



Agenda digitale veiligheid 2028

Digitale veiligheid is de (gedrags)norm in onze gemeenten

Inhoud

Voorwoord	3
Inleiding	5
Hoofdthema's	7
Vorbereiding op digitale ontwrichting	7
Weerbare inwoners en ondernemers	8
Eigen huis op orde - robuuste informatiebeveiliging	9
Randvoorwaarden	12
Onderliggende thema's	13
Vorbereiding op Europese en nationale wet- en regelgeving	13
Leiderschap en professionalisering digitale veiligheid bij de lokale overheid	13
Arbeidsmarktkrapte het hoofd bieden	14
Conclusie	15

Voorwoord

Digitalisering en de inzet van nieuwe technologieën zoals kunstmatige intelligentie (AI) bieden veel kansen, maar brengen ook een groeiend aantal risico's met zich mee. Steeds meer voorzieningen, waar we als samenleving afhankelijk van zijn, zijn gedigitaliseerd. Denk aan de infrastructuur, voedselvoorziening, gezondheidszorg en onderwijs. Het is belangrijk dat deze functies betrouwbaar en veilig zijn. Maar dat is niet vanzelfsprekend. Het vraagt om een kritische blik op onze groeiende afhankelijkheid van technologie: wat vinden we acceptabel en wat kunnen we lokaal doen om de risico's te beheersen en kansen te benutten?

Het dreigingsbeeld is veranderd. Criminelen zijn niet alleen uit op financieel gewin, zij zetten technologische mogelijkheden ook in voor destabiliserende activiteiten. Steeds vaker zijn het statelijke actoren, die zich richten op het verstoren van essentiële processen en maatschappelijke ontwrichting. Dit maakt de samenleving kwetsbaar. Het tempo en de complexiteit van digitale aanvallen nemen toe. Vaak zijn criminele actoren maanden ongemerkt in de systemen aanwezig voordat zij hun aanval uitvoeren. Hiermee kunnen ze essentiële dienstverlening voor langere tijd verstoren.

Gemeenten zijn verantwoordelijk voor de digitale veiligheid van hun gemeente, hun inwoners, ondernemers en de eigen organisatie. In de steeds complexer wordende informatiesamenleving hebben we dagelijks met digitale veiligheidsvraagstukken te maken. De scheiding tussen online en offline wereld vervaagt. Criminelen doen zich online voor als bekenden of (officiële) instanties. Met gelekte of geroofde persoonsgegevens vindt inmiddels een wereldwijde handel plaats. Wanneer inwoners slachtoffer van online- of identiteitsfraude worden, worden zij in hun bestaanszekerheid geraakt. Dat vraagt om aandacht voor de digitale weerbaarheid van de samenleving en een veilige gemeentelijke dienstverlening. Er zijn afspraken nodig over hoe we omgaan met AI, deepfakes en fake news, en welke rol de gemeente daarin speelt.

De digitale dreiging is voor gemeenten de afgelopen jaren steeds groter geworden. De digitale weerbaarheid kan daarop niet achterblijven. Gemeenten kunnen de uitdagingen op het gebied van de digitale veiligheid vaak niet alleen aan. Ze maken deel uit van gemiddeld 30 samenwerkingsverbanden en gebruiken diensten van derden, zoals softwareleveranciers. Via ketenpartners en toeleveranciers, maar ook via medewerkers, weten kwaadwillenden steeds vaker door de digitale verdediging heen te breken. Zo'n digitaal incident in de keten kan de gemeentelijke dienstverlening verstoren, waardoor gevoelige gegevens in verkeerde handen kunnen vallen. Dit vraagt om robuuste informatiebeveiliging en privacybescherming. Slimme technologie in de fysieke leefomgeving en vitale infrastructuur die op afstand wordt uitgelezen of aangestuurd, zoals bruggen, gemalen, sluizen en verkeersregelingssystemen, kan ook op afstand gemanipuleerd worden door kwaadwillenden.

Honderd procent veiligheid bestaat niet, maar informatiebeveiliging is een belangrijke voorwaarde. Gericht risicobeheer is noodzakelijk, waarbij digitale risico's net als juridische en financiële risico's worden meegewogen. Daarbij moeten gemeenten zich goed voorbereiden op en snel kunnen handelen bij digitale verstoringen, incidenten en crises, of aanvallen van criminele netwerken of statelijke actoren. Dit vraagt om een digitaal veiligheidssysteem in samenhang met het fysieke veiligheidssysteem, een sterke lokale informatiepositie, de juiste expertise aan boord en structurele financiering. Bovendien is er aandacht nodig voor preventie, zoals het versterken van de digitale weerbaarheid van specifieke doelgroepen die kwetsbaar zijn voor online criminaliteit. Door te investeren in digitale veiligheid kunnen gemeenten niet alleen hun eigen dienstverlening beschermen, maar ook bijdragen aan een veiligere digitale omgeving voor hun inwoners en ondernemers.

