gemeente **Barneveld**

Nr. 1080828

Collegevoorstel

Onderwerp:
Voorstel betreffende informeren van de gemeenteraad over informatiebeveiliging in het kader van Eenduidige Normatiek Single Information Audit (ENSIA).

Gevraagde beslissing:

Ctrl-klik hier voor een toelichting voor het invullen van het voorstel

1. In het kader van ENSIA moet de gemeenteraad van de gemeente Barneveld geïnformeerd worden over informatiebeveiliging.

Raad
☑ Ter kennisname naar de raad
Nummer beleidsproduct:
☐ Op overzicht Bestaand beleid (website)

Datum 21 juni 2018 Steller: T.A. Arends
Afd: BDV-IA Aantal bijlagen 1
Afd.hoofd: Mevr. B. Lamberts-Bruins Portefeuillehouder De heer André van de Burgwal

Openbaarheid
Besluit (voorblad) openbaar: ◉ Ja ○ Nee, zie beslispunt :
Groentje openbaar: ○ Ja ◉ Nee, zie beslispunt :
Bijlagen openbaar: ◉ Ja ○ Nee, vermelden op bijlage

	Akkoord	Bespreken	Aantekeningen
Secretaris			
Burgemeester			
Wethouder A. de Kruijf			
Wethouder P.J.T. van Daalen			
Wethouder A.H. van de Burgwal			
Wethouder D. J. Dorrestijn-Taal			

Beslissing burgemeester en wethouders : 16 JULI 2018

conform advies.

Nummer op besluitenlijst: 28/15

Jaarverslag informatiebeveiliging gemeente Barneveld 2017

Inleiding

In het kader van de nieuwe verantwoordingsnormenkader ENSIA (Eenduidig Normatiek Single Information Audit) is het van belang de gemeenteraad te informeren over de huidige stand van zaken over informatiebeveiliging. Bij het informeren van de gemeenteraad staan de uitslagen vanuit audits, die voortkomen uit de ENSIA verantwoording, centraal. Daarnaast staat er een statusupdate over de algemene informatiebeveiliging in en geeft het jaarverslag de belangrijkste aandachtspunten voor aankomend jaar aan.

Nut & noodzaak

De primaire taak van de gemeente Barneveld is dienstverlening richting burgers. Hierdoor is het van essentieel belang dat de informatie over burgers op een veilige manier geborgd wordt. Daarnaast is het ook van essentieel belang dat de dienstverlening richting de burgers gecontinueerd blijft en dat er geen informatie van burgers openbaar wordt.

In het kader van dienstverlening heeft iedere gemeente in Nederland toegang tot vertrouwelijke informatiebronnen (DigiD/Suwinet/BAG/BGT) waarvoor specifieke regels zijn opgesteld voor gebruik daarvan. Deze regels worden jaarlijks getoetst om te bewerkstelligen dat de gemeente ‘in-control’ is.

In 2012 hebben alle gemeenten de convenant: “Informatieveiligheid Gemeenten” getekend naar aanleiding van de resolutie: “Informatieveiligheid, randvoorwaarde voor de professionele gemeente”. Hiermee heeft de gemeente Barneveld zich geconformeerd aan het toepassen/implementeren van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Sinds juli 2017 is er nieuw verantwoordingsnormenkader voor gemeenten geïmplementeerd, Eenduidig Normatiek Single Information Audit (ENSIA). De ENSIA verplicht gemeenten om verantwoording af te leggen over:

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
- Digitale iDentiteit (DigiD);
- Wet structuur uitvoeringsorganisatie werk en inkomen (Suwinet);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Grootschalige Topografie (BGT).

Hierbij blijft de jaarlijkse onafhankelijke audit door een extern auditbureau van toepassing voor DigiD en Suwinet.

De scope voor de implementatie van de BIG is, zo volledig als mogelijk aan de gestelde kaders voldoen. Het college van Burgemeester en Wethouders volgt de BIG, maar heeft de mogelijkheid om gemotiveerd af te wijken van de gestelde norm. Er is geen wettelijke verplichting tot het volgen van de BIG naast de conformering uit 2012.

Informatiebeveiliging in de praktijk

Informatiebeveiliging is tegenwoordig van cruciaal belang om de continuïteit van dienstverlening naar burgers van de gemeente Barneveld te kunnen garanderen. Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen.

Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: pasjessysteem om het gemeentehuis binnen te komen, hoe om te gaan met mobiele apparaten en wachtwoord + token voor telewerken.

