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**
Ledenbrief stand van zaken informatiebeveiliging	BABVI/U201201301 Lbr. 12/081	6 september 2012

Samenvatting

Op 7 februari jongstleden informeerden wij u via een ledenbrief (kenmerk: BABVI/U201200230) over de aangescherpte beveiligingseisen DigiD en de ondersteuning van VNG en KING. Het onderwerp informatiebeveiliging werd recent opnieuw actueel toen het Dorifel/Citadel virus toesloeg, ook bij een aantal gemeenten.

De onderzoeken op het gebied van informatiebeveiliging die wij aankondigden zijn opgeleverd. Het betreft het onderzoek van de Onderzoeksraad voor Veiligheid "Het DigiNotarincident", de gemeentebrede aanpak ICT beveiliging en de impactanalyse ICT beveiligingsassessments DigiD. Deze brief informeert u over de uitkomsten en vervolgstappen.

De aanbevelingen van 7 februari, blijven onverminderd van kracht. Inmiddels heeft u, rondom de ICT beveiligingsassessments DigiD, ook een nadere brief van de Minister van BZK ontvangen (gedateerd 26 juni 2012) waarin zij de urgentie voor gemeenten om te handelen, nogmaals onderstreept. De Minister van BZK roept specifiek op om zoveel mogelijk stappen van het stappenplan van Logius al in 2012 af te ronden. Hiermee toont de Minister begrip voor het feit dat niet alle gemeenten het ICT beveiligingsassessment in 2012 volledig kunnen afronden, en deelt de Minister tegelijkertijd de urgentie die de Tweede Kamer met de Minister op dit onderwerp voelt.

De VNG deelt dit gevoel voor urgentie en sluit zich bij deze oproep aan. De VNG is echter van mening dat, vanuit de verantwoordelijkheid van de gemeenten, er meer nodig is dan alleen het ICT beveiligingsassessment DigiD om te komen tot een adequate informatiebeveiliging. Denk hierbij ook aan de brief die u ontving van de staatsecretaris SZW over de informatiebeveiliging in het SZW domein. Mede daarom vragen wij u uw alertheid op dit onderwerp en uw medewerking en steun voor de gezamenlijke initiatieven die voortvloeien uit de onderzoeken.

Aan de leden

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8393		
betreft	**ons kenmerk**	**datum**
Ledenbrief stand van zaken informatiebeveiliging	BABVI/U201201301 Lbr. 12/081	6 september 2012

Geacht college en gemeenteraad,

DigiNotar, Lektober en recent het Dorifel/Citadel incident hebben laten zien dat gemeenten kwetsbaar zijn in hun informatiebeveiliging. Continuïteit van dienstverlening, de bescherming van (persoonsgegevens van) burgers en het imago van gemeenten zijn in het geding. Het recente rapport over het DigiNotarincident van de Onderzoeksraad voor Veiligheid schetst, onder andere, de situatie bij gemeenten en analyseert de aard van het probleem. Het worden toegerust op het nemen van verantwoordelijkheid, en de voorwaarden scheppen om digitale veiligheid te kunnen beheersen, staan centraal. Dit sluit aan bij onze ambities zoals geformuleerd in "@genda 2015: slimme verbindingen gemeentelijke agenda informatiebeleid".

In verschillende domeinen staat informatiebeveiliging hoog op de agenda. Dit raakt gemeenten. De GBA audits, maar ook op het gebied van Sociale Zaken en het ICT-beveiligingsassessment DigiD is sprake van toegenomen aandacht voor dit dossier. Ook de brief van (demissionair) staatssecretaris De Krom van Sociale Zaken en Werkgelegenheid (SZW), van 8 juni jl., die gemeenten oproept kritisch te kijken naar de beveiliging van persoonsgegevens sociale zekerheid bij gebruik Suwinet, getuigt hiervan. Trendrapporten, de Nationale Cyber Security strategie, en de voorziene meldplicht bij datalekken leiden tot de verwachting dat het dossier nog volop ontwikkelt.

Onderzoeksraad voor de Veiligheid: "Het DigiNotarincident"
Het DigiNotar incident is onderwerp van onderzoek geweest van de Onderzoeksraad voor Veiligheid. In juni 2012 presenteerde de Onderzoeksraad zijn advies. Onderdeel van de onderliggende analyse is onderzoek onder gemeenten. Het beeld dat wordt geschetst, wordt herkend door de VNG en sluit aan bij de bevindingen uit onderzoeken van de VNG zelf.

