Vereniging van Nederlandse Gemeenten

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

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8393		
betreft	**ons kenmerk**	**datum**
Informatiebeveiliging	BABVI/U201300696 Lbr. 13/057	6 juni 2013

Samenvatting

In september en oktober 2012 hebben wij u via ledenbrieven geïnformeerd over informatiebeveiliging in brede zin en, in aanloop naar de BALV van 12 oktober 2012, de Informatiebeveiligingsdienst voor gemeenten (kenmerken: BAVI/U201201301 en BAVI/U201201379).

Met deze ledenbrief willen wij u informeren over de actuele stand van zaken rondom de Informatiebeveiligingsdienst voor gemeenten (IBD), de ondersteuningsaanpak voor gemeenten aangaande het ICT-Beveiligingsassessment DigiD en de eerste invulling van “verplichtende zelfregulering” voor het gemeentelijke domein.

De VNG roept gemeenten voorts op om werk te maken van informatiebeveiliging door:
- de gemeentelijke organisatie voor te bereiden op het volledige aanbod van en samenwerking met de Informatiebeveiligingsdienst (IBD);
- aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten de informatiebeveiliging binnen de gemeente op orde te brengen;
- het verplichte ICT-Beveiligingsassessment DigiD, voor zover nog niet gestart, nog voor de zomer te starten en uiterlijk eind 2013 in te dienen waarmee de gemeente afsluiting van DigiD door de minister kan voorkomen.

Vereniging van Nederlandse Gemeenten

Aan de leden

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8393		
betreft	**ons kenmerk**	**Datum**
Informatiebeveiliging	BABVI/U201300696 Lbr. 13/057	6 juni 2013

Geacht college en gemeenteraad,

In september en oktober 2012 hebben wij u via ledenbrieven geïnformeerd over informatiebeveiliging in brede zin en, in aanloop naar de BALV van 12 oktober 2012, de Informatiebeveiligingsdienst voor gemeenten (kenmerken: BAVI/U201201301 en BAVI/U201201379).

Met deze ledenbrief willen wij u informeren over de actuele stand van zaken rondom de Informatiebeveiligingsdienst voor gemeenten (IBD), de ondersteuningsaanpak voor gemeenten aangaande het ICT-Beveiligingsassessment DigiD en de eerste invulling van “verplichtende zelfregulering” voor het gemeentelijke domein.

De VNG roept gemeenten voorts op om werk te maken van informatiebeveiliging door:

- de gemeentelijke organisatie voor te bereiden op het volledige aanbod van en samenwerking met de Informatiebeveiligingsdienst (IBD);
- aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten de informatiebeveiliging binnen de gemeente op orde te brengen;

het verplichte ICT-Beveiligingsassessment DigiD, voor zover nog niet gestart, nog voor de zomer te starten en uiterlijk eind 2013 in te dienen waarmee de gemeente afsluiting van DigiD door de minister kan voorkomen.

Informatiebeveiligingsdienst voor gemeenten
Burgers en bedrijven moeten kunnen vertrouwen op de dienstverlening van de gemeente als de meest nabije overheid. Nu meer en meer dienstverlening en processen langs digitale weg plaatsvinden, en ICT daarmee wezenlijk onderdeel is van de vitale infrastructuur, is informatiebeveiliging van steeds groter belang. DigiNotar, Lektober, het Dorifel/Citadel incident en recent de DDoS-aanvallen op websites laten zien dat dienstverlenende organisaties, dus ook gemeenten, uitermate kwetsbaar zijn als het gaat om digitale dienstverlening. Continuïteit van dienstverlening, de bescherming van (persoonsgegevens van) burgers en het betrouwbaarheidsimago van gemeenten zijn in het geding.
Daarom hebben gemeenten tijdens de BALV van 12 oktober 2012 ingestemd met de propositie voor de Informatiebeveiligingsdienst voor gemeenten (IBD) zoals deze door VNG en KING was voorgesteld. Voor de IBD is jaarlijks € 2 miljoen beschikbaar gesteld middels een uitname uit het gemeentefonds.
Eind 2012 heeft de IBD een kwartiermakersfase doorlopen en sinds 1 januari 2013 is de IBD operationeel. Onder meer met een helpdesk waar alle gemeenten incidenten op het vlak van informatiebeveiliging kunnen melden en ondersteuning krijgen bij de oplossing ervan. De IBD verricht deze werkzaamheden in nauwe samenwerking met onder meer het Nationaal Cyber Security Centrum (NCSC) en leveranciers.

