Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

B201801804

Gemeente Heerhugowaard (NH)
T.a.v. de Raadsgriffier
Postbus 390
1700 AJ HEERHUGOWAARD

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2018-0000058642

Uw kenmerk

Datum 9 februari 2018
Betreft Bewustzijn digitale informatiebeveiliging

Geachte burgemeester,
Geachte raadsgriffier,

Op 21 maart a.s. vinden verkiezingen plaats. Het vertrouwen in onze verkiezingen is groot. Dat komt in belangrijke mate door de wijze waarop de gemeenten de verkiezingen organiseren en uitvoeren. Het behoud van het vertrouwen in de verkiezingen is voor ons allen een prioriteit. Daarom moeten we alert zijn op ontwikkelingen die dit vertrouwen zouden kunnen aantasten.

Nieuwe technologieën kunnen dreigingen met zich meebrengen. De AIVD signaleert in de jaarverslagen dat er statelijke actoren zijn die zich richten op Nederland. Het Cyber Security Beeld Nederland 2017 laat zien dat statelijke actoren ook de intentie en capaciteit hebben om zich via digitale middelen te mengen in democratische processen.

Op 19 december jl. is, in de zogenoemde verkiezingscirculaire, door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) aan de gemeenten gevraagd om een analyse uit te voeren van de kwetsbaarheden in de eigen gemeentelijke organisatie en van de processen die worden ingericht voor de verkiezingen en om, als de analyse daartoe aanleiding toe geeft, maatregelen te treffen om kwetsbaarheden te verminderen c.q. weg te nemen. In vervolg hierop vragen wij u nu om de politieke partijen die in uw gemeente mee gaan doen aan de gemeenteraadsverkiezing te informeren over mogelijke dreigingen zodat de partijen zich daarvan bewust zijn en waar nodig maatregelen kunnen treffen.

Begin 2017 heeft het Nationaal Cyber Security Centrum (NCSC, onderdeel van de Nationaal coördinator terrorismebestrijding en veiligheid), bijeenkomsten gehouden voor de ICT-beheerders van de politieke partijen die gingen deelnemen aan de Tweede Kamerverkiezing. In die bijeenkomsten is ingegaan op de

mogelijkheden die ICT-beheerders hebben om hun gebruikers en systemen beter te beschermen tegen digitale dreigingen.

Het is van belang dat dergelijke voorlichting ook gegeven gaat worden aan de politieke partijen die deelnemen aan de komende gemeenteraadsverkiezingen. De Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten kan u daarin bijstaan. Dat doet de IBD allereerst door adviezen te geven die de digitale weerbaarheid vergroten. U treft deze adviezen aan in de factsheet die bij deze brief is gevoegd. U kunt ook terecht bij de IBD met vragen en meldingen. De contactgegevens van de IBD staan in de factsheet.

Wij hebben er alle vertrouwen in dat u aan deze oproep gevolg zult geven en gebruik zult maken van de deskundige hulp die de IBD u kan bieden.

De minister van Binnenlandse Zaken
en Koninkrijksrelaties,

drs. K.H. Ollongren

De voorzitter van de Vereniging
Nederlandse Gemeenten,

mr. J.H.C. van Zanen

INFORMATIE
BEVEILIGINGS
DIENST

Bescherm uzelf en uw (politieke) organisatie tegen digitale dreigingen

Een ongeluk zit in een klein hoekje, ook in het digitale verkeer. Met de grote hoeveelheid e-mails, berichten op sociale media en het toenemend gebruik van apparatuur die verbonden is met het internet neemt het risico van digitale dreigingen toe. Phishing, virusbesmettingen, verlies of diefstal van gegevens, digitale sabotage of bekladding van websites en andere narigheid zijn helaas aan de orde van de dag. De gevolgen kunnen groot zijn, zeker voor mensen die toch al in de schijnwerpers staan zoals raadsleden en bestuurders.

De Informatiebeveiligingsdienst (IBD), in 2013 opgericht door alle Nederlandse gemeenten, ondersteunt uw gemeente bij informatiebeveiliging in het algemeen en is voorafgaand en tijdens de verkiezingen 24x7 beschikbaar voor hulp, coördinatie en ondersteuning aan (aankomend) raadsleden en bestuurders. De IBD monitort hierbij in samenwerking met het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) de actuele dreiging. In dit kader wijzen wij u in deze factsheet op twee aandachtspunten: ongewenste beïnvloeding van de verkiezingen en uw eigen informatiebeveiliging.

Beïnvloeding

Er is veel aandacht voor beïnvloeding van verkiezingen, onder andere naar aanleiding van mogelijke onregelmatigheden bij de presidentsverkiezingen in de Verenigde Staten. Er is momenteel geen aanleiding om aan te nemen dat grootschalige beïnvloeding rondom de gemeenteraadsverkiezingen aan de orde is. Iedere vorm van oneigenlijke beïnvloeding blijft desondanks ongewenst en de IBD raadt aan berichtgeving rond uzelf en uw politieke organisatie goed in de gaten te houden. Bij een vermoeden van ongewenste beïnvloeding adviseren wij u melding te 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

Meldt misbruik en vermoeden van beïnvloeding ook bij de informatiebeveiligingsfunctionaris van uw gemeente en bij de IBD, zie ook punt 5 in deze factsheet. De IBD kan daarmee op basis van meldingen andere gemeenten waarschuwen als dit noodzakelijk is.

