Vereniging van Nederlandse Gemeenten

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

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8020		0
Betreft	**ons kenmerk**	**datum**
DigiD en ICT-beveiliging	BABVI/U201200230 Lbr. 12/015	07 februari 2012

Samenvatting
De Diginotar-crisis en de computer-hacks tijdens Lektober hebben de kwetsbaarheid van ICT systemen nadrukkelijk getoond. Ook gemeenten blijken kwetsbaar te zijn.

In deze brief informeren wij u welke ondersteuning de VNG en KING aan gemeenten willen gaan bieden om de informatiebeveiliging te verbeteren. Daarnaast geven wij aan wat u zelf kunt doen en welke maatregelen de minister ten aanzien van de veiligheid van DigiD heeft aangekondigd.

Wat kunt u op korte termijn doen?
Om de informatiebeveiliging van uw gemeente te verbeteren adviseren wij u de volgende maatregelen te nemen:

- Neem kennis van de NCSC "*ICT-beveiligingsrichtlijn voor webapplicaties*" en de ISO 27001/27002 beveiligingsstandaard. Ga na in hoeverre uw eigen beveiligingsbeleid voldoet aan deze richtlijnen
- Neem contact op met uw EDP auditor om na te gaan in hoeverre uw gemeente voldoet aan de geldende informatiebeveiligingsnormen en welke maatregelen genomen kunnen worden (of noodzakelijk zijn) om deze te verbeteren
- Wacht de nadere informatie van Logius af, met betrekking tot de ICT-assessments van systemen die gebruik maken van DigiD
- Geef uw suggesties, aanbevelingen of opmerkingen door ten aanzien van de collectieve ondersteuning die VNG en KING willen organiseren om de informatiebeveiliging van gemeenten te verbeteren. U kunt dit aan de VNG doorgeven.

Over de uitkomsten van de in de brief genoemde onderzoeken zullen wij u zo spoedig mogelijk nader informeren.

Vereniging van
Nederlandse Gemeenten

Aan de leden

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8020		0
betreft	**ons kenmerk**	**datum**
DigiD en ICT-beveiliging	BABVI/U201200230	07 februari 2012
	Lbr. 12/015	

Geacht college en gemeenteraad,

De Diginotar-crisis en de computer-hacks tijdens Lektober hebben de kwetsbaarheid van ICT systemen nadrukkelijk getoond. Ook gemeenten blijken kwetsbaar te zijn.

In deze brief informeren wij u welke ondersteuning de VNG en KING aan gemeenten willen gaan bieden om de informatiebeveiliging te verbeteren. Daarnaast geven wij aan wat u zelf kunt doen om uw ICT-beveiliging te verbeteren en welke maatregelen de minister ten aanzien van de veiligheid van DigiD heeft aangekondigd.

Relevante richtlijnen voor ICT-beveiliging
De beveiliging van gemeentelijke ICT-systemen en informatie is uw eigen verantwoordelijkheid. Op 6 februari heeft het NCSC (Nationaal Cyber Security Center, voorheen Govcert.nl) de "*ICT-beveiligingsrichtlijn voor webapplicaties*" gepubliceerd.[1]
Daarnaast geldt de internationale beveiligingsstandaard ISO 27001/27002. deze standaard geeft een opsomming van eisen die u aan uw informatiebeveiliging kunt stellen, en geeft daarnaast een beschrijving hoe u een goede beveiliging procesmatig kunt inrichten. De ISO standaard is door het College Standaardisatie vastgesteld, en geldt voor alle Nederlandse overheden als een verplichting, op basis van pas-toe-of-leg-uit.

Wij adviseren u om uw eigen gemeentelijke websites en uw infomatiebeveiligingsbeleid te toetsen aan de richtlijn van het NCSC en de ISO beveiligingsstandaard.

---

[1] De richtlijn kunt u downloaden op https://www.ncsc.nl/actueel/nieuwsberichten/ict--beveiligingsrichtlijnen.html

Gefaseerde aanpak beveiliging DigiD-keten

De beheerder van DigiD (Logius), maakt in de loop van februari bekend op welke manier de bovengenoemde richtlijn van NCSC als norm gehandhaafd gaat worden voor overheidswebsites, die DigiD gebruiken.

Eerder heeft de minister van BZK in een brief aan de Tweede Kamer[2] gemeld dat alle partijen vóór 1 april 2012 een ICT-beveiligingsassessment uitgevoerd moesten hebben. De VNG heeft bij de minister aangegeven dat voor de gemeenten deze termijn onhaalbaar is, onder andere omdat de norm nog niet is vastgesteld. Op basis van een concept van de NCSC-beveiligingsrichtlijn heeft KING geconcludeerd dat de benodigde aanpassingen en de doorlooptijd bij gemeenten niet onderschat moeten worden. Daarop is in overleg met het ministerie besloten tot een gefaseerde aanpak. De minister heeft deze aanpak gemeld aan de Tweede Kamer.[3]

De eerste stap is dat KING de eerste helft van dit jaar bij een beperkt aantal gemeenten en leveranciers een impactanalyse uitvoert. De uitkomsten hiervan bieden inzicht in de inspanning die vanuit gemeenten nodig is om aan de norm te voldoen. Daarnaast geeft het input voor een gestandaardiseerde aanpak voor ICT-beveiligingassessments bij gemeenten.

