Brief aan de leden
T.a.v. het college en de raad

Datum
7 januari 2019

Ons kenmerk
TIS/U201801170
Lbr. 19/002

Telefoon
(070) 373 8393

Bijlage(n)
2

Onderwerp
Standaardverklaring Baseline Informatiebeveiliging Overheid

Samenvatting

Informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een vernetwerkte overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Gemeenten, Rijk, waterschappen en provincies gaan daarom over op één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Voor gemeenten is 2019 voorzien als voorbereidingsjaar. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.

Met de BIO is informatiebeveiliging meer dan voorheen een zaak van de bestuurder. Als bijlage bij deze ledenbrief ontvangt u daarom ter ondersteuning ’De 10 bestuurlijke principes voor informatiebeveiliging.

Verder zend ik u ter kennisname het onlangs verschenen Dreigingsbeeld Nederlandse Gemeenten 2019 toe. In dit dreigingsbeeld worden de belangrijkste risicofactoren rond gemeentelijke informatieveiligheid geduid. Net als voorgaand jaar zijn de belangrijkste risico’s te vinden in het imago en menselijk handelen. Bestuurlijk een relevant onderwerp. Het dreigingsbeeld biedt mede in het licht van de BIO een handelingsperspectief om de belangrijkste risico’s aan te pakken. Wij adviseren u dit dreigingsbeeld met uw gemeentelijke CISO te bespreken en voor uw gemeente passende acties te initiëren.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Aan de leden

Datum
7 januari 2019

Ons kenmerk
TIS/U201801170
Lbr. 19/002

Telefoon
(070) 373 8393

Bijlage(n)
2

Onderwerp
Standaardverklaring Baseline Informatiebeveiliging Overheid

Geacht college en gemeenteraad,

Via deze weg willen wij u graag informeren over de standaardverklaring van de Baseline Informatiebeveiliging Overheid (BIO) per 1 januari 2020.

Aanleiding

In de buitengewone algemene ledenvergadering op 30 november 2018 hebben gemeenten ingestemd met het proces van standaardverklaring. Dat maakt Samen Organiseren mogelijk. Samen Organiseren is het vliegwiel voor het verbinden en versnellen van de Gezamenlijke Gemeentelijke Uitvoering (GGU). Echt samen organiseren houdt in dat gemeenten standaarden afspreken. Daarmee worden ook kosten voor individuele gemeenten bespaard (één keer ontwikkelen, 355 maal toepassen). Voor standaarden in informatiebeleid, informatietechnologie en dienstverlening hebben gemeenten het College van Dienstverleningszaken (CvD) in het leven geroepen. De BIO is de eerste standaard waarover het CvD positief advies heeft afgegeven aan het VNG Bestuur. Het bestuur heeft hier positief op gereageerd en de BIO tot standaard verklaard per 1 januari 2020.

Aanvullend zijn daarbij ook “De 10 bestuurlijke principes voor informatiebeveiliging” tot standaard verklaard die de bestuurder ondersteunen in de aansturing van informatieveiligheid. De BIO is eveneens interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO).

Informatiebeveiliging meer dan voorheen zaak van bestuurder

Informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een vernetwerkte overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Gemeenten, Rijk, waterschappen en provincies gaan daarom over op één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Voor gemeenten is 2019 voorzien als voorbereidingsjaar. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Verandering voor gemeenten: risicomanagement centraal
De BIO betekent een verandering voor gemeenten. Ten opzichte van de huidige Baseline Informatiebeveiliging Gemeenten (BIG) worden bijna 200 maatregelen niet meer genoemd. Gemeenten krijgen zo meer ruimte om voor hen op basis van het risico relevante maatregelen te treffen. De maatregelen uit de BIG die in de BIO nog wel worden genoemd gelden als verplicht voor alle overheden. De BIO positioneert de bestuurder en het management sterker dan voorheen in de rol waarin hij of zij risico-gebaseerd stuurt op het gebied van informatieveiligheid. Zij zullen hierover op het advies van de betrokken Chief Information Security Officers afspraken moeten maken. Ter ondersteuning daarbij zijn 'De 10 bestuurlijke principes voor informatiebeveiliging' vastgesteld. Ze dienen als handvatten voor dat gesprek.

De 10 bestuurlijke principes voor informatiebeveiliging:

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

Standaardisering van informatiebeveiliging
Met de vaststelling van de Gezamenlijke Gemeentelijke Uitvoering en het Jaarprogramma 2019 kiezen we er als gemeenten voor om gezamenlijk te standaardiseren in de uitvoering van beleidsarme thema's, en een nieuwe gemeenschappelijke en generieke (sectoronafhankelijke) basisinformatievoorziening te realiseren. Standaarden kunnen in belangrijke mate bijdragen aan het realiseren van gezamenlijke uitvoeringskracht en daarmee ruimte voor maatwerk op terreinen waarop gemeenten het verschil willen maken. De BIO is de eerste standaard waarover het College van Dienstverleningszaken (CvD) positief advies heeft afgegeven aan het VNG Bestuur. Het bestuur heeft hier positief op gereageerd en de BIO daarmee verbindend verklaard voor gemeenten per 1 januari 2020. De baseline is interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO).

De belangrijkste reden voor de interbestuurlijke adoptie van de BIO is het samenwerken in een vernetwerkte overheidsomgeving, waarbij we impliciet moeten kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Het bestaan van meerdere overheidsbaselines is bovendien niet efficiënt. De BIO zorgt voor een overheidsbrede standaardisatieslag en sluit aan bij de voor de markt geldende NEN-ISO 27002:2013 norm. Daarop zijn een tweetal aanvullingen op de standaard gekomen die op details ingaan, maar geen afbreuk doen aan de principes zoals deze in de NEN 2013 geformuleerd staan. Deze NEN 2013 is de meest recente basis. Als gemeente kunt u er daarmee op vertrouwen dat u én de andere overheidspartners met deze BIO aan de meest recente normen voldoet.

IBD ondersteunt ambtelijke organisatie
Voor de jaren 2018 en 2019 verantwoorden gemeenten zich nog over de BIG. Voor het jaar 2020 zal de verantwoording zijn aangepast aan de BIO. Voor de inrichting van informatiebeveiligings-maatregelen kunnen gemeenten gebruik maken van de ondersteuningsproducten van de IBD. De bestaande producten worden momenteel aangepast aan de BIO en komen in het eerste halfjaar van 2019 beschikbaar. Andere ondersteuningsproducten, zoals een quickscan, worden voor de gezamenlijke overheidslagen onder regie van het Rijk ontwikkeld en door de IBD toepasbaar gemaakt voor gemeenten. Aanvullend ontwikkelt de VNG een ondersteuningsprogramma gericht op het management en het bestuur van gemeenten.

Mocht u als bestuurder op de hoogte willen zijn van de voor uw gemeente relevante dreigingen en risico's dan kan het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020 u op weg helpen. Het dreigingsbeeld laat zien dat de belangrijkste beveiligingsrisico's niet zozeer technisch van aard zijn, maar met name liggen in de eigen organisatie (waaronder het menselijk handelen) en in de samenwerking met ketenpartners. We adviseren u hierover met uw CISO in gesprek te gaan en met deze functionaris voor uw gemeente passende acties te initiëren.

Met vriendelijke groet,

Vereniging van Nederlandse Gemeenten

J. Kriens
Algemeen directeur