Digitale veiligheid is cruciaal voor gemeenten om verschillende redenen:

- **Continuïteit van dienstverlening:** Gemeenten bieden tal van digitale diensten aan al hun inwoners en ondernemers. Een cyberaanval kan deze diensten verstoren, wat kan leiden tot grote problemen voor inwoners of de bredere samenleving.
- **Vertrouwen in de integriteit van de overheid:** Het beschermen van bestuurders en ambtenaren tegen integriteitsschendingen, het organiseren van actieve ondersteuning van inwoners en ondernemers en het zorgen voor snel herstel na digitale incidenten, helpt om het vertrouwen in de overheid te waarborgen en polarisatie te voorkomen.
- **Weerbaarheid tegen cybercriminaliteit:** Gemeenten moeten hun digitale dienstverlening beschermen en de weerbaarheid van hun inwoners en ondernemers versterken tegen gedigitaliseerde criminaliteit en cybercrime, zoals phishing en ransomware-aanvallen.
- **Bescherming van gevoelige informatie:** Gemeenten beheren veel persoonlijke en gevoelige gegevens van inwoners. Het is essentieel om deze informatie te beschermen tegen cyberaanvallen en datalekken.
- **Omgang met online aangejaagde ordeverstoringen:** Het vroegtijdig signaleren van en anticiperen op online opruiing en daaruit voortkomende openbare ordeverstoringen.
- **Voorbereiden op digitale ontwrichting:** In het kader van crisisbeheersing kunnen gemeenten zich (in de koude fase) voorbereiden op digitale ontwrichting, incidenten en crises met maatschappelijke gevolgen en cascade-effecten. De vraag is immers niet of digitale ontwrichting zich kan voordoen, maar wanneer.
- **Economische stabiliteit:** Een goed beveiligde digitale infrastructuur draagt bij aan het draaiende houden van de lokale economie en het waarborgen van de welvaart.
- **Naleving van wet- en regelgeving:** Er zijn steeds meer Europese en nationale wetten en regels die eisen stellen aan digitale veiligheid. Gemeenten moeten hieraan voldoen om juridische en financiële risico's te vermijden.

Maar hoe ga je hier als lokale bestuurder mee om? En wat is er nodig om tot een betere, veilige digitale samenleving te komen? Daarom is er nu de Agenda Digitale Veiligheid 2028, waarin we vastleggen wat er nodig is om gemeenten te helpen op weg naar digitale veiligheid.

Deze *Agenda Digitale Veiligheid, de (gedrags)norm in onze gemeenten* is een vervolg op de eerdere versie uit 2020. Het bouwt voort op wat de afgelopen jaren al is bereikt. Daarnaast is de Agenda Digitale Veiligheid verbonden met zowel de *Verenigingsstrategie VNG 2030 Stap naar voren*, als de in september 2024 gelanceerde *Digitale Agenda Gemeenten 2028 Regie op één digitale samenleving*. De Digitale Agenda Gemeenten 2028 stelt drie principes centraal om te sturen op digitalisering: door te normeren en te democratiseren, door mogelijk te maken en door kansen te benutten.

Inleiding

In de huidige digitale samenleving is het waarborgen van digitale veiligheid een cruciale taak voor gemeenten. Burgemeesters, wethouders, ambtenaren en raadsleden staan voor de uitdaging om hun gemeenten te beschermen tegen groeiende dreigingen van cybercriminaliteit en digitale verstoringen en een veilige digitale samenleving te creëren voor alle inwoners.

Eén van de grootste uitdagingen daarbij is het voldoen aan de steeds complexer wordende Europese Digital Decade wet- en regelgeving. Daaronder vallen onder andere de privacywetgeving en verschillende cyberbeveiligingswetten. Deze regelgeving vereist een proactieve en goed gecoördineerde aanpak om de digitale weerbaarheid van gemeenten te versterken.

Daarnaast is er een dringende behoefte aan sterk leiderschap en professionalisering binnen de interne organisatie. Gemeenten moeten investeren in de ontwikkeling van vaardigheden en kennis van hun medewerkers om effectief te kunnen reageren op digitale dreigingen. Bovendien is er in Nederland een tekort aan gekwalificeerd personeel op het gebied van digitale veiligheid, wat de noodzaak voor samenwerking en gerichte wervings- en opleidingsprogramma's benadrukt.

Met de Agenda Digitale Veiligheid bieden we perspectief voor lokale bestuurders en zoeken we synergie om de gemeentelijke beleids- en uitvoeringspraktijk te ondersteunen: zowel voor de digitale veiligheid van de gemeentelijke dienstverlening als de digitale weerbaarheid van de inwoners en ondernemers. Centraal in onze voorstellen aan het rijk zetten we de lokale opgave voor een digitaal veiligheidsstelsel, een sterke informatiepositie en structurele financiering. Beleid, wet- en regelgeving moeten haalbaar, betaalbaar en uitvoerbaar zijn voor het lokaal bestuur.

De toekomst van digitale veiligheid voor gemeenten ligt in een geïntegreerde en proactieve aanpak en het werken aan goed voorbeeldgedrag. Door samen te werken en kennis te delen, kunnen gemeenten een robuuste digitale infrastructuur opbouwen die bestand is tegen de uitdagingen van morgen.

