

Adviezen in verband met de gemeenteraadsverkiezingen

Op 21 maart zijn in 334 gemeenten de gemeenteraadsverkiezingen. Ook wordt op deze dagen het raadgevend referendum over de Wet op de Inlichtingen en Veiligheidsdiensten gehouden. De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft op 17 december een circulaire¹ aan alle gemeenten verzonden over de verkiezingen en het referendum.

In aanloop naar de Tweede Kamerverkiezing van maart 2017 heeft het kabinet een analyse gemaakt van de kwetsbaarheden in het verkiezingsproces. Voor gemeenten gelden een aantal generieke kwetsbaarheden in de eigen organisatie en in de processen die worden ingericht voor de verkiezingen (weergegeven in sectie A en B van dit advies). In de afgelopen periode is veel aandacht geweest voor de integriteit van verkiezingen, vooral ingegeven door mogelijke buitenlandse inmenging in de presidentsverkiezingen in de Verenigde Staten. Dit leidde tot vragen over de beveiliging van de verkiezingen en het verkiezingsproces in Nederland. De IBD geeft gemeenten daarom in verband met de gemeenteraadsverkiezingen enkele adviezen in lijn met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Generieke kwetsbaarheden

A1. Spionage en ondermijning

Staatelijke actoren en beroepscriminelen proberen zich mogelijk toegang te verschaffen tot informatie van en personen binnen het lokale bestuur. Er is op dit moment geen indicatie van een verhoogde dreiging rondom de verkiezingen. De NCTV heeft in samenwerking met de AIVD een handleiding ontwikkeld om zelf de kwetsbaarheid voor spionage vast te stellen en de weerbaarheid te verhogen.² In verband met specifieke digitale dreigingen hebben de AIVD en de MIVD de brochure 'Bent u zich bewust van de risico's van cyberspionage?'³ uitgebracht voor bestuurders en ICT-beveiligers. Om de weerbaarheid tegen ondermijning te verhogen heeft de VNG een ondersteuningspakket ontwikkeld met praktische tips voor gemeenten.⁴

A2. Integriteit van (aankomend) politici

In het openbaar bestuur is integriteit een belangrijk thema. Dit is niet voor niets. Dat individuele bestuurders, raadsleden en overheidsorganisaties geloofwaardig zijn, en goed functioneren is essentieel voor het vertrouwen in de overheid als geheel.⁵ De handreiking integriteit politieke ambtsdragers bij gemeenten, provincies en waterschappen⁶ bevat modellen voor gedragscodes en praktische aanbevelingen om integriteitsschendingen zoveel als mogelijk te voorkomen.

A3. Beïnvloeding

De beïnvloeding van kiezers met gerichte digitale middelen is zorgelijk. Door bijvoorbeeld gebruik te maken van data kunnen ongevraagd campagnes op bepaalde personen worden gericht. Dat stelt een commissie die het politieke systeem in Nederland doorlicht, onder leiding van Johan Remkes.⁷

Gemeenten kunnen bij een vermoeden van ongewenste beïnvloeding melding maken bij het medium waarop de informatie staat gepubliceerd. Meer informatie over het melden van misbruik op populaire (sociale) media treft u via de volgende links:

- Facebook: https://nl-nl.facebook.com/help/1753719584844061?helpref=hc_global_nav
- Twitter: <https://help.twitter.com/nl/safety-and-security/report-abusive-behavior>
- Instagram: <https://help.instagram.com/165828726894770>
- Google: <https://support.google.com/sites/answer/116262?hl=en>

Meld misbruik en vermoeden van beïnvloeding bij de IBD, zie ook punt D. De IBD kan daarmee op basis van meldingen andere gemeenten waarschuwen als dit noodzakelijk is. Daarnaast kunt u als gemeente aangifte doen bij de politie via dit formulier: <https://www.politie.nl/aangifte-of-melding-doen/meldformulier.html?sid=c1d02db9-dba7-48fb-be0d-5c6a5f016199>.

Procesinrichting

B1. Integriteit van het kiezersbestand

De IBD heeft gemeenten bij de Tweede Kamerverkiezingen in samenwerking met de verwerkende toeleverancier gewezen op aandachtspunten rond de beveiliging van gegevens van kiesgerechtigden. De IBD raadt aan om de beveiligingsinstructies van de leverancier strikt op te volgen.

