Digitale Veiligheid: kerntaak voor gemeenten

Aanleiding

In 2013 stemde de Algemene Ledenvergadering in met de resolutie 'Informatieveiligheid randvoorwaarde voor de professionele gemeente'. Die resolutie riep op tot het nemen van (bestuurlijke) verantwoordelijkheid om de gemeentelijke informatiehuishouding 'veilig' te organiseren.
Terugkijkend kunnen we constateren dat gemeenten goed gehoor hebben gegeven aan deze eigen oproep: ze blijken over het algemeen adequaat te kunnen anticiperen en reageren op digitale dreigingen.

Digitalisering is een van de motoren waarop de samenleving draait

De digitalisering in de samenleving zet door. Niet alleen het dagelijkse werk wordt in hoge mate ondersteund door ICT, steeds vaker nemen slimme applicaties, algoritmes en innovaties werk van mensen over. Daarmee nemen ook de risico's ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid toe.
Bij gemeenten bestaat het toenemende bewustzijn dat zij aan inwoners, ondernemers en ketenpartners (waaronder partijen in het verlengd lokaal bestuur) verplicht zijn hun verantwoordelijkheid te nemen in de digitale samenleving. Bestuurders streven naar een verdere verhoging van de digitale weerbaarheid in brede zin: in de eigen organisatie, bij ketenpartners en voor inwoners en ondernemers. Dat betekent dat permanent aandacht besteed wordt aan digitale veiligheid bij bestuur, gemeenteraadsleden en ambtenaren.
Dat vraagt om een bestuurlijke agenda voor digitale veiligheid. De VNG ontwikkelt handvatten om bestuurders te ondersteunen bij het opstellen van een agenda digitale veiligheid voor de eigen gemeente.

Samenhang en visie

Digitale veiligheid is een zaak van de gehele overheid. Het is van groot belang om samenhang te brengen in initiatieven van gemeenten en medeoverheden en in het bijzonder met die van de rijksoverheid. Dat vraagt om een duidelijke visie vanuit de gemeentelijke overheid op digitale veiligheid. Daarom heeft het bestuur van de VNG de Agenda Digitale Veiligheid gemeenten 2020-2024 vastgesteld. Met deze agenda draagt de VNG ertoe bij dat de gezamenlijke inspanningen van de Nederlandse overheid doelmatig en doeltreffend zijn. De agenda biedt een handvat om in de komende jaren vorm te geven aan de praktische uitwerking. Alleen als gemeentelijk bestuurders, raadsleden èn ambtenaren zich bewust zijn van hun verantwoordelijkheid voor die digitale veiligheid, kunnen we de opgave die voor ons ligt waarmaken. Dat betekent dat geïnvesteerd moet worden in het verhogen van de weerbaarheid, dat gemeenten samenwerken bij preventie, in crisissituaties èn in de nasleep daarvan. Dat is de kern van de voorliggende resolutie.

Resolutie

De leden van de VNG, in de BALV bijeen op 12 februari 2021, komen overeen,

overwegende:

- dat gemeenten een verantwoordelijkheid hebben voor een veilige samenleving en dat de samenleving zich in toenemende online afspeelt
- dat gemeenten zich bewust zijn van de kansen en risico's van digitalisering voor de eigen organisatie, ketenpartners, inwoners en ondernemers
- dat voortschrijdende technologie leidt tot nieuwe afhankelijkheden en kwetsbaarheden die vragen om een weerbare samenleving
- dat informatie en de systemen waarin deze zich bevindt adequaat dienen te zijn beveiligd om uitval, onbedoelde wijziging of vernietiging en onbevoegde inzage te voorkomen
- dat deze verantwoordelijkheid van gemeenten zich uitstrekt tot de veiligheid van de samenleving bij het optreden van digitale incidenten en het voorkomen en bestrijden van cybercriminaliteit,

stellen vast:

- dat het bestuur van de VNG in februari 2020 de agenda digitale veiligheid gebaseerd op bovenstaande overwegingen heeft vastgesteld.

Het bestuur geeft daaraan invulling:

- door binnen de kaders van het fonds GGU te investeren in de doorontwikkeling van de Informatiebeveiligingsdienst (IBD) vanuit zijn verantwoordelijkheid als gemeentelijk CERT binnen het landelijk dekkend stelsel
- door het opstellen van kaders voor samenwerking onder regie van de IBD om invulling te geven aan gemeentelijke solidariteit bij het voorkomen en oplossen van cyberincidenten
- door te onderzoeken hoe gemeentelijk bestuurlijke verantwoordelijkheden voor openbare orde en veiligheid in de fysieke wereld zich verhouden tot het voorkomen, herkennen en oplossen van (digitale) veiligheidsincidenten
- door met betrokken beleidsdepartementen te werken aan samenhangend beleid gericht op het verhogen van de weerbaarheid door:
  - het ontwikkelen van en implementeren van overheidsbrede beveiligingsnormen en standaarden waaronder de doorontwikkeling van de Baseline Informatieveiligheid Overheden (BIO)
  - bij te dragen aan de ontwikkeling van een gecoördineerde incidentbestrijdingsprocedures en een bijbehorend opschalingsmodel voor digitale incidenten (en bijbehorende oefenscenario's) waarin de verantwoordelijkheden van het lokaal bestuur en de lokale politiek kunnen worden waargemaakt
- door bij te dragen aan de ontwikkeling van initiatieven die de weerbaarheid van inwoners en ondernemers ten aanzien van cybercriminaliteit vergroten
- door digitale veiligheid als beleidsprioriteit in te brengen bij de voorbereidingen voor het volgende kabinet,

roept de leden van de VNG op:

- incidenten te delen met de IBD wanneer een dergelijk incident ook zou kunnen optreden bij andere gemeenten en / of andere sectoren
- jaarlijks een incidentoverzicht op categorieniveau te delen met de IBD, zodat een compleet inzicht bestaat van dreigingen, trends en ontwikkelingen
- een digitaal incidentbestrijdingsplan vast te stellen en jaarlijks te actualiseren
- invulling te geven aan de noodzakelijke intergemeentelijke solidariteit bij (gemeentelijke) digitale incidenten mede op aangeven van de Informatiebeveiligingsdienst
- periodiek te oefenen met cyberincidenten om daarmee de gemeentelijke weerbaarheid te toetsen en te vergroten
- periodiek het onderwerp digitale veiligheid in het college van B&W te agenderen
- in de Integrale Veiligheidsplannen ook de digitale aspecten expliciet te benoemen:
  - de veiligheid van de samenleving bij het optreden van digitale incidenten
  - het voorkomen en bestrijden van cybercriminaliteit
  - het beveiligen van de informatie waarvoor zij verantwoordelijkheid draagt

- naar het advies van de CyberSecurityRaad[1] voldoende budget vrij te maken in gemeentelijke begrotingen voor blijvende weerbaarheid tegen digitale dreigingen
- waar mogelijk gebruik te maken van de gezamenlijk ontwikkelde voorzieningen en programma's die zich richten op digitale veiligheid[2],

stemmen ermee in:

- dat het VNG-bestuur de ingezette beleidslijn op digitale veiligheid zoals hierboven verwoord tot uitvoering brengt
- dat op basis van een met het College voor Dienstverleningszaken afgestemd plan van aanpak structureel voldoende budget vrijgemaakt wordt vanuit het fonds GGU, gericht op de realisatie van het bovenstaande.

1 Meerjarenstrategie CyberSecurityRaad 2018-2021.
2 Zie https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/ en https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/