De Onderzoeksraad komt tot een drietal aanbevelingen:

1) "*Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK)* : Zorg dat bestuurders van alle overheidsorganisaties hun verantwoordelijkheid nemen voor het beheersen van digitale veiligheid" (p.86);
   Hierbij gaat het vooral om: het doordringen van het belang van digitale veiligheid en hiertoe het verwerven van voldoende inzicht en vaardigheden om actief sturing te kunnen

geven aan de beheersing van digitale veiligheid in hun organisatie; en het afleggen van verantwoordelijkheid.

2) *"Aan de minister van BZK en de minister van Veiligheid en Justitie (VenJ)*: Schep voorwaarden zodat overheidsorganisaties hun digitale veiligheid systematisch beheersen" (p.86);
Betreft het naleven van normen die gezamenlijk een kader bieden voor systematische digitale veiligheidszorg en daarnaast het besteden van aandacht aan het voorbereid zijn op, en het herstellen van schade van, digitale incidenten.

3) "*Aan de minister van BZK, minister van EL&I*: Realiseer een veiliger uitgifte en gebruik van digitale certificaten". (p.87)
Betreft wijzigingen in de rol van OPTA en Logius en een cultuuromslag in de certificaatdienstverlening.

Gemeentebrede aanpak ICT beveiliging: de gemeentelijke Informatiebeveiligingsdienst
Onderzoek van VNG en KING, in de vorm van een gatewayreview en in samenwerking met gemeenten, landelijke overheid en diverse experts, geeft aan dat haast gemaakt dient te worden met het opzetten van een structurele ondersteuning van gemeenten bij hun informatiebeveiliging. Het onderzoek suggereert ondersteuning in de vorm van een (gemeentelijke) Informatiebeveiligingsdienst.

VNG en KING hebben op basis van dit onderzoek, samen met gemeenten, een propositie opgesteld voor een gemeentelijke Informatiebeveiligingsdienst (IBD). Het bestuur van de VNG heeft op basis van deze propositie op 28 juni jl. besloten tot het starten van een kwartiermakerfase voor de oprichting van de IBD die alle gemeenten generiek ondersteunt. Deze fase loopt tot eind 2012. Uitgangspunt is dat alle gemeenten gebruik (kunnen) maken van de IBD. De dienstverlening is generiek van aard. De IBD ondersteunt individuele gemeenten en daarmee ook een collectief belang, namelijk de slagvaardigheid waarmee gemeenten werken aan informatiebeveiliging. Dit borgt het imago van gemeenten.

De IBD, onder opdrachtgeverschap van de VNG en voorzien als een functie van KING, ondersteunt gemeenten in het nemen van hun verantwoordelijkheid op het gebied van informatiebeveiliging. De IBD doet dit zonder deze verantwoordelijkheid over te nemen. De IBD heeft als missie om IT & informatie gerelateerde veiligheidsincidenten die kunnen optreden bij gemeenten in samenwerking met haar deelnemers, partners en leveranciers, te bestrijden en waar mogelijk te voorkomen.

De IBD werkt daartoe langs een drietal lijnen, daarbij bestaande kennis en ervaring steeds aanvullend vanuit het gemeenteperspectief, te weten: detectie en coördinatie bij het oplossen van incidenten; preventie en; kennisdeling/expertise. De IBD dupliceert geen taken, maakt optimaal gebruik van bestaande kennis, en is 'lean en mean' ingericht. Een belangrijke (kennis)partner van de IBD zal het Nationaal Cyber Security Centrum (NCSC) zijn.

Onderdeel van de kwartiermakerfase is besluitvorming over de wijze van structurele financiering. Het VNG bestuur legt dit onderwerp voor aan de Buitengewone Algemene Ledenvergadering van de VNG in oktober 2012.