B2. Instructies gebruik ondersteunende software

In de circulaire van het ministerie van BZK worden specifieke instructies gegeven over het gebruik van ondersteunende software (OSV) en de overdracht van de uitslag⁸:

- Deze dient alleen op standalone computers te worden gebruikt;
- De integriteit van de software dient te worden gecontroleerd door middel van de hash-code die de gemeente van de Kiesraad heeft ontvangen;
- De gegevens die nodig zijn voor het berekenen van de uitslag moeten twee maal en door verschillende personen in OSV worden ingevoerd;



- Net als bij de Tweede Kamerverkiezing moet de overdracht aan de Kiesraad van de totalen in verband met het raadgevend referendum gebeuren aan de hand van de papieren documenten.

B3. Het gebruik van de stembureau App

Een aantal gemeenten gebruikt apps, aanvullend aan de handmatige telling en de verificatie, de stemmen te tellen en de opkomst te meten. De IBD raadt in verband met deze apps het volgende aan:

- Gebruik de app op een apparaat dat nergens anders voor is of wordt gebruikt;
- Gebruik de app op een apparaat waarvoor software-updates beschikbaar zijn;
- Zorg dat het apparaat is bijgewerkt naar de meest recente officiële softwareversie van de fabrikant;
- Neem technische maatregelen om te zorgen dat alleen verbinding kan worden gemaakt met noodzakelijke diensten.
- Neem technische maatregelen om te voorkomen dat netwerkverkeer kan worden afgeluisterd of gemanipuleerd.
- Beveilig het apparaat met een veilig wachtwoord en stel dit alleen beschikbaar aan de voorzitter van het stembureau;
- Laat het apparaat in geen geval onbeheerd achter;
- Onthoud dat de handmatige telling en de verificatie daarop leidend zijn bij het vaststellen van de einduitslag.

Algemene adviezen voor de gemeentelijke CISO

De IBD adviseert gemeentelijke CISO's beschikbaar en bereikbaar te zijn voor vragen in verband met informatiebeveiliging rondom de verkiezingen.

- Breng (aankomend) politici en lokale politieke partijen op de hoogte van de in dit bericht genoemde publicaties over spionage, ondermijning, integriteit en beïnvloeding.
- Meld gevallen van ongewenste beïnvloeding bij de relevante (sociale) media en doe waar nodig aangifte bij de politie.

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.IBDgemeenten.nl. Hier kunnen gemeenten bovendien via de community relevante informatie met elkaar delen, vragen aan elkaar stellen en documenten uitwisselen. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 373 8011 of

- Maak uzelf bekend bij de Griffie en zorg dat (aankomend) raadsleden en bestuurders u weten te vinden in geval van vragen over informatiebeveiliging en / of kwetsbaarheden rondom de verkiezingen.
- Treed in contact met de lokale organisator van de verkiezingen en zorg dat de deze u weet te vinden in geval van vragen over informatiebeveiliging en / of kwetsbaarheden rondom de verkiezingen.
- Meld kwetsbaarheden en incidenten aan de IBD. Voor een volledig beeld van de informatiebeveiliging rondom de verkiezingen is een landelijk beeld essentieel. De IBD zal de meldingen waar nodig geanonimiseerd verwerken in adviezen aan de VNG.

IBD als centraal meldpunt voor kwetsbaarheden en incidenten verkiezingen

Het ministerie van BZK zal gemeenten wijzen op de bereikbaarheid van de IBD via 070 373 8011 en info@IBDgemeenten.nl. De IBD fungeert als centraal meldpunt voor kwetsbaarheden en incidenten in verband met de verkiezingen en kan waar nodig 24 uur per dag worden benaderd voor spoedeisende vragen en meldingen.

Links en verwijzingen

1. https://nvvb.nl/media/cms_page_media/620/Bijlage%20Circulaire.pdf
2. https://www.nctv.nl/onderwerpen_a_z/spionage/index.aspx
3. <https://www.aivd.nl/actueel/nieuws/2017/05/22/bent-u-zich-be-wust-van-de-risicos-van-cyberspionage>
4. <https://vng.nl/raadgevers/veiligheid/ondermijning>
5. <https://vng.nl/onderwerpenindex/arbeidsvoorwaarden-en-personeelsbeleid/integriteit/raadgever-integriteit>
6. <https://kennisopenbaarbestuur.nl/media/254384/handreiking-integriteit-politieke-ambtsdragers.pdf>
7. <https://www.nrc.nl/nieuws/2017/10/19/commissie-vrees-voor-digitale-beïnvloeding-bij-verkiezingen-13564071-a1577785>
8. https://nvvb.nl/media/cms_page_media/620/Bijlage%20Circulaire.pdf_p.3