

# Lokale cyber- wegenkaart 3.0

1 van de 4 wegen naar een  
cyberweerbare gemeente:  
Eigen huis op orde



**Gemeenten hebben een belangrijke rol om te voorkomen dat inwoners, bedrijven, voorzieningen én de gemeente zelf, slachtoffer worden van cybercriminaliteit. Om gemeenten te helpen, worden vier wegen onderscheiden waarop een gemeente actie dient te ondernemen, namelijk:**

1. Eigen huis op orde
2. Cyberincidenten en -crises
3. Cybercrime en gedigitaliseerde criminaliteit
4. Online aangejaagde ordeverstoringen

**In de beschrijvingen van deze vier wegen wordt duidelijk welke rol de gemeente kan nemen, welke gevaren er op de weg zijn en waar de gemeente hulp (de zogenoemde wegwacht) kan invoeren. Er is geen volgorde in het nemen van de vier wegen. Elke weg kan nu en naast elkaar genomen worden. Voor elke weg is een aparte factsheet beschikbaar. In deze factsheet gaan we in op 'Eigen huis op orde'.**

## EIGEN HUIS OP ORDE



### Doel van deze weg

Gemeenten zijn verantwoordelijk voor het betrouwbaar, veilig en continu functioneren van de eigen digitale systemen (hardware, en software, cloud- en ketenvoorzieningen) en informatievoorziening. Dit is noodzakelijk om de dienstverlening en bedrijfsvoering in goede orde te laten verlopen en om persoonsgegevens en andere gevoelige informatie bij de gemeente adequaat te beschermen.

'Eigen huis op orde' betekent dat digitale veiligheid structureel is ingebed in de governance, het risicomanagement en de planning- en controlcyclus van de gemeente. Digitale risico's worden daarbij gelijkwaardig gewogen aan financiële en juridische risico's. Dat vraagt om meer dan technische maatregelen alleen: hoewel informatiebeveiliging vaak wordt geassocieerd met informatie- en communicatietechnologie (ICT), wordt het eigen huis op orde brengen in belangrijke mate bepaald door mensen, cultuur en processen.



### Risico's op de weg

Gemeenten zijn voor hun dienstverlening afhankelijk van goed werkende en veilige ICT- en Operationele Technologie (OT) voorzieningen. De digitale dreiging is structureel en complex geworden. Criminele netwerken én statelijke actoren richten zich niet alleen op financieel gewin, maar ook op verstoring van essentiële processen. Denk hierbij aan hacks en datalekken, ransomware waarbij systemen worden gegijzeld, verstoring van leveranciers, misbruik van accounts via phishing, of manipulatie van fysieke infrastructuur (zoals bruggen en gemalen). De gemeentelijke CISO (chief information security officer), dan wel degene die binnen de gemeente is aangewezen voor de informatieveiligheid, adviseert het bestuur onder andere bij het adequaat inrichten van de systemen volgens de normen (zoals de Baseline Informatiebeveiliging Overheid 2, BIO2) en wet- en regelgeving (zoals de Cyberbeveiligingswet) - en over het beheersen van deze risico's.



### Wie zit er aan het stuur

Bestuurlijk: de eindverantwoordelijkheid ligt bij het college van burgemeesters en wethouders (B&W). De bestuurder met ICT in portefeuille draagt bestuurlijke verantwoordelijkheid voor passende beveiliging van digitale systemen en informatievoorzieningen. Digitale veiligheid is een bestuurlijke kerntaak en integraal onderdeel van risicomanagement en de planning- en controlcyclus. Op grond van de Cyberbeveiligingswet moeten bestuurders actief toezicht houden op naleving van wettelijke verplichtingen en beveiligingsmaatregelen, zorgen voor voldoende middelen en organisatorische borging, en periodiek en aantoonbaar geschoold zijn in cyberrisico's en passende maatregelen.

Gemeenten zijn wettelijk verplicht om de BIO2 risicogebaseerd te implementeren en te voldoen aan de verplichtingen uit de Cyberbeveiligingswet, zoals onder meer de zorg-, meld- en de registratieplicht. De Rijksdienst Digitale Infrastructuur houdt toezicht op naleving.

De CISO of security officer heeft binnen de gemeente een onafhankelijke toezichthoudende en adviserende rol rondom informatieveiligheid. De CISO rapporteert rechtstreeks aan het bestuur en moet direct geïnformeerd worden als er sprake is van een (mogelijk) incident. Afhankelijk van de impact kan een gemeentelijk (cyber)crisisteam geïnstalleerd worden.

Ambtelijk: De proceseigenaar is verantwoordelijk voor de beveiliging en continuïteit van de eigen (informatie) systemen. Dit betekent dat beveiligingsmaatregelen, updates en toegangsbeheer structureel worden uitgevoerd en gemonitord. De CISO of security officer adviseert en toetst op naleving van beveiligingsnormen en risicobeheersing, maar de verantwoordelijkheid voor de uitvoering ligt bij het lijnmanagement. Digitale veiligheid is daarmee geen exclusieve taak van de ICT-afdeling, maar een organisatiebrede verantwoordelijkheid.