Wij werken daarom de komende jaren verder aan de volgende hoofdthema's:

- **Voorbereiding op digitale ontwrichting:** Gemeenten moeten voorbereid zijn op mogelijke digitale ontwrichting met grote maatschappelijke gevolgen en cascade-effecten. Dit vraagt om een digitaal veiligheidsstelsel dat in samenhang werkt met het fysieke veiligheidsstelsel.
- **Weerbare inwoners en ondernemers:** Het is cruciaal om inwoners en ondernemers te informeren en te trainen in digitale veiligheid, zodat zij zelfredzaam en weerbaar zijn tegen digitale bedreigingen.
- **Eigen huis op orde - robuuste informatiebeveiliging:** Een solide basis van informatiebeveiliging is noodzakelijk. Dit omvat integraal risicomanagement, waarbij digitale risico's en privacybescherming gelijk worden meegewogen met de juridische en financiële risico's. Het planmatig implementeren van sterke beveiligingsmaatregelen, het monitoren en het regelmatig testen en updaten van systemen van de gemeentelijke dienstverlening en de fysieke leefomgeving worden een regulier onderdeel van het procesmanagement.

Voor deze drie hoofdthema's zijn de volgende onderliggende thema's van belang:

- **Voorbereiding op Europese en nationale wet- en regelgeving:** Gemeenten moeten zich voorbereiden op en voldoen aan de steeds veranderende Europese en nationale regelgeving op het gebied van digitale veiligheid. Het is van belang dat deze regelgeving in samenhang lokaal uitvoerbaar, haalbaar en betaalbaar is.
- **Leiderschap en professionalisering van digitale veiligheid bij de lokale overheid:** Sterk en integer leiderschap en voortdurende professionalisering van verschillende functies in de gemeente zijn essentieel om digitale veiligheid effectief te beheren en te verbeteren.

- **Arbeidsmarktkrapte het hoofd bieden:** Het aantrekken, behouden en opleiden van voldoende gekwalificeerd personeel is een uitdaging die moet worden aangepakt om de continuïteit en kwaliteit van digitale veiligheid te waarborgen.

Om deze uitdagingen succesvol aan te pakken moet wel aan een aantal randvoorwaarden worden voldaan:

- Structurele middelen voor gemeenten om de digitale veiligheid te verhogen.
- Een digitaal veiligheidstelsel dat samenhangt met het fysieke veiligheidstelsel.
- Een sterke informatiepositie van gemeenten op digitale veiligheid.

Door het uitwerken van deze thema's werkt de Agenda Digitale Veiligheid 2028 aan een veilige digitale toekomst met alle gemeenten.

Hoofdthema's

Voorbereiding op digitale ontwricting

Organisaties lopen een risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze aanbieden en/of de mogelijke buit die er te halen is. Statelijke actoren kunnen heimelijk toegang verkrijgen tot digitale systemen van overheden en (vitale) bedrijven. Hierbij kan het doel digitale spionage, beïnvloeding en/of sabotage zijn om strategische doelen te behalen.

Cyberweerbaarheid staat voor het vermogen van organisaties om cybersecuritydreigingen te herkennen en hier adequaat op te anticiperen. De aanname is dat iedere organisatie in de loop der tijd te maken krijgt met een cybersecurityincident. Dit betekent dat organisaties zich niet alleen moeten richten op preventieve maatregelen om een incident te voorkomen, maar ook op detectie en respons. De cyberbeveiligingswetten voorzien in wettelijke maatregelen om het algemene niveau van cyberbeveiliging te verhogen, met een zorgplicht, extern toezicht en meldplicht.

Online aangejaagde ordeverstoringen

Gemeenten worden steeds vaker geconfronteerd met online aangejaagde ordeverstoringen, waarbij via sociale media oproepen worden gedaan en mensen zich snel kunnen organiseren om de openbare orde te verstoren. Ook hebben geopolitieke ontwikkelingen ertoe geleid dat statelijke actoren in toenemende mate een dreiging vormen voor de nationale veiligheid. De impact van cyberveiligheid en de dreigingen van statelijke actoren reiken ook tot het niveau van de lokale overheid. De online en offline leefwereld zijn inmiddels niet meer van elkaar te onderscheiden en kennen lokale beïnvloeding en druk op gemeentebestuurders.

De fysieke gevolgen van online uitingen kunnen onvoorspelbaar zijn en de aanpak hiervan vereist meer tijd, geld en mankracht van gemeenten en politie. De bestuurders willen aan de voorkant voorzieningen kunnen treffen om wanordelijkheden in het fysieke domein te voorkomen, zoals een meldpunt waar bestuurders desinformatie, schadelijke content en online opruiende berichten kunnen melden.

Om digitale veiligheid naar een hoger niveau te tillen is een sterke informatiepositie nodig over de rolverdeling en verantwoordelijkheden bij crises. Voorbeelden hiervan zijn: kaders voor gemeentelijk onlineonderzoek, de online bevoegdheden van het lokaal bestuur en de voorbereiding op digitale ontwricting.