De volgende stap is dat alle gemeenten zelf een assessment dienen uit te voeren op basis van de door Logius vastgestelde norm. Elke gemeente dient het beveiligingsassessment uit te laten voeren onder verantwoordelijkheid van een Register EDP-auditor. Gemeenten met een eigen Register EDP-auditor in dienst, kunnen een zogeheten *self-assessment* uitvoeren. De gemeente dient vervolgens de conclusies van de assessment aan Logius op te leveren.

Uiterlijk eind 2013 moeten de gemeenten aan de norm voldoen.

In de loop van februari zal Logius u nader informeren over de norm waaraan u dient te voldoen en de manier waarop de ICT-beveiligingsassessments uitgevoerd moeten worden. VNG en KING zullen de gemeenten te zijner tijd ondersteunen bij het uitvoeren van de assessments, bijvoorbeeld door middel van een helpdesk.

Onderzoek naar gemeentebrede aanpak ICT-beveiliging

Naar aanleiding van de Diginotar-crisis en Lektober heeft de VNG samen met KING de ICT-beveiliging bij gemeenten geanalyseerd. Voor het behoud van het vertrouwen van de burger in de kwaliteit van gemeenten en (elektronische) dienstverlening is het van belang dat adequate maatregelen worden genomen om de vertrouwelijkheid van (persoons)gegevens te waarborgen.

---

[2] Tweede Kamer 26643-193, Lekken in een aantal gemeentelijke websites, 11 oktober 2012

[3] Zie http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/kamerstukken/2012/02/03/kamerbrief-over-ict-beveiligingsassessments-bij-digid-gebruikende-organisaties.html

Diverse gemeenten hebben de VNG gevraagd of het mogelijk is om collectieve ondersteuning te organiseren bij het verbeteren van de informatiebeveiliging. De VNG heeft daarop de contouren verkend van een ondersteuningsaanpak voor informatiebeveiliging bij gemeenten. Daarbij zijn verschillende gemeenten, leveranciers en ICT-deskundigen betrokken. De conclusies zijn dat de gemeentelijke ICT kwetsbaar is, dat er mogelijkheden voor verbetering zijn en dat er bij gemeenten behoefte is aan een gecoördineerde en gestandaardiseerde aanpak.

De VNG en KING doen op dit moment via de gezaghebbende Gatewaymethode nader onderzoek naar hoe een dergelijke ondersteuningsaanpak voor gemeenten vorm kan krijgen. Onderwerpen die in het onderzoek aan de orde komen zijn hoe gemeenten effectief gesignaleerd kunnen worden bij het optreden van beveiligingsincidenten, wat de rol van VNG en KING is in het ondersteunen van gemeenten in het oplossen van die incidenten en op welke manier VNG en KING gemeenten structureel kunnen ondersteunen bij het verbeteren van hun informatie-beveiliging. De resultaten van het onderzoek zullen in de tweede helft van maart gereed zijn, en dan aan u worden toegezonden.

Follow-up Diginotar

De Diginotar-crisis in september 2011 heeft voor veel overheden als een wake-up call gewerkt. Door de crisis is duidelijk geworden hoezeer de gemeente in (elektronische) ketens is verweven met andere organisaties, en hoe kwetsbaar die ketens zijn. Daarnaast is gebleken dat aan de gangbare wijze van beveiliging (middels zogeheten PKI-certificaten) risico's verbonden zijn.

De Onderzoeksraad voor Veiligheid doet onderzoek naar de oorzaken en gevolgen van de inbraak in de computersystemen van Diginotar. Het onderzoek richt zich op de vraag hoe overheden de digitale veiligheid bestuurlijk en organisatorisch kunnen waarborgen. Deelaspecten van het onderzoek richten zich op het voorval bij Diginotar, de werking van het PKI-overheid certificaten-stelsel en een brede verkenning van de wijze waarop overheden - waaronder gemeenten - digitale informatiebeveiliging hebben georganiseerd en uitvoeren.
VNG en KING zijn bij het onderzoek betrokken. Op initiatief van de Onderzoeksraad worden twee rondetafelbijeenkomsten georganiseerd waaraan een aantal gemeenten deelneemt. Publicatie van het rapport is voorzien voor de zomer van 2012.

Wat kunt u op korte termijn doen?

Om de informatiebeveiliging van uw gemeente te verbeteren adviseren wij u:

- Kennis te nemen van de NCSC "*ICT-beveiligingsrichtlijn voor webapplicaties*" en de ISO 27001/27002 beveiligingsstandaard. Ga na in hoeverre uw eigen beveiligingsbeleid voldoet aan deze richtlijnen
- Contact op te nemen met uw EDP auditor om na te gaan in hoeverre uw gemeente voldoet aan de geldende informatiebeveiligingsnormen en welke maatregelen genomen kunnen worden (of noodzakelijk zijn) om deze te verbeteren
- De nadere informatie af te wachten van Logius, met betrekking tot de ICT-assessments van systemen die gebruik maken va DigiD

- U kunt uw suggesties, aanbevelingen of opmerkingen ten aanzien van de collectieve ondersteuning die VNG en KING willen organiseren om de informatiebeveiliging van gemeenten te verbeteren, aan de VNG doorgeven.

Vragen
Als u vragen heeft over het vervolg van de ICT-beveiligingsassessments, het voorgenomen VNG en KING onderzoek of andere punten naar aanleiding van deze brief kunt contact opnemen met het VNG informatiecentrum op informatiecentrum@vng.nl of telefonisch op 070 – 3738393.

Hoogachtend,
Vereniging van Nederlandse Gemeenten

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

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