### Welke richting te nemen

Goede preventieve maatregelen kunnen veel voorkomen maar helaas niet alles. Het gaat niet om óf je wordt gehackt, maar wanneer. Dit betekent dus een samenhangende aanpak van preventie, detectie én response. Zorg in ieder geval voor: tijdige installatie van updates, multifactorauthenticatie, structurele bewustwording van medewerkers, offline en geteste back-ups, monitoring en logging om incidenten tijdig te detecteren, duidelijke procedures voor incidentmelding en crisisopschaling en periodieke controle op de effectiviteit van de genomen maatregelen. Als de gemeentelijke systemen alsnog schade wordt aangebracht, is dit niet alleen het probleem van de ICT-afdeling, maar raakt het de hele gemeentelijke organisatie. Digitale verstoringen kunnen leiden tot uitval van dienstverlening en maatschappelijke impact. Daarom moeten vooraf heldere besluitvormingslijnen, communicatieprotocollen en escalatieroutes zijn vastgelegd. Digitale veiligheid is integraal onderdeel van risicomangementment en moet worden meegenomen bij inkoop, aanbestedingen en samenwerkingsverbanden. Een ketenperspectief ten opzichte van externe afhankelijkheden en risico's en adequaat leveranciersmanagement zijn hierbij essentieel.



### Wegenwacht

- Als gemeente kun je ondersteuning krijgen van de Informatiebeveiligingsdienst (IBD), onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD is de sectorale CERT/CSIRT voor gemeenten en fungeert als centraal meldpunt bij digitale incidenten. De IBD adviseert onder meer over handelingsperspectief, crisisaanpak en communicatie. De IBD is aangesloten bij het Nationaal Cyber Security Centrum (NCSC) en deelt actief dreigingsinformatie en waarschuwingen met gemeenten. <https://www.informatiebeveiligingsdienst.nl/over-de-ibd/>
- De mindmap 'Informatiebeveiliging - Eigen huis op orde' biedt inzicht in de verschillende aspecten van informatiebeveiliging en de rol van bestuurder daarbij. <https://vng.nl/artikelen/mindmaps-informatieveiligheid>
- Het Dreigingsbeeld informatiebeveiliging gemeenten 2025-2026 laat zien dat de risico's voor gemeenten toenemen en vraagt om bestuurlijke aandacht en ondersteuning. De Handreiking Digitale veiligheid en de gemeentelijke bestuurder geeft vijf bestuurlijke prioriteiten bij het dreigingsbeeld. <https://vng.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2025-2026-uit>

- Laat bestuurders oefenen zodat zij bewust worden van de bestuurlijke gevolgen en belangen tijdens een cybercrisis. <https://vng.nl/artikelen/interactieve-cyberoefening>
- Om het eigenaarschap bij het management op de kaart te zetten heeft de IBD gesprekskaartjes voor de Gemeentesecretaris ontwikkeld. Met deze kaartjes wordt de gemeentesecretaris met basiskennis geholpen zodat zij of hij weet welke vragen te stellen aan adviseurs en aan proceseigenaren. <https://www.informatiebeveiligingsdienst.nl/product/gesprekskaartjes-voor-de-gemeentesecretaris/>
- VNG Academie biedt een leeraanbod om de kennis en vaardigheden van bestuurder op diverse digitale veiligheidsthema's, zoals interne informatiebeveiliging, voorbereiding op digitale ontwrichting, en de weerbaarheid van inwoners te versterken <https://vng.nl/artikelen/leeraanbod-digitale-veiligheid-voor-bestuurders-van-gemeenten>
- Bekijk het overzicht van kennisproducten in relatie tot de Baseline Informatiebeveiliging Overheid 2. <https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid-versie-2-bio2/>
- Met de BIO2-handreiking krijgen gemeenten een praktisch groeimodel om stap voor stap hun informatiebeveiliging in te richten. <https://www.informatiebeveiligingsdienst.nl/nieuws/nieuwe-bio2-handreiking-een-realistische-aanpak-voor-informatiebeveiliging/>
- Om gemeenten te helpen met het verhogen van de digitale weerbaarheid heeft de IBD een ondersteuningspakket ontwikkeld voor de processen en maatregelen uit de BIO met de hoogste prioriteit. <https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/>
- Zie ook de Agenda Digitale Veiligheid 2028 van de VNG, waarin de ambities richting 2028 staan op het gebied van robuuste informatiebeveiliging, risicomangementment, toezicht en bestuurlijke professionalisering. 'Eigen huis op orde' vormt één van de hoofdthema's. <https://vng.nl/publicaties/agenda-digitale-veiligheid-2028>
- In de Tooling Cyberbeveiligingswet vind je diverse hulpmiddelen om je organisatie voor te bereiden op de Cyberbeveiligingswet. <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/tooling-cyberbeveiligingswet/>

**CCV** centrum voor  
criminaliteitspreventie en  
veiligheid

Deze Lokale cyberwegenkaart is in opdracht van het ministerie van Justitie en Veiligheid door het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) speciaal voor gemeenten ontwikkeld. Ondanks raadplegingen bij diverse netwerkpartners, beseffen wij ons dat wij niet geheel volledig kunnen zijn. En je kunt dan ook geen recht ontlenen aan de genoemde informatie of aan de bronnen waar naar verwezen wordt. Heb je vragen naar aanleiding van de Lokale cyberwegenkaart, neem dan contact op met het CCV, via [info@hetccv.nl](mailto:info@hetccv.nl).

© het CCV, maart 2026, [www.hetccv.nl/cybercrime](http://www.hetccv.nl/cybercrime)