We werken een digitaal veiligheidsstelsel in relatie tot het fysieke veiligheidsstelsel verder uit. Het denken over digitale veiligheid wordt verder geïntegreerd met de reguliere denkbeelden over veiligheid. Netwerkpartners zijn in beeld en de communicatie en samenwerking met hen wordt duidelijk ingericht. De samenwerking met de veiligheidsregio's wordt versterkt, zodat digitale verstoringen met fysieke gevolgen, -incidenten en -crises snel hersteld kunnen worden. Voor een adequaat optreden van het gemeentebestuur is een lokaal integraal informatiebeeld essentieel.

Ambities voor 2028:

- In het digitale veiligheidsstelsel zijn taken, verantwoordelijkheden en bevoegdheden geconcretiseerd, uitgebreid en vastgelegd. Gemeenten hebben een goede informatiepositie met betrekking tot (geopolitieke) ontwikkelingen en de effecten op de digitale veiligheid op lokaal niveau. Hierover zijn afspraken gemaakt met de veiligheidspartners en de gemeenten, zowel met de afdelingen Informatiebeveiliging als Openbare orde en veiligheid.
- Oefenen is gemeengoed: periodiek worden cybercrisoefeningen uitgevoerd, zowel intern als in samenwerking met de veiligheidsregio's. De geleerde lessen worden direct opgepakt en actief

met elkaar gedeeld. De rollen en verantwoordelijkheden zijn duidelijk en worden preventief, tijdens de *koude fase*, regelmatig bekeken. Scenario's en handreikingen binnen de veiligheidsregio's en in de driehoek zijn beschikbaar en worden ook breed gebruikt.

- Er is een meldvoorziening waar bestuurders melding kunnen doen van onrechtmatige of schadelijke online content. De aanvullende bestuursrechtelijke bevoegdheden bij online aangejaagde ordeverstoringen zijn uitgewerkt en gemeenten beschikken over een monitoringtool voor de informatieverzameling en -verwerking binnen de juridische kaders van openbare orde en veiligheid.
- Bestuurders en gemeentelijke ambtenaren zijn zich bewust van het onderwerp statelijke dreigingen en hoe statelijke actoren een dreiging kunnen vormen op het gebied van digitale veiligheid op lokaal niveau. Gemeenten weten wat de risico's zijn, waar hun verantwoordelijkheden liggen en hoe ze kunnen handelen.

Weerbare inwoners en ondernemers

Cybercrime en gedigitaliseerde criminaliteit zijn groeiende zorgen binnen het veiligheidsdomein. Op deze toenemende dreiging blijft de (cyber)weerbaarheid van onze samenleving achter. Dit vraagt om een gezamenlijke maatschappelijke aanpak om inwoners en ondernemers weerbaar te maken. Gemeenten spelen daar een cruciale rol in en staan in nauw contact met hun inwoners en ondernemers. De aanpak van cybercriminaliteit is opgenomen in het Integraal Veiligheidsplan van gemeenten.

Uit de cijfers van het Veiligheidsonderzoek van CBS blijkt dat 16% van de Nederlandse bevolking in 2023 slachtoffer is geweest van online criminaliteit. Als je kijkt naar het totaal aantal slachtoffers in Nederland, dan is 42% slachtoffer van online criminaliteit en 58% van traditionele criminaliteit. Online oplichting, online fraude en hacks zijn de meest voorkomende vormen hiervan (CBS, 2023). Cybercriminelen worden daarnaast steeds professioneler, waardoor het moeilijker wordt om pogingen tot cybercrime tijdig te herkennen (OM, z.d). Inwoners en ondernemers ondervinden psychische, emotionele en financiële gevolgen van online criminaliteit (CBS, 2023) en het vertrouwen in elkaar en in digitale infrastructuur wordt hierdoor aangetast (Digitale Overheid, 2024).

Ook blijkt uit onderzoek van het CBS dat slechts 17% van de slachtoffers van online criminaliteit aangifte doet. Het lage aantal heeft meerdere oorzaken: slachtoffers schamen zich, zijn zich niet bewust dat ze een misdrijf hebben ondergaan, de schade is beperkt of wordt vergoed of ze gaan ervan uit dat de daders toch niet opgespoord worden (NSCR, 2023). De lage aangiftebereidheid heeft tot gevolg dat gemeenten en andere partners onvoldoende zicht krijgen op verschijningsvormen van cybercrime en gedigitaliseerde criminaliteit, wie de daders zijn (de daderprofielen) en wie de slachtoffers zijn (de slachtofferprofielen). Tegelijkertijd is dit een criminaliteitsvorm met een relatief lage pakkans. Hierdoor heeft de politie en OM weinig zicht op de aard en omvang van digitale criminaliteit en lopen veel daders nog vrij rond. Om deze vicieuze cirkel te doorbreken, is intensievere samenwerking met politie en OM nodig met een sterkere informatiepositie voor gemeenten. Het inzicht in online criminaliteit en in de verschijningsvormen hiervan is cruciaal om interventies op lokaal niveau te kunnen bepalen. Daarnaast is het van belang dat de verantwoordelijkheden en rolverdeling tussen gemeente, politie en OM in de aanpak van online criminaliteit helder zijn vastgelegd.