Informatiebeveiliging

De gemeente doet er veel aan om informatiesystemen te beveiligen en beveiligd te houden. Als raadslid of misschien wel bestuurder is het uw verantwoordelijkheid om hierop toe te zien. Goed voorbeeld doet goed volgen. Daarom is het des te belangrijker om uzelf en uw apparatuur adequaat te beschermen tegen digitale dreigingen. Er is momenteel geen indicatie van een verhoogde dreiging tegen politici, maar u bent net zo kwetsbaar als ieder ander op internet. De impact van een incident kan voor u groot zijn. Wat u overkomt haalt wellicht de krant van morgen en kan gevolgen hebben voor uw politieke loopbaan en het vertrouwen dat inwoners hebben in de overheid. De IBD geeft u in deze factsheet enkele tips om uzelf en uw (politieke) organisatie weerbaarder te maken. De IBD heeft aanvullend ook een factsheet uitgebracht voor de gemeentelijke informatiebeveiligingsfunctionarissen.[1]

1. Wees bewust van uw kroonjuwelen en hoe die beschermd zijn

Uw apparatuur bevat **waardevolle informatie**: uw contacten, uw e-mails en berichten, uw foto's, uw bankzaken, uw agenda; allemaal beschikbaar in uw broekzak en bij de meeste mensen beschermd door een pincode van vier cijfers. Een hoe is het eigenlijk gesteld met uw laptop? **Vergrendelt u uw scherm** als u koffie haalt? **Weet u wat u deelt** met apps en **denkt u na voordat u klikt op links** of bijlage opent? De risico's zijn talrijk: uw apparatuur wordt gestolen, uw website is onbereikbaar of wordt beklad, iemand anders plaatst berichten op Twitter of Facebook uit uw naam, iemand leest uw vertrouwelijke e-mails. De eerste tip is om goed **na te gaan of de beveiliging past bij het risico** ofwel de kans dat er iets gebeurt en de impact die dat heeft. Heeft u daarbij hulp nodig? Praat dan eens met de informatiebeveiligingsfunctionaris binnen uw gemeente of bel de IBD (zie ook tip 5).

2. Kies een sterke(re) toegangsbeveiliging

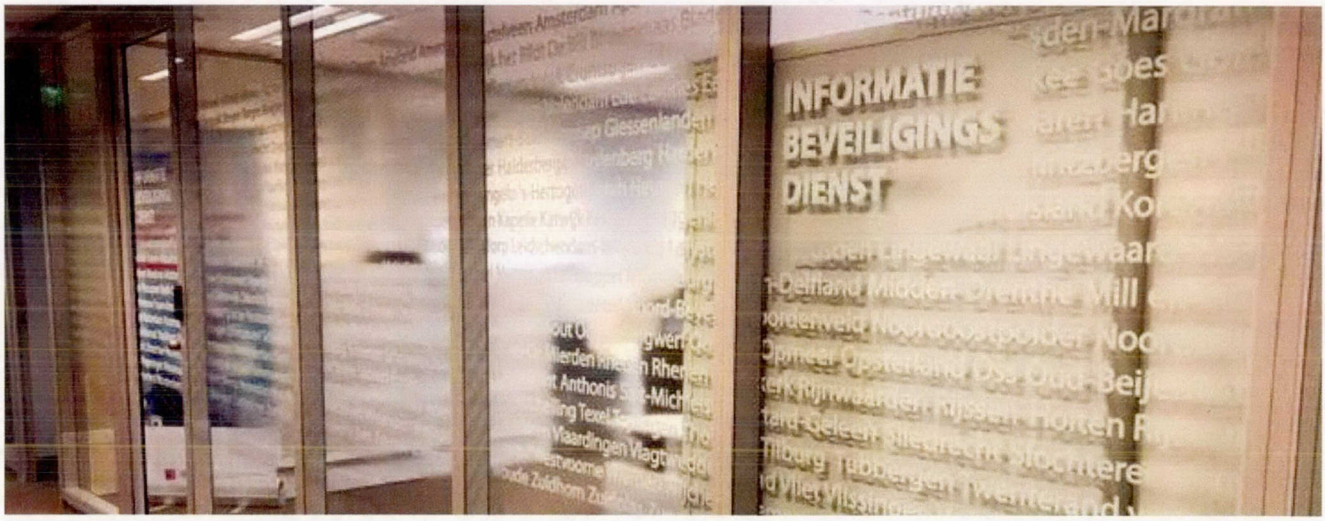
De top drie van meest gebruikte pincodes op smartphones is 0000, 1234, 2580. De top drie van meest gebruikte wachtwoorden: 123456, abc123, qwerty. Veel smartphones, laptops en tablets hebben de mogelijkheid om **sterkere wachtwoorden** in te stellen of aanvullend gebruik te maken van andere toegangsmogelijkheden zoals een vingerafdruk of gezichtsherkenning. De IBD raadt aan om voor ieder apparaat en iedere dienst een uniek wachtwoord van ten minste 12 tekens te gebruiken en daarbij geen gebruik te maken van herkenbare of herleidbare dingen zoals uw naam, geboortedatum, postcode, namen van kinderen, huisdieren of woorden die voorkomen in het woordenboek. Als u voor ieder apparaat en voor iedere dienst een uniek wachtwoord gebruikt dan kunt u deze wachtwoorden waarschijnlijk niet allemaal in uw hoofd onthouden. Een **wachtwoordmanager** biedt hiervoor uitkomst.