De gemeente hanteert de volgende uitgangspunten; deze zijn gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIG:

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het lijnmanagement, met het College van B&W als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een continu verbeterproces. "Plan, do, check en act" vormen samen het management systeem van informatiebeveiliging.
4. De informatiebeveiligingsfunctionaris/Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
5. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

De belangrijkste acties van 2017

De gemeente Barneveld is al jaren bezig met het waarborgen van haar informatie door het inzetten van informatiebeveiliging. Om de gemeenteraad inzicht te geven is onderstaande lijst opgesteld met daarin een aantal uitgevoerde activiteiten uit 2017 opgesomd:

- Het uitvoeren van een gemeente-breed bewustwordingscampagne voor strategisch, tactisch en operationeel medewerkers. Bij de uitvoering van de bewustwordingscampagne is het college van Burgemeester & Wethouders ook bewuster gemaakt.
- Het informatiebeveiligingsbeleid is herzien en bijgesteld om te waarborgen dat de actuele missie, visie en strategie erin beschreven staat.
- Het informatiebeveiligingsplan is geactualiseerd om de prioriteiten van activiteiten te bepalen. De bepaling is in samenspraak met de gemeentesecretaris en de directeur uitgevoerd.
- Periodiek overleg met management/directie/gemeentesecretaris/college B&W voor prioriteiten te stellen en te informeren.
- De aandachtspunten implementeren die vanuit het rekenkamer onderzoek (eind 2016) zijn aangedragen.
- Normenkader toets om de huidige stand van zaken te inventariseren met betrekking tot de voortgang implementatie van de BIG. Hierbij spreekt men van een GAP-/IMPACT-analyse BIG.
- Simulatie uitgevoerd met betrekking tot een digitale aanval zoals 'ransomware'. Op basis van de simulatie zijn procedures geactualiseerd om zo doeltreffend mogelijk te zijn.
- Jaarlijkse uitwijktest van datacenter.
- Jaarlijkse test van back-up hersteltermijn.

Resultaten ENSIA in relatie tot BIG

Onderstaand worden de resultaten uit ENSIA op hoofdlijnen weergeven.

ENSIA verantwoording	Resultaat
ENSIA algemeen	Voldoende, formele vastlegging wenst aanscherping
BRP	Geslaagd zonder opmerkingen
PUN	Geslaagd zonder opmerkingen
DigiD	Geslaagd zonder opmerkingen
Suwinet	Geslaagd zonder opmerkingen
BAG	Geslaagd zonder opmerkingen
BGT	Geslaagd zonder opmerkingen

Vanaf 2012 wordt de BIG door alle Nederlandse gemeenten gehanteerd, hierdoor heeft de gemeente Barneveld veel maatregelen al voltooid. Na het uitvoeren van een GAP-/IMPACT-analyse (nulmeting) zijn er onderstaande aandachtsgebieden gedefinieerd:

Aandachtspunten	Uitleg
1. P&O	In de praktijk is er veel ingeregeld, maar formalisatie wenst aandacht. Wenselijk om vooruitgang te boeken op BIG normenkader.
2. Fysieke toegang	Verdere uitwerking binnen de organisatie n.a.v. Hoffman onderzoek en wenselijk om vooruitgang te boeken op BIG normenkader.
3. Organisatie	Verdere uitwerking van de organisatie m.b.t. het inregelen van functionarissen/overleggroepen o.a. strategisch/tactisch/operationeel overleg.
4. Privacy	Nadere samenwerking inregelen voor het waarborgen van de Algemene Verordening Gegevensbescherming (AVG) & BIG.

Activiteiten 2018

De gemeente Barneveld heeft een informatiebeveiligingsplan 2018 opgesteld waarin alle activiteiten met prioriteit zijn opgesomd. Onderstaand een kleine greep uit het gehele overzicht:

1. Procedure voor in-/uitdiensttreding nader onderzoeken.
2. Acties ondernemen n.a.v. Hoffman onderzoek fysieke beveiliging.
3. Op dit moment wordt er periodiek, minimaal 1x per kwartaal, strategisch overleg gevoerd. Aankomend jaar gaat er aandacht worden besteed om meer functionarissen in de gemeente aan te stellen als informatiebeveiligingsfunctionarissen. Hierdoor is de voorkeur uitgesproken om naast strategisch overleg ook tactisch & operationeel overleg te gaan houden als aanvulling op de bestaande werkzaamheden (geen uitbreiding van fte's).
4. De gemeente gaat verder met het borgen van de BIG normenkader en de AVG. Door middel van het formaliseren en controleren van beleidsstukken/procedures borgt de gemeente dat de informatiestukken toepasbaar en actueel blijven. Bij eventuele gebreken wordt er direct bijsturing uitgevoerd.

Appendix A: Gewaarmerkte collegeverklaring

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en SUWInet

Het college van burgemeester en wethouders van de gemeente Barneveld 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 verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de 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 (GeVS/Suwinet).

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 DigID (aansluitnummer: 1002253) en Suwinet. 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, op het openbare deel van de websites van het ministerie van BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring "bijlage 1 DigiD" blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk Ensia 2017.1) en Suwinet (bijlage 2 Suwinet met kenmerk Ensia 2017.2) geïnformeerd .

Verklaring college

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

Barneveld, 16 april 2018

burgemeester en wethouders,

H. [illegible] Leden — secretaris

dr. J.W.A. van Dijk — burgemeester

1 https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/
2 https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten
3 https://www.ensia.nl/

BKBO
Voorstraat 20
5251 CP VLIJMEN
M 06-28978955