Ambities voor 2028:

- In de integrale en systematische aanpak van cybercrime en gedigitaliseerde criminaliteit zijn de rollen en verantwoordelijkheden van gemeenten, politie en OM vastgelegd. De lokale partijen weten wat zij van elkaar kunnen verwachten en nemen hun verantwoordelijkheid in de integrale aanpak van cybercrime en gedigitaliseerde criminaliteit. In samenwerking met relevante lokale partners (bibliotheken, hulpverleners, scholen, PVO's) verhogen zij de digitale weerbaarheid van inwoners en ondernemers.
- Gemeenten ondersteunen inwoners en ondernemers bij het vergroten van hun digitale weerbaarheid. Hiervoor beschikken gemeenten over voldoende financiële middelen, expertise en

mankracht om het onderwerp cybercrime en gedigitaliseerde criminaliteit op te pakken.

- Met periodieke (politie)regionale cyberbeelden over cybercrime en gedigitaliseerde criminaliteit kunnen gemeenten de benodigde inzet bepalen en hebben zij zicht op snel veranderende modus operandi van cybercriminelen. Zij hebben effectieve en uitvoerbare interventies die zij kunnen inzetten om de digitale weerbaarheid van inwoners en ondernemers te verhogen. Dit stelt hen in staat om snel in te spelen op nieuwe verschijningsvormen van cybercrime en gedigitaliseerde criminaliteit.
- De VNG biedt een platform voor het verspreiden van best practices voor het verhogen van digitale weerbaarheid van inwoners en ondernemers. Daarnaast verbindt de VNG verschillende partijen en hun initiatieven met elkaar zodat synergievoordelen in het versterken van digitale weerbaarheid behaald kunnen worden. Ook pleit de VNG voor structurele financiële middelen voor gemeenten, om de lokale aanpak cybercrime en gedigitaliseerde criminaliteit goed vorm te kunnen geven.

Eigen huis op orde - robuuste informatiebeveiliging

Met het team Digitale Veiligheid, de Informatiebeveiligingsdienst (IBD) en ENSIA (Eenduidige Normatiek Single Information Audit) ondersteunen we gemeenten in de versterking van hun digitale weerbaarheid. Bestuurders moeten zich uitermate bewust zijn van de noodzaak van informatiebeveiliging en privacy. Net als financiën moeten informatiebeveiliging en privacy een vast onderdeel van de risicoafwegingen zijn, standaard op de agenda staan en eenzelfde controlecyclus doorlopen. Alleen op deze manier krijgen gemeenten hun informatiebeveiliging en privacy onder controle.

Basis op orde

Nederlandse gemeenten implementeren risicogebaseerd de beheersmaatregelen voor informatiebeveiliging en gaan slim samenwerken voor de implementatie van de Cyberbeveiligingswet (Cbw), de onderliggende BIO2.0 en andere wetten van de EU Digital Decade Program. Dit omvat een efficiënte en samenhangende aanpak van informatiebeveiliging en gegevensbescherming, waarbij kosten in balans zijn met de feitelijke veiligheid en continuïteit van dienstverlening.

Risicomanagement

Voor gegevensbescherming en informatiebeveiliging is risicomanagement onderdeel van de dagelijkse bedrijfsvoering binnen een gemeentelijke organisatie. Gemeenten bevinden zich op een dynamisch speelveld waarin de dienstverlening en werkwijze snel veranderen. Dit heeft te maken met de politieke omgeving, maar ook de snelle digitalisering van de afgelopen jaren. Hierdoor is risicomanagement een doorlopend proces en essentieel om vermijdbare digitale incidenten te voorkomen.

Sterk leveranciersmanagement en opdrachtgeverschap

Gemeenten gebruiken veelal (cloud)diensten van derden, zoals softwareleveranciers. Met deze afhankelijkheid van een beperkt aantal aanbieders is het belangrijk om kritisch te blijven kijken naar onze groeiende afhankelijkheid van technologie. Gemeenten stellen grenzen aan wat ze acceptabel vinden en beperken zo de risico's van technologie vanuit landen met een offensief cyberspionageprogramma.

De cyberbeveiligingswetgeving stelt eisen aan bestuurders met betrekking tot waarborgen in de toeleveranciersketens. Hoewel die wetgeving zich richt op juridische aspecten en aantoonbaarheid van digitale veiligheid, is er voor de daadwerkelijke veiligheid meer regie nodig op het gebied van inkoop en leveranciersmanagement. De Agenda Digitale Veiligheid werkt samen met de rijksoverheid en andere medeoverheden aan eenduidigheid in leveranciersmanagement. Hierbinnen staan de afstemming van inkoopinitiatieven en de harmonisatie van inkoop-eisen centraal. Dit biedt duidelijkheid aan welke wettelijke verplichtingen leveranciers moeten voldoen en waar aanvullende wettelijke kaders of contractuele afspraken noodzakelijk zijn, met name ook voor IT- en OT-leveranciers.