De doelstelling van de IBD is echter breder dan coördineren van het oplossen van informatiebeveiligingsincidenten, de IBD richt zich in de kern op het vergroten van de weerbaarheid van gemeenten op het gebied van informatiebeveiliging. De IBD zal daarom kennisdeling initiëren en stimuleren en verder worden ingericht met activiteiten gericht op bewustwording en preventie, detectie en coördinatie van incidenten.
Tevens zal de IBD gemeenten gerichte expertise en generieke, projectmatige ondersteuning bieden. Vanuit deze ondersteuning is inmiddels een eerste product opgeleverd: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Deze Baseline, die samen met gemeenten is opgesteld, is een directe afgeleide van de Baseline Informatiebeveiliging Rijksdienst (BIR) en biedt de gemeente handvatten om de ISO-normen voor informatiebeveiliging stapsgewijs te implementeren. Zowel op strategisch als op tactisch niveau. De BIG is voor gemeenten te downloaden via de website van KING (https://new.kinggemeenten.nl/informatiebeveiliging).

Tot 2015 zal de dienstverlening van de IBD zich fasegewijs ontwikkelen tot een volwaardige positie in 2015. Hierbij is een stapsgewijze opschaling in het aanbod naar steeds meer gemeenten randvoorwaardelijk voor het op lange termijn succesvol inrichten van deze IBD-dienstverlening. Het vergt bovendien een actieve houding van de gemeente om basisinformatie op ICT-vlak te delen met de IBD en de organisatie zodanig in te richten dat ze het volledige aanbod van de IBD kan gebruiken. De IBD informeert gemeenten hierover binnenkort met concrete details.

ICT beveiligingsassessments DigiD
In 2012 heeft toenmalig minister Spies van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de maatregel aangekondigd dat alle gemeenten jaarlijks een ICT-

Beveiligingsassessment DigiD moeten uitvoeren. Dit om de veiligheid van koppelingen met DigiD, hét digitale authenticatiemiddel voor de overheid en dienstverleners met een publieke taak, te borgen. En zo het vertrouwen van burgers in het digitaal regelen van hun zaken bij gemeenten via DigiD te behouden.

De gemeente is in alle gevallen zelf verantwoordelijk voor het inleveren van de auditrapportage bij Logius, de beheerder van DigiD. Ook indien de gemeente taken als bijvoorbeeld hosting heeft uitbesteed aan een leverancier, of gebruikt maakt van een SaaS oplossing, ligt de verantwoordelijkheid voor het afronden en indienen van de rapportage bij de gemeente. De minister heeft het recht een organisatie die het assessment niet heeft uitgevoerd óf het assessment onvoldoende heeft doorstaan, van DigiD af te sluiten

In opdracht van de VNG en gefinancierd door BZK ondersteunt KING/IBD gemeenten bij de ICT Beveiligingsassessments DigiD. De VNG heeft onlangs, in overleg met het ministerie van BZK, bereikt dat deze ondersteuning tot eind 2013 wordt verlengd.
In veel gevallen zijn gemeenten, in meer of mindere mate, afhankelijk van leveranciers. Vanuit het ondersteuningsproject worden de leveranciers daarom benaderd en gestimuleerd om aan de gestelde eisen te voldoen, en dit te delen met gemeenten. De samenwerkingsconvenanten die KING met de leveranciers heeft zijn hierop uitgebreid met een addendum voor het ICT-Beveiligingsassessment DigiD welke inmiddels door dertien leveranciers is ondertekend.
Daarnaast wordt vanuit het ondersteuningsproject een vijftal koploper-gemeenten begeleid om nog voor de zomer het assessment te doorlopen en een audit-rapportage in te dienen. De ervaringen van deze gemeenten, en de wijze van afhandeling van de ingediende rapportages door de minister, zal vanuit het ondersteuningsprogramma met de overige gemeenten worden gedeeld.

Uit de eerder uitgevoerde impactanalyse, en de ervaringen van gemeenten blijkt dat, om de gestelde deadline van eind 2013 te halen, het van belang is om nog voor de zomer gestart te zijn. Vanuit de voortgangsinformatie van het ondersteuningsprogramma blijkt dat de meeste gemeenten inmiddels zijn gestart met het assessment. Er zijn echter ook gemeenten die nog niet zijn gestart.
De VNG wijst gemeenten op het risico van afsluiting en wil hierbij tevens het belang van tijdig starten met (de voorbereidingen op) het assessment benadrukken. Voor uw gemeente, voor het imago van het gemeentelijke domein en natuurlijk voor het DigiD-stelsel zelf.

