/3/4
11	Toegangsbeveiliging	🙂	1/2
12	Verwerving, ontwikkeling en onderhoud van informatiesystemen	😐	1/2
13	Beheer van informatiebeveiligingsincidenten	🙂	2
14	Bedrijfscontinuïteitsbeheer	☹	3
15	Naleving	🙂	3

11.2 Uitkomsten Suwinet IT auditvragen

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De gemeente Zaanstad maakt gebruik van Suwinet voor uitvoering van de volgende taken:

- Suwinet voor de Participatiewet, IOAZ en IOAW

Onze gemeente maakt hiernaast gebruik van Suwinet door de volgende niet-SUWI partijen:

- Suwinet voor Burgerzaken
- Suwinet voor Gemeentelijk gerechtsdeurwaarders

De gemeente Zaanstad is voor Suwinet voor RMC (Regionaal Meldpunt Coördinatie voortijdig schoolverlaters) aangesloten bij de gemeente Amsterdam.

De verbeterpunten voor de normen op het gebied van autorisatie die naar voren zijn gekomen tijdens de zelfevaluatie zijn opgenomen in een verbeterplan.

11.3 Uitkomsten DigiD

De gemeente Zaanstad beschikt over 4 DigiD aansluitingen.

11.3.1 Aansluiting 1000065 – Webformulieren Zaanstad.

De DigiD aansluiting ‘Gemeente Zaanstad webformulieren’ wordt voor authenticatie gebruikt voor de website www.zaanstad.nl. Deze functionaliteit wordt geboden door de webapplicatie Mozard van leverancier Mozard.

Deze omgeving wordt binnen de gemeente Zaanstad gehost waardoor in de zelfevaluatie een uitgebreide set aan de DigiD normen is getoetst. Voor twee normen is tijdens de zelfevaluatie geconstateerd dat er verdere verbetering of uitwerking nodig zijn om te voldoen aan de DigiD-normen. Voor het verbeteren van deze normen is een verbeterplan opgesteld.

11.3.2 Aansluiting 100385 – Schuldhulpverlening

De DigiD aansluiting ‘Schuldhulpverlening’ wordt voor authenticatie gebruikt voor de website mijnschulden.zaanstad.nl. Deze functionaliteit wordt geboden door de webapplicatie Allegro van

leverancier Innovadis. De DigiD aansluiting voor Schuldhulpverlening is in 2018 afgebouwd en eind 2018 opgezegd. De verplichting tot verantwoording aan de toezichthouder is hiermee komen te vervallen.

11.3.3 Aansluiting 100785 – Gemeente Zaanstad Parkeren

De DigiD aansluiting 'Gemeente Zaanstad Parkeren' wordt voor authenticatie gebruikt voor het aanvragen/wijzigen of beëindigen van parkeervergunningen via de website parkeren.zaanstad.nl. Deze functionaliteit wordt geboden door de webapplicatie CityPermit van leverancier Sigmax. In de zelfevaluatie zijn de op de gebruikersorganisatie van toepassing zijnde normen getoetst. Voor één norm is tijdens de zelfevaluatie geconstateerd dat er verdere verbetering of uitwerking nodig is om te voldoen aan de DigiD-norm. Voor het verbeteren van deze norm is een verbeterplan opgesteld.

11.3.4 Aansluiting 1002129 – Mijn inkomen

Centric biedt de functionaliteit aan voor de DigiD aansluiting Mijn inkomen. Hierbij gaat het om het inzien van de status van uitkeringen en het doorgeven van wijzigingen. In de zelfevaluatie zijn de op de gebruikersorganisatie van toepassing zijnde normen getoetst. Voor één norm is tijdens de zelfevaluatie geconstateerd dat er verdere verbetering of uitwerking nodig is om te voldoen aan de DigiD-norm. Voor het verbeteren van deze norm is een verbeterplan opgesteld.

gemeente Zaanstad

Stadhuisplein 100, 1506 MZ Zaandam
Postbus 2000, 1500 GA Zaandam

T14 075
antwoord@zaanstad.nl
www.zaanstad.nl