VNG Realisatie

De informatiebeveiligingsdienst (IBD)

De IBD werkt aan het verhogen en op peil houden van de informatiebeveiliging van Nederlandse gemeenten vanuit de kracht van het collectief. De IBD is een initiatief van alle Nederlandse gemeenten. Alle gemeenten, intergemeentelijke sociale diensten en belastingsamenwerkingen kunnen gebruik maken van de diensten van de IBD. De IBD ondersteunt gemeenten bij informatiebeveiligingsincidenten met advies en coordinatie. De IBD brengt regelmatig kennisproducten uit die gemeenten kunnen gebruiken bij het opstellen en uitvoeren van hun eigen informatiebeveiligingsbeleid. Aanvullend werkt de IBD doorlopend aan kennisdeling met en tussen gemeenten. Meer informatie treft u op www.informatiebeveiligingsdienst.nl

De IBD is bereikbaar via het telefoonnummer 070 - 373 8011 (24 uur per dag ingeval van spoedeisende meldingen) of via info@IBDgemeenten.nl.



Op de site van 'Veilig Internetten'[2] en 'Laat je niet hack maken'[3] staan goede tips voor het installeren en gebruiken van een wachtwoordmanager. Hoe goed uw wachtwoord ook is, het kan altijd worden gestolen. Veel online diensten[4] hebben de mogelijkheid om **tweestapsbeveiliging**, een extra beveiliging, toe te voegen, zoals een SMS, Tan-code of een code van een authenticatie-app. Als u deze instelt dan bent u extra beschermd.

3. Installeer updates en gebruik een antivirusprogramma

Alle apparatuur en software bevatten zogenaamde kwetsbaarheden ofwel gaten in de beveiliging. Door automatische **updates** aan te zetten, of regelmatig handmatig updates aan te zetten zorgt u dat uw apparatuur en software beschermd blijven. Door gebruik te maken van een **antivirusprogramma** verlaagt u de kans op besmetting met virussen en andere schadelijke software. Gebruik waar dat kan **bestandsversleuteling**[5], hierdoor kan niemand bij uw gegevens als uw apparatuur onverhoopt in verkeerde handen raakt.

4. Zorg voor een plan B: maak backups

Hoe goed uw beveiliging ook is, een ongeluk kan altijd gebeuren. Door regelmatig **backups** te maken kunt u uw bestanden en instellingen terugzetten na een incident. Hiermee verkleint u de schade van diefstal of verlies van data.

5. Lees mee en neem bij vragen contact op met de informatiebeveiligingsfunctionaris van de gemeente of met de IBD

Op de site van 'Veilig Internetten'[6] en 'Laat je niet hack maken'[7] staan goede en praktische tips over veilig internetten. Deze tips zijn in lijn met de '10 vuistregels voor veilig internetten' van het NCSC[8] en worden regelmatig bijgewerkt aan de hand van de actualiteit. Uw gemeente heeft een informatiebeveiligingsfunctionaris, de Chief Information Security Officer ofwel CISO. Deze functionaris kan u op weg helpen bij vragen over informatiebeveiliging. Vraag de contactgegevens na bij uw eigen gemeente en houd deze bij de hand. Informeer te allen tijde de CISO bij een incident zoals een virusbesmetting, verlies of diefstal van gegevens of misbruik van uw inloggegevens. De IBD is voorafgaand en tijdens de verkiezingen ook bereikbaar voor (aankomend) politieke ambtsdragers voor vragen en meldingen over informatiebeveiliging. U kunt de IBD bereiken via 070 373 8011 of via info@IBDGemeenten.nl. In geval van nood is de IBD 24 uur per dag bereikbaar. Buiten kantooruren wordt u via het algemene nummer verwezen naar het actuele piketnummer.

Links

1 Zie de factsheet **Adviezen rondom de gemeenteraadsverkiezingen** van de IBD
2 https://veiliginternetten.nl/themes/basisbeveiliging/situatie/ik-kan-mijn-wachtwoord-niet-onthouden/
3 https://laatjeniethackmaken.nl/
4 Apple, Google, Facebook, Dropbox, LinkedIn, Microsoft, Twitter, WhatsApp
5 O.a. door de functie Bitlocker in Windows of Filevault in MacOS.
6 https://veiliginternetten.nl
7 https://laatjeniethackmaken.nl/
8 https://www.ncsc.nl/actueel/factsheets/factsheet-10-vuistregels-voor-veilig-internetten.html