CCV centrum voor criminaliteitspreventie en veiligheid

# Lokale cyber-wegenkaart 2.0

De vier wegen naar een cyberweerbare gemeente


**Gemeenten hebben een belangrijke rol om te voorkomen dat inwoners, bedrijven, voorzieningen én de gemeente zelf, slachtoffer worden van cyber gerelateerde zaken. Om gemeenten te helpen, worden vier wegen onderscheiden waarop een gemeente actie dient te ondernemen, namelijk:**
**1. Eigen huis op orde**
**2. Cybercrisis en -incidenten**
**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 wegenwacht) kan inroepen. 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 goed functioneren van de eigen digitale systemen (hardware en software) en digitale informatievoorzieningen, zodat de dienstverlening en bedrijfsvoering in goede orde verloopt en de beschikbare informatie bij de gemeente goed beveiligd is.

### Risico's op de weg

Gemeenten zijn voor hun dienstverlening afhankelijk van goed werkende ICT-voorzieningen. De gemeentelijke CISO (chief information security officier), dan wel degene die binnen de gemeente is aangewezen voor de informatieveiligheid, adviseert en ondersteunt het bestuur onder andere bij het adequaat inrichten van de systemen volgens de normen en wet- en regelgeving. En hij of zij zorgt voor de beveiliging van de data tegen risico's zoals criminele activiteiten. Denk hierbij aan gemeentelijke systemen die worden gehackt, data die worden ontvreemd, malware dat wordt geïnstalleerd of informatiesystemen die worden gegijzeld (ransomware).

### Wie zit er aan het stuur

Bestuurlijk: de eindverantwoordelijkheid ligt bij de bestuurder die ICT in portefeuille heeft binnen het college van BenW. Deze bestuurder zorgt ervoor dat de gemeente passende beveiliging heeft op haar digitale systemen en informatievoorzieningen. Het ministerie van BZK heeft de Baseline Informatiebeveiliging Overheid (BIO) opgesteld waar de gemeentelijke informatievoorziening aan dient te voldoen. Het goed laten functioneren van alle systemen ligt bij de ICT-afdeling van de gemeente. De CISO of security officer heeft binnen de gemeente een onafhankelijke toezichthoudende en adviserende rol rondom informatieveiligheid. Hij moet direct geïnformeerd worden als er sprake is van een (mogelijk) incident. Er kan eventueel een gemeentelijk (cyber)crisisteam geïnstalleerd worden.

Ambtelijk: de verantwoordelijkheid voor een goede beveiliging van de (informatie)systemen ligt bij de eigenaar van het proces. Bijvoorbeeld Stadsbeheer moet zorgen voor de juiste maatregelen (zoals updates) voor hun handhavingssysteem. De CISO of security officer per gemeentelijke afdeling is hierin adviserend.

### 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 preventie, detectie én response. Zorg in ieder geval dat de gemeentelijke systemen voorzien zijn van de laatste updates en zorg ervoor dat de eigen werknemers alert zijn op phishingmails en sterke wachtwoorden hebben. Als de gemeentelijke systemen alsnog schade wordt aangebracht, is dit niet meer alleen het probleem van de afdeling ICT, maar raakt het de hele gemeentelijke organisatie doordat bijvoorbeeld niet meer (veilig) kan worden gewerkt. Zorg als gemeente voor een zorgvuldige risico-afweging en duidelijke procedures als er problemen zijn met de ICT en de informatiebeveiliging.

### Wegenwacht

- Als gemeente kun je de hulp inroepen van de Informatie-beveiligingsdienst (IBD); een onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD adviseert hoe de gemeente het beste kan handelen en staat je bij voor advies op woordvoering. De IBD functioneert hier als de gemeentelijke CERT (Computer Emergency Response

Teams). De CERT is aangesloten bij het Nationaal Cyber Security Centrum (NCSC) en ontvangen daar ook belangrijke informatie (risico's, kwetsbaarheden) van. Naast het bieden van hulp, zal de IBD gemeenten zelf ook actief informeren als er belangrijke gevaren dreigen.
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 de bestuurder daarbij.
https://www.informatiebeveiligingsdienst.nl/ciso-toolkit/
- Bekijk het overzicht van kennisproducten op het gebied van Informatiebeveiliging en Privacy voor Baseline informatiebeveiliging overheid (BIO).
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
- Laat bestuurders de IBD-crisisgame spelen zodat zij bewust worden van de bestuurlijke gevolgen en belangen tijdens een cybercrisis.
https://www.informatiebeveiligingsdienst.nl/ibd-crisisgame/
- Lees de factsheet: "Gehackt, hoe nu verder".
https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/
- De Toolbox cyberincident neemt gemeenten mee in de verschillende stappen die je kunt zetten bij een cyberincident: rapporteren, beoordelen, bijeenroepen, uitvoeren en oplossen.
https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/oefenen-en-kennisdelen/toolbox-cyberincident/
- Zie ook de 'Agenda digitale veiligheid' van de VNG, die uiteenzet welke concrete actielijnen komende jaren binnen het lokaal bestuur worden ontwikkeld, óók om het eigen huis op orde te krijgen.
https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

**VOORBEELDEN**

- **Citrix:** https://www.informatiebeveiligingsdienst.nl/nieuws/kwetsbaarheden-in-citrix-lessen-voor-gemeenten-en-de-ibd/
- **Gemeente Lochem:** https://www.informatiebeveiligingsdienst.nl/product/leren-van-lochem-lessen-uit-een-informatiebeveiligingsincident/

## "Onze digitale veiligheid staat voortdurend onder druk"

*Het is niet de vraag geweest óf er een keer iets flink mis zou gaan in de 'digitale wereld', maar wel wannéér dat zou gebeuren. Dat zei Ferd Grapperhaus, toenmalig minister van Justitie en Veiligheid, na aanleiding van de beveiligingsproblemen met de citrix-software in januari 2020.*

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.