Uitgelicht: beveiligingsassessments DigiD

Naast deze algemene ontwikkelingen vraagt op dit moment specifiek de beveiliging van DigiD aandacht. Ook de minister van BZK en de Tweede Kamer hebben aangedrongen de kwaliteit van de ICT-beveiliging van DigiD gebruikende organisaties een impuls te geven. De minister van BZK heeft concrete maatregelen aangekondigd om de kwaliteit te verbeteren. Hierover heeft zij u een brief gestuurd (gedateerd 26 juni 2012). Alle DigiD-gebruikende organisaties dienen een ICT-beveiligingsassessment DigiD uit te voeren. Deze moeten voldoen aan de norm die hiervoor is opgesteld door Logius, de beheerder van DigiD, en die is gebaseerd op de beveiligingsrichtlijn webapplicaties van het NCSC.

KING is in opdracht van BZK en VNG eind maart jl. gestart met een analyse om de impact van deze ICT-beveiligingsassessments voor gemeenten in kaart te brengen en een ondersteuningsaanpak voor gemeenten op te stellen. Deze impactanalyse is afgerond. Negen gemeenten, te weten Apeldoorn, Doetinchem, Eindhoven, Heerhugowaard, Lisse, Nieuwegein, Zuidplas, Zutphen en Zwolle, hun leveranciers, een aantal geselecteerde audit- en pentestorganisaties en andere betrokken partijen zoals BZK/Logius, de beroepsorganisatie van IT-auditors (NOREA), en NCSC, hebben eensgezind samengewerkt om op basis van de aanwezige informatie de impact van de ICT-beveiligingsassessment DigiD op gemeenten te onderzoeken.

De impact van de voorgeschreven ICT-beveiligingsassessments DigiD op gemeenten is fors. Zowel wat betreft voorbereiding, uitvoering en nazorg. Het gemeentelijke applicatielandschap is complex en moet in kaart worden gebracht. Bij het uitvoeren van de assessments zijn veel partijen betrokken, waaronder de gemeente zelf, maar ook haar leveranciers, en de audit- en pentestpartijen. Het begeleiden en opdrachtgeverschap en de voorbereiding vraagt het nodige in deze fase evenals het afhandelen van benodigde formele goedkeuringen. Het is goed mogelijk dat de assessments leiden tot aanvullende werkzaamheden/ wijzigingen aan de bestaande ICT omgeving. De gemeente zal moeten investeren in eigen activiteiten bij het uitvoeren van de voorbereidingen. Ook het inhuren van auditors, het laten uitvoeren van een pentest, en het oplossen van de bevindingen uit de assessments, zal investeringen vragen.

Uit de impactanalyse is gebleken dat een gestandaardiseerde centrale ondersteuningsaanpak voordelen biedt. Bundeling van werkzaamheden bij gemeenten en leveranciers is mogelijk, wat geld en tijd bespaart. Dit ondersteuningsaanbod is nader uitgewerkt en inmiddels zijn de voorbereidende werkzaamheden gestart. Nadere informatie treft u aan op de website van VNG en KING.

Tot slot
Graag maken wij u attent op de volgende initiatieven:

- Dit najaar organiseert de VNG eAwarenessdiners. Deze bijeenkomsten vinden plaats om u te informeren over hoe u informatiebeleid kunt vormgeven en kunt aanwenden voor de realisatie van uw beleidsdoelstellingen. U ontvangt voor deze diners een uitnodiging. U bent van harte uitgenodigd zich aan te melden, informatiebeveiliging is één van de onderwerpen die aan de orde komt.
- Vraag en Antwoord Informatiebeveiliging – VNG en KING hebben de belangrijkste *Frequently Asked Questions* gebundeld op een website: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/informatiebeveiliging/vraag-en-antwoord.

Als u vragen heeft naar aanleiding van deze brief kunt contact opnemen met het VNG informatiecentrum via informatiecentrum@vng.nl of telefonisch op 070 – 3738393.

Links:
Het DigiNotarincident, Onderzoeksraad voor Veiligheid:
http://www.onderzoeksraad.nl/docs/rapporten/Rapport_Diginotar_NL_web_def_20062012.pdf
Gemeentelijke Informatiebeveiligingsdienst:
http://www.vng.nl/eCache/DEF/1/16/504.html
Impactanalyse ICT-assessments DigiD:
http://www.vng.nl/eCache/DEF/1/16/680.html

Hoogachtend,
Vereniging van Nederlandse Gemeenten

mr. R.J.J.M. Pans
voorzitter directieraad

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