Incidenten beheersen

Voor de continuïteit van de bedrijfsvoering en processen is het van belang dat gemeenten zich goed voorbereiden op en snel kunnen handelen bij digitale verstoringen, incidenten en crises, of aanvallen van criminele netwerken of statelijke actoren. Met gerichte oefenprotocollen kan de gemeente met partners in het veiligheidsveld de inrichting van de crisisorganisatie toetsen en de afhandeling van incidenten en crises oefenen. Het streven is om het aantal vermijdbare digitale incidenten vanaf 2028 zoveel mogelijk te beperken, en daarmee de basis te leggen om deze in 2030 volledig te voorkomen.

Verantwoording en toezicht

Gemeenten verantwoorden horizontaal aan de gemeenteraad als hoogste politieke orgaan. De informatie die hiervoor wordt gebruikt kan ook dienen voor de verantwoording aan de verticale toezichthouder (RDI) en individuele stelselhouders. Het toezichtregime van de Cbw concentreert zich op de risico's die gemeenten lopen bij de uitvoering van hun taken en houdt tegelijkertijd rekening met de toezichtregimes van andere EU-wet- en regelgeving die voortkomen uit de Digital Decade. Dit betekent een verschuiving van een jaarlijkse totaalverantwoording van de BIO naar een strategische focus op de meest urgente risico's.

In de samenwerking met de rijksoverheid zijn de uitgangspunten: het verminderen van auditlasten door het gebruik van bestaande regimes, harmoniseren van verticale verantwoordingseisen en de overgang naar *continuous auditing en monitoring*.

Ambities voor 2028:

- De Cbw is duidelijk uitgewerkt voor gemeenten. Het is duidelijk wat de gemeenten nodig hebben om te voldoen aan de zorg- en meldplicht.
- De rol en dienstverlening van de IBD als CSIRT zijn bekend bij gemeenten.
- Het is duidelijk wat het toezichtkader betekent in relatie tot ENSIA en wat gemeenten hiervoor aan moeten passen voor het horizontaal toezicht aan de gemeenteraad en de nieuwe externe toezichthouders. Ook is duidelijk welke sancties de externe toezichthouders kunnen opleggen.
- Voor de inzet van technologie in de gemeentelijke domeinen worden de afgesproken kaders voor ethiek, grondrechten en digitale veiligheid toegepast.

Informatiebeveiligingsdienst (IBD) als Computer Emergency Response Team en Computer Security Incident Response Team (CSIRT)

De IBD is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

De IBD is een frontrunner binnen het LDS (Landelijk Dekkend Stelsel) door de inzet van EASM (Enterprise Attack Surface Management) tooling. Deze tooling zorgt voor het extern scannen van de IT-omgevingen van gemeenten op kwetsbaarheden in hardware en software. Deze tooling geeft invulling aan de eis die NIS2 stelt aan een sectorale CERT met betrekking tot het scannen van hun entiteiten. Via deze dienstverlening en tooling worden dreigingsanalyses uitgevoerd en worden de geïdentificeerde risico's per organisatie gedeeld met alle gemeenten. Met dit platform en de dienstverlening die we daarmee bieden, kan de IBD centraal de regie voeren op risico's bij alle aangesloten organisaties.

De IBD vormt eveneens het centrale informatiepunt bij incidenten. Ook adviseert de IBD de gemeenten bij de implementatie van de Baseline Informatiebeveiliging Overheid (BIO) en aanverwante standaarden. Om gemeenten te helpen met het verhogen van de digitale weerbaarheid heeft de IBD het ondersteuningspakket Verhogen Digitale Weerbaarheid (VDW) ontwikkeld.

ENSIA (Eenduidige Normatiek Single Information Audit)

Alle Nederlandse gemeentebesturen leggen jaarlijks, op één en hetzelfde moment, via één en dezelfde methode, verantwoording af over hun informatieveiligheid, datakwaliteit en data-integriteit. Het op orde hebben van deze zaken is belangrijk voor de gegevensbescherming en de continuïteit van de dienstverlening, denk aan het verstrekken van uitkeringen of het uitgeven van paspoorten. Inwoners en ondernemers mogen erop vertrouwen dat gemeenten dit goed hebben geregeld.

Gemeenten verantwoorden zich al zeven jaar via de ENSIA-methode aan de gemeenteraad en toezichthouders binnen de rijksoverheid. Per 2026 hebben gemeentebestuurders de wettelijke plicht (met toezicht, meldplicht en sancties) om, eveneens via ENSIA, aan te tonen dat de informatiebeveiliging op orde is. Het verantwoordingsmoment is ook hét vaste jaarlijkse moment waarop het college, risicogericht, de noodzakelijke verbeteringen doorvoert in de eigen organisatie. Gemeenten kunnen hierbij gebruik maken van het aanbod van de IBD. De ENSIA-systematiek sluit aan op de planning en controlcyclus van de gemeente en bestaat uit digitale vragenlijsten die gemeenten zelf doorlopen, met op onderdelen een externe audit.

De VNG stelt gemeenten in staat om collectief de wensen van vandaag en de uitdagingen van de toekomst het hoofd te bieden. Zo zorgen we er samen met gemeenten voor dat ENSIA meer inzicht in de werking van genomen maatregelen geeft. En onderzoeken we de integratie van bestaande en nieuwe wetgeving in ENSIA om auditlasten te beperken. We behartigen de belangen van gemeenten richting rijk en onderhouden contact met partners.

