Checklist Digitale Veiligheid Raadsleden

versie 1.0 | januari 2023

De digitale transitie biedt kansen en uitdagingen. Ook gemeenten moeten weerbaar worden én blijven tegen digitale dreigingen. Maar wat kunt u als raadslid doen om de digitale weerbaarheid voor uw gemeente te versterken? U kunt hier vanuit verschillende rollen naar kijken. In dit document zetten we de verschillende rollen van gemeenteraadsleden op een rij.

Wie doet wat?

De **burgemeester** heeft in het borgen van de digitale veiligheid meerdere verantwoordelijkheden:

1. Gemeentelijke organisatie digitaal veilig (eigen huis op orde)
2. Voorbereiding op maatschappelijke ontwrichting, incidenten en crises
3. Weerbaarheid verhogen van inwoners en ondernemers, preventie cybercriminaliteit.

Als **raadslid** kunt u bijdragen aan het verhogen van de digitale veiligheid door:

- vooraf aan een nieuwe beleidsperiode goede kaders stellen (kaderstellende rol);
- regelmatig het thema agenderen (volk vertegenwoordigende rol);
- actief het college controleren (controlerende rol).

Meer informatie over de rol van de raad bij digitale veiligheid: https://vng.nl/artikelen/raadgever-digitale-veiligheid

In bepaalde gevallen gaat het om gevoelige informatie, zoals bijvoorbeeld persoonlijke mails of vertrouwelijk gedeelde informatie. Dan is het van belang om deze informatie goed te beveiligen, zodat deze informatie niet uitlekt of in verkeerde handen valt. Wanneer het gaat om geheim verklaarde stukken, dan kan het zelfs strafbaar zijn om de geheimhouding van informatie te schenden.

1. Volksvertegenwoordigende rol

Overweeg een ethische commissie waarin u bespreekt:

- Wat voor raadslid wilt u zijn?
- Wat voor 'soort' gemeente u wil zijn? Bijvoorbeeld bij de inzet van technologie, om de veiligheid te vergroten. https://vng.nl/nieuws/agenda-digitale-grondrechten-en-ethiek-2022-2026-uit

En waarin u uitzoekt:

- Hoe gaat u om met maatschappelijke knelpunten en problemen in uw gemeente ten aanzien van digitale veiligheid?

Verken de mate van weerbaarheid bij uw achterban

- Welke (negatieve) ervaringen zijn er met diverse vormen van gedigitaliseerde criminaliteit, zoals identiteitsfraude, WhatsApp-oplichting en online bedreiging?
- Welke ervaringen hebben zij met voorlichtingscampagnes, presentaties en bijeenkomsten op dit thema?

Organiseer het maatschappelijke debat (eventueel samen met andere partners)

- Wat zijn de ervaringen van bedrijven of winkels in uw gemeente? Ga bij ze langs!
- Wat is voor de lokale partijen de balans tussen privacy en veiligheid? Ga in gesprek!
- Welke werkgevers/werknemers (van welke bedrijven) vertegenwoordigen u als raad?

Zorg dat uw kennis over het thema up to date is.

Er is een groot leeraanbod met handige trainingen en oefeningen voor raadsleden. Daarnaast is er een webinar-reeks van vijf afleveringen die u op weg helpen.

Online veiligheid van raadsleden, ongewenst gedrag en integriteitskwesties.

Online pesten en desinformatie verspreiden zijn vormen van ondermijnend gedrag en een aantasting van de integriteit. Hier kunt u als raadslid ook mee te maken krijgen. Vragen die dan spelen zijn:

1. Kunnen raadsleden ergens in de gemeente terecht wanneer zij zich online onveilig voelen?
2. Heeft de raad onderling online omgangsvormen afgesproken?
3. Speelt de gemeente een actieve rol in het bevorderen van sociale veiligheid online en het bestrijden van desinformatie of ondermijnend gedrag online?

2. Kaderstellende rol

Werk digitale veiligheid uit in het Integraal Veiligheidsplan (IVP).
Is digitale veiligheid uitgewerkt in het IVP van uw gemeente? Gebruik hiervoor het Focusblad Digitale Veiligheid, wat hier handvatten voor biedt.

Richt een lokaal cybercrisisteam in en oefen.
Is er een lokaal cybercrisisteam ingericht in uw gemeente en worden hiermee cybercrisisoefeningen (eventueel i.s.m. de Veiligheidsregio) geoefend?

Vraag naar een periodieke agendering digitale veiligheid in portefeuillehouders-overleg.
Wordt digitale veiligheid periodiek geagendeerd in het portefeuillehouders-overleg burgemeester met de afdeling OOV?