Voor eventuele vragen over de IBD, de BIG of het ICT-Beveiligingsassessment DigiD kan contact worden opgenomen met de helpdesk van de Informatiebeveiligingsdienst voor gemeenten: 070-373 8011 of via het e-mailadres IBD@kinggemeenten.nl.

Verplichtende zelfregulering
Gemeenten zijn verantwoordelijk voor het op orde hebben van de informatiebeveiliging binnen de eigen gemeente. Dit zullen en mogen burgers en bedrijven, maar ook de ketenpartners, van de gemeente verwachten. Niet voor niets namen gemeenten daarom in 2012 het initiatief voor de oprichting van de IBD.
De gemeente moet scherp zijn op de potentiële risico's die het loopt en daarop adequate (preventieve) maatregelen nemen. De Informatiebeveiligingsdienst voor gemeenten zal gemeenten hierbij, middels de eerder genoemde activiteiten, ondersteunen. In alle gevallen vanuit het perspectief van de eigen verantwoordelijkheid.

De Onderzoeksraad Voor Veiligheid heeft, naar aanleiding van DigiNotar, onder andere geconstateerd dat informatiebeveiliging de bestuurlijke tafel te weinig bereikt. Op 13 februari heeft de Bestuurlijke Regiegroep Dienstverlening en e-Overheid, een interbestuurlijk overleg waar de VNG aan deelneemt, besloten tot instelling van de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Deze taskforce, gefinancierd door het ministerie van BZK, zal alle overheidslagen de komende twee jaar ondersteunen bij zelfregulering van informatiebeveiliging. Indien zelfregulering niet voldoende van de grond komt, dan volgt mogelijk wetgeving.

Gemeenten werken, middels VNG en de IBD, samen met de Taskforce BID om te komen tot deze 'verplichtende zelfregulering' voor het gemeentelijke domein. Uitgangspunt hierbij is dat wordt aangesloten op de initiatieven die gemeenten individueel en als collectief al in gang hebben gezet. Voor de uitwerking van verplichtende zelfregulering zijn in maart drie bijeenkomsten georganiseerd: zowel met bestuurders, top-managers en informatiebeveiligers als een interbestuurlijke bijeenkomst waar ervaringen met en door andere bestuurslagen werden gedeeld. De VNG ziet de volgende lijn met betrekking tot zelfregulering voor het gemeentelijke domein, deze lijn wordt de komende tijd nader uitgewerkt.

1. Een gemeenschappelijk normenkader moet als basis dienen. Bepaald moet worden of de eerder genoemde Baseline Informatiebeveiliging Nederlandse Gemeenten dit gemeenschappelijke normenkader kan worden.
2. Lokaal moet informatiebeveiligingsbeleid worden vastgesteld. Met gebruik van het gemeenschappelijke normenkader maakt de gemeente een afweging en prioritering, onderbouwd vanuit een eigen nul-meting.
3. Borging moet plaats vinden door zelfregulering vorm te geven middels een interne cyclus, door transparantie, collegiale toetsing en een vorm van extern toezicht.

Een groot deel van de aandacht rondom de opdracht tot zelfregulering moet echter worden gevestigd op het vlak van communicatie en bewustwording. Hier zal de Taskforce BID dan ook prioriteit van maken middels bijeenkomsten bij bestaande gremia, opleidingen en borgingsmechanismen. De Taskforce kent op dit onderdeel een relatie met de IBD die ook bewustwording stimuleert: IBD is hierbij met name operationeel gericht, de Taskforce BID bestuurlijk. In nauwe afstemming wordt geborgd dat de activiteiten elkaar versterken.

Een laatste belangrijke opbrengst vanuit de bijeenkomsten in maart is de oproep om toe te werken naar het verlagen van de auditlast voor gemeenten. De mogelijkheden hiertoe worden door VNG, KING/IBD en de Taskforce BID op interbestuurlijk niveau nader verkend.

Hoogachtend,

Vereniging van Nederlandse Gemeenten

J. Kriens
Voorzitter directieraad

Deze ledenbrief staat ook op www.vng.nl onder brieven.