Het ENSIA-team van de VNG heeft klanttevredenheid en gebruiksvriendelijkheid hoog in het vaandel staan. Het ondersteunt daarom ENSIA-coördinatoren in de gemeente bij de zelfevaluatie, bij het voeren van 'het goede gesprek' over de inzichten met (de portefeuillehouder van) het college en bij het afleggen van verantwoording aan college en raad. Dat kan met behulp van praktische producten en diensten, een forum en een helpdesk. Het team stimuleert en faciliteert ook kennisuitwisseling tussen ENSIA-coördinatoren onderling.

Randvoorwaarden

Om effectief aan de slag te gaan met het thema digitale veiligheid zijn, zowel voor weerbare inwoners en ondernemers als voor de gemeentelijke organisatie, op lokaal niveau de volgende randvoorwaarden noodzakelijk:

- Om de uitdagingen het hoofd te bieden, is **structurele financiering** voor digitale veiligheid voor gemeenten essentieel. Gemeenten moeten beschikken over voldoende middelen om duurzame veiligheidsmaatregelen te implementeren en te onderhouden.
- Daarnaast is het van belang om een **digitaal veiligheidsstelsel** te ontwikkelen dat nauw samenwerkt met het fysieke veiligheidsstelsel. Dit omvat duidelijke verantwoordelijkheden en oefenprotocollen voor alle betrokken rollen, zodat er snel en effectief kan worden gereageerd op incidenten.
- Een **optimale informatiepositie** is eveneens cruciaal, zodat gemeenten beschikken over actuele en gedetailleerde informatie over de digitale veiligheid binnen hun grenzen. Dit omvat een cyberbeeld dat zowel lokaal als regionaal inzicht geeft in cybersecurity, cybercrime en de status van kritieke entiteiten.

Onderliggende thema's

De implementatie kan pas soepel verlopen als het bij gemeenten niet op te hoge kosten, capaciteitsproblemen of andere issues stuit. Daarom moeten we ook werken aan de volgende onderliggende thema's:

Vorbereiding op Europese en nationale wet- en regelgeving

Het Europese beleidsprogramma 'Digital Decade' moet ervoor zorgen dat Europa klaar is om de digitale transformatie door te maken. Met een samenhangend pakket aan wet- en regelgeving, standaarden en een digitale infrastructuur wil de Europese Commissie de digitale transformatie van Europa vormgeven. Dit heeft ook invloed op de Nederlandse wet- en regelgeving. De Europese richtlijnen worden in Nederland door verschillende vakministers uitgewerkt en omgezet in nationale wetgeving. Dit zorgt voor een versnipperd beeld. Deze wetten hebben grote impact op de informatiebeveiliging en gegevensbescherming bij gemeenten en andere overheden. Om de belangen van lokale uitvoering te waarborgen en kansen te benutten, is een planmatige en financieel onderbouwde aanpak vanuit het rijk noodzakelijk.

Ambities voor 2028:

De VNG zet zich in om de implementatie van de nieuwe richtlijnen voor gemeenten zo haalbaar, betaalbaar en uitvoerbaar mogelijk te maken. Er is nauw contact met onder andere de betrokken ministeries over de totstandkoming van de wetteksten en de implicaties hiervan voor lokale overheden. Het gaat dan om:

- Een duidelijke scope en de verantwoordelijkheidsverdeling tussen de partijen.
- Geharmoniseerd toezicht op informatiebeveiliging bij de overheid.
- Vermindering van de auditlast.

Tegelijkertijd moeten gemeenten worden geholpen met de voorbereiding op de implementatie. Vanuit deze Agenda Digitale Veiligheid werken we collectieve oplossingen uit voor gemeenten en versterken we lokale bestuurders als opdrachtgever van ICT-diensten en bij inkoop, contract- en leveranciersmanagement van digitale technologie.

Leiderschap en professionalisering digitale veiligheid bij de lokale overheid

De VNG versterkt de professionalisering op het terrein van digitale veiligheid van gemeentelijke ambtelijke experts (zoals de adviseur openbare orde en veiligheid, chief information security officer, functionaris gegevensbescherming en privacy officer) en van de gemeentebestuurders (burgemeesters, gemeentesecretarissen, wethouders en raadsleden). Met intervisie en gerichte trainingen helpt de VNG de verschillende gemeentefunctionarissen om onderling de rollen te versterken, kennis te delen en te reflecteren op opgedane ervaringen.

Ambities voor 2028:

- Gemeentebestuurders krijgen een realistisch handelingsrepertoire aangereikt voor het voorkomen van, prepareren op en afwenden van cyberincidenten. Hiermee raken gemeentebestuurders vertrouwd met het interpreteren van het integrale lokale dreigingsbeeld en het meten, bewaken en verantwoorden van de feitelijke digitale veiligheid in de gemeenten. Dit geldt zowel voor de digitale als fysieke openbare ruimte. Zo groeien gemeenten in bestuurlijke materiekennis en lenigheid in digitale veiligheidssituaties.
- Gemeenten hebben de governance over digitale veiligheid op orde gebracht. Bewustwording wordt ingebed in de gemeentelijke organisaties bij alle betrokken functionarissen. Alle gemeenten voeren periodiek het bestuurlijke gesprek met de burgemeester, gemeentesecretaris, OOV-er,

CISO en FG/Privacy Officer over de breedte van digitale veiligheid en de bestuurlijke dilemma's die zij hierin ondervinden. Hierdoor stimuleren we de groei in (inter-)bestuurlijk integraal risicomanagement.