Vraag naar een periodiek overleg betrokken functionarissen
Vindt er periodiek overleg plaats tussen de burgemeester, gemeentesecretaris, de OOV-er, de CISO en FG over digitale veiligheid?

Stel geld beschikbaar voor de aanpak van digitale veiligheid (breed)

- Hoeveel geld wordt besteed aan het bevorderen van digitale veiligheid van inwoners en ondernemers, aan voorbereiding op digitale ontwrichting/ incidenten/crises en aan de weerbaarheid van de gemeente zelf (eigen huis op orde)? Bespreek met het college de ambities en het noodzakelijke budget. Gebruik hiervoor het IVP.
- Wat als de gemeente/samenwerking/ regeling toch geraakt wordt? Uit welke gelden wordt dat gefinancierd? Is daar over nagedacht/beleid op?

Voorbereiding op digitale incidenten
Wat als cruciale processen/elementen in uw gemeente digitaal ontregeld worden? Zijn mogelijke gevolgeffecten in beeld? Is dan voor iedereen duidelijk wie wat doet? Is dan duidelijk waar de kosten worden geboekt?

Bij iedere vraag kunt u zich afvragen hoeveel geld of inspanning voldoende is. Dat is bij uitstek een politieke vraag. Het vrijmaken van voldoende middelen is cruciaal. In de begrotings- en verantwoordings-besprekingen is het raadzaam daar tijd voor te blijven inruimen.

3. Controlerende rol

Toets de borging van de bedrijfscontinuïteit
- Kent u de ENSIA rapportage en waarstaatje-gemeente.nl? Door de ENSIA rapportages te bespreken en mee te draaien in lokale crisisoefeningen kunt u hierop toezien.
- Wordt er verantwoording afgelegd over de digitale veiligheid en bedrijfscontinuïteit door de samenwerkingsverbanden? Raadsleden zijn ook verantwoordelijk voor de koers, de uitvoering en de controle op samenwerkingsverbanden en zogeheten verbonden partijen. Ook t.a.v. digitale veiligheid.

Geef uitvoering aan het IVP
- Wordt er voldoende uitvoering gegeven aan de digitale veiligheidsaspecten uit het IVP?
- Is duidelijk welke cruciale diensten in de gemeente staan, welke bij digitale verstoring tot fysieke gevolgeffecten met maatschappelijke ontwrichting kunnen leiden?

Hulptroepen

Digitale veiligheid lijkt een specialistisch onderwerp. Vraag rond naar expertise die in uw fractie aanwezig is, of bij inwoners die hierop mee willen denken vanuit hun dagelijkse werk. Maak gebruik van de ondersteuning van de griffie en ambtelijke bijstand. Denk aan onafhankelijke instanties zoals de ombudsman of de (lokale) media.

Nodig de CISO of de FG uit voor een gesprek, zodat u weet wat u aan elkaar heeft. Dat hoeft niet alleen over beleid te gaan, maar ook over uw rol als onderdeel van de gemeente.

Kijk hoe andere gemeenten het doen (benchmarks, rekenkamerrapporten, werkbezoeken)
- Hoeveel geld geven soortgelijke gemeenten uit aan digitale veiligheid? Hoeveel incidenten doen zich voor bij andere gemeenten? Maak gebruik van benchmarks of vraag een lokale rekenkamer om een onderzoek te doen.

Monitor op digitale veiligheid
- Heeft de raad zicht op cijfers t.a.v. gedigitaliseerde criminaliteit, zoals diverse vormen van online fraude?
- Heeft de raad zicht op de relatie van het onderwerp ten aanzien van andere thema's als ondermijning en maatschappelijke onrust?
- Welke gegevens over digitale veiligheid vindt u terug in de bestuursrapportages?
- Welke informatie mist u in de periodieke P&C stukken?

⚠ Besef dat het lastig is om te controleren of de genomen maatregelen een dreiging hebben voorkomen. U kunt ook geluk hebben gehad – en er heeft zich geen dreiging voorgedaan. Voorkomen is beter dan genezen.

De VNG ondersteunt, faciliteert en adviseert gemeenten vanuit de Agenda Digitale Veiligheid bij de digitale transitie. Met elkaar zorgen we voor meer (bestuurlijke) bewustwording, betrokkenheid en kennisdeling. Het doel is om gemeenten te helpen bij het voorkomen, bestrijden en oplossen van cybercriminaliteit en cyberincidenten. Dit doen we samen met onze stakeholders. Vanuit de Agenda Digitale Veiligheid krijgen gemeenten concrete handvatten aangereikt die aansluiten bij de bestuurlijke en ambtelijke praktijk.

Meer informatie vindt u op:
https://digitaleveiligheid.pleio.nl
Contact via: teamadv@vng.nl