Raadsvoorstel

Gemeente ROZENDAAL

Onderwerp

Digitale weerbaarheid raad – gebruik van gemeentelijke, centraal beheerde apparatuur

Adviseur	: Griffie	**Behandeldatum**	: 26 mei 2026
Programma	: Bestuur en Organisatie	**Kenmerk**	: …..
Programmanummer	: …	**Openbaar**	: ja
Portefeuillehouder	: Burgemeester		

Advies

1. Gemeentelijke, centraal beheerde apparatuur vast te stellen als standaard voor het verrichten van raadswerkzaamheden.
2. Gebruik van privé apparatuur uitsluitend toe te staan indien wordt voldaan aan vastgestelde technische en organisatorische beveiligingseisen.
3. De griffie opdracht te geven deze eisen uit te werken in een regeling digitale weerbaarheid voor raadsleden en deze jaarlijks te evalueren.

Aanleiding

De digitale dreiging richting gemeenten is structureel en neemt toe. Gemeenten zijn doelwit van ransomware, phishing en digitale verstoring. In het licht van geopolitieke spanningen en statelijke cyberactiviteiten wordt versterking van digitale weerbaarheid nadrukkelijk verwacht.
Raadsleden beschikken over vertrouwelijke informatie en persoonsgegevens. Het gebruik van privé apparatuur brengt risico's met zich mee voor informatiebeveiliging, privacy en bestuurlijke continuïteit.
Landelijke kaders zoals de BIO, AVG en NIS2 vragen om aantoonbare risicobeheersing. Ook de VNG benadrukt in haar handreikingen digitale veiligheid voor raadsleden het belang van centrale beveiliging en duidelijke kaders.

Beoogd effect

Versterking van de digitale weerbaarheid van de raad en beperking van risico's op datalekken en cyberincidenten, passend binnen landelijke wettelijke verplichtingen.

Argumenten

1. Digitale veiligheid raakt de bestuurlijke verantwoordelijkheid

Onvoldoende beveiligde apparatuur van individuele ambtsdragers kan een toegangspunt vormen tot gemeentelijke systemen. Centrale beheersing van apparatuur verkleint deze kwetsbaarheid.

2. Landelijke normen vragen om aantoonbare maatregelen

De BIO, AVG en NIS2 vragen om passende technische en organisatorische beveiliging. Gemeentelijke apparatuur maakt centrale monitoring, updatebeheer en incidentrespons mogelijk en aantoonbaar.

3. Bescherming van persoonsgegevens
Raadsleden hebben in het kader van hun publieke taak toegang tot stukken waarin persoonsgegevens van inwoners en andere betrokkenen kunnen voorkomen, bijvoorbeeld in zienswijzen bij ruimtelijke procedures of in inspreeknotities en burgerbrieven aan de raad.
De gemeente is op grond van de AVG verwerkingsverantwoordelijke en dient passende technische en organisatorische beveiligingsmaatregelen te treffen. Duidelijke kaders voor apparatuur gebruik dragen bij aan het beperken van risico's op datalekken en ongeautoriseerde toegang en versterken daarmee de digitale en bestuurlijke weerbaarheid van de gemeente.

4. Continuïteit bij incidenten
Bij verlies of besmetting kan gemeentelijk beheerde apparatuur direct worden geblokkeerd of gewist. Dit is bij privéapparatuur beperkter uitvoerbaar.

5. Reputatie en vertrouwen
Een datalek of cyberaanval heeft naast technische en financiële gevolgen ook directe impact op het vertrouwen van inwoners in het gemeentebestuur. Openbaar worden van vertrouwelijke informatie of persoonsgegevens kan leiden tot reputatieschade, bestuurlijke druk en aantasting van de geloofwaardigheid van de raad. Investeren in digitale beveiliging is daarmee ook een investering in bestuurlijke betrouwbaarheid en continuïteit.

Kanttekeningen
1. Gemeentelijke apparatuur vraagt een hogere eenmalige investering.
2. Het gebruik van privéapparatuur onder voorwaarden vereist structurele controle en toezicht.
3. Beheeroplossingen op privéapparatuur kunnen als ingrijpend worden ervaren.
4. Microsoft Office functionaliteit op privéapparatuur is beperkt tot de Webversies van Mail/Agenda, Word, Excel, OneDrive, SharePoint etc..

Personele gevolgen
De griffie verzorgt implementatie, instructie en periodieke evaluatie. Dit vraagt bij invoering extra inzet.

Financiën
Uitgangspunt: 9 raadsleden en 9 commissieleden:

- Structurele kosten (geldt voor alle varianten): jaarlijkse M365-licenties en technisch beheer circa € 10.500.
- Aanvullende kosten bij gemeentelijke apparatuur: eenmalige investering hardware iPad Air 11 of 13 inch: € 14.400 - € 18.000.
- Rekening te houden met periodieke vervanging, op te nemen in de meerjarenraming.
- Aanvullende (ingeschatte) kosten bij gebruik privéapparatuur (indien toegestaan): mogelijke inzet MDM/MAM[1]-oplossing en extra beheerinspanning: eenmalig MDM/MAM: € 3.200, jaarlijks € 10.000. Alleen MAM: eenmalig € 1.600, jaarlijks € 1.000.

[1] MDM: de privéapparatuur wordt op afstand beheerd door de ICT partij van gemeente Rozendaal. De ICT-partij kan wachtwoordvereisten afdwingen, het toestel vergrendelen, applicaties installeren/verwijderen en op afstand alle data (inclusief privéfoto's) wissen.

Investering wordt bij keuze voor gemeentelijke apparatuur betrokken bij de eerstvolgende Kadernota en verwerkt binnen programma Bestuur en Organisatie.

Vervolg

Uitwerking regeling digitale weerbaarheid.
Technische implementatie.
Instructiebijeenkomst voor raadsleden.
Jaarlijkse evaluatie via de griffie.

Communicatie

Interne communicatie via de griffie richting raad en commissieleden

Slotbeschouwing

Dit voorstel sluit aan bij de bredere bestuurlijke weerbaarheidsopgave van Rozendaal. Door duidelijke keuzes te maken over digitale inrichting wordt de continuïteit en betrouwbaarheid van de lokale democratie versterkt. Digitale weerbaarheid is daarmee niet alleen een wettelijke verplichting, maar ook een voorwaarde voor het behouden van maatschappelijk vertrouwen in de lokale democratie.

Corrie Steenbergen,
griffier

Ingrid Timmer,
burgmeester