- Gemeenteraden en colleges zijn betrokken bij het brede thema digitale veiligheid, ook als dat zich deels afspeelt in gemeenschappelijke regelingen en samenwerkingsverbanden. Het is zaak dat gemeenten ketenregie en democratisch toezicht op gemeenschappelijke regelingen houden. De VNG vervult de platformfunctie om praktijkvoorbeelden en geleerde lessen onderling uit te ruilen, kennis en onderzoeksresultaten te delen, intervisie over digitale veiligheid te faciliteren en gemeentebestuurders te ondersteunen in het voeren van het gesprek met de gemeenteraad. We werken daarin samen met het onderwijsveld en de arbeidsmarkt.

Arbeidsmarktkrapte het hoofd bieden

Het tekort aan cybersecurity- en OOV-professionals met kennis en kunde op het gebied van digitale veiligheid is in heel Nederland een probleem. De VNG ondersteunt gemeenten bij het vissen in deze kleine vijver en biedt oplossingen voor zowel de korte als lange termijn. Met het project Arbeidsmarktkrapte onderzoeken we wat het daadwerkelijke tekort is bij gemeenten, creëren we meer stage- en traineeplekken met gepaste arbeidsvoorwaarden, vergroten we de effectiviteit via om- en bijscholing van het huidige personeelsbestand en adviseren we over de inzet van technologische oplossingen.

Ambities voor 2028:

We willen het tekort aan cybersecurity-, privacy en digitale OOV-professionals bij de VNG en gemeenten terugbrengen en daarmee de eerste lastenverlichting opleveren met betrekking tot hun taakstellingen op dat gebied. Om deze ambitie te realiseren, zetten we in op drie zaken: meer inzicht, meer mensen en meer efficiëntie.

- Effectief beleid vraagt om meer inzicht door een gedegen probleemanalyse. De VNG zet zich in om het tekort aan digitale veiligheid-professionals bij gemeenten beter in beeld te brengen. Daarbij wordt gekeken naar aantallen maar ook naar benodigde expertise. Door de ontwikkeling van het tekort regulier te monitoren, moet het mogelijk worden voor de VNG en gemeenten om strategisch te sturen op hun personeelsbeleid. Op die manier zorgen we voor een oplossing die past bij het probleem, nu maar ook in de toekomst.
- De VNG wil gemeenten gaan ondersteunen bij het binnenhalen en -behouden van gekwalificeerd personeel. Belangrijk hierbij is om ook breed te kijken naar de cybersecurity- en privacyspecialisten, OOV'ers, juristen, beleidsmedewerkers en inkoopmanagers, allen functies die een belangrijke rol spelen bij de digitale veiligheid van gemeenten. De VNG ondersteunt bij het realiseren van nieuwe stageplekken, traineeships en meeloopdagen en bij de deelname aan stage- en banenmarkten. Verder ondersteunt de VNG gemeenten met advies over de juiste arbeidsvoorwaarden en actieve communicatie naar de doelgroep.
- Hoe zorg je dat je zo goed mogelijk gebruik maakt van je huidige personeelsbestand en zo de efficiëntie vergroot? De VNG adviseert gemeenten over de expertise en vaardigheden die nodig zijn om de digitale veiligheid te kunnen borgen en koppelt dat aan interne en externe opleidingsmogelijkheden. Daarnaast adviseert de VNG over technologische oplossingen, waarmee zittende professionals hun werk beter, sneller en efficiënter kunnen doen. Ten slotte faciliteert de VNG technische en personele samenwerking tussen gemeenten, zodat 'de groten de kleinen kunnen helpen'.

Conclusie

Samen verder, digitaal veilig de (gedrags)norm

In het licht van de toenemende digitale dreigingen en de noodzaak voor een robuuste digitale infrastructuur, is het essentieel dat gemeenten zich richten op een geïntegreerde aanpak van digitale veiligheid.

De Agenda Digitale Veiligheid wordt uitgewerkt in een proactieve en samenhangende strategie met meerjarenplannen om de digitale weerbaarheid van gemeenten te versterken, verbeteren en te waarborgen voor de inwoners, ondernemers en de eigen organisatie.

Door gezamenlijk op te trekken en te investeren in digitale veiligheid kunnen gemeenten een veilige digitale omgeving creëren voor hun inwoners en ondernemers. Samenwerking, kennisdeling en voortdurende verbetering zijn de sleutels tot succes. Laten we van digitale veiligheid de gedragsnorm maken en samen werken aan een weerbare en toekomstbestendige digitale samenleving.



**Vereniging van
Nederlandse Gemeenten**

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

juni 2025