Agenda Digitale Veiligheid 2020 – 2024

Een veilige (digitale) gemeente

Samenvatting

AWARENESS

1. Digitale veiligheid raakt ons allemaal. Gemeentebestuurders zorgen ervoor dat bestuurders en ambtenaren zich hiervan bewust zijn en zorgen ervoor dat zowel bestuurders en ambtenaren over kennis beschikken die past bij hun taak en verantwoordelijkheid
   (zie Actielijn 1, pagina 8).
2. Gemeenten zijn zich ervan bewust dat digitale incidenten en -crises altijd kunnen voorkomen en verder reiken dan de gemeentelijke bedrijfsvoering. Daarom bereiden zij zich voor zodat zij bij digitale incidenten en -crises veerkrachtig en daadkrachtig met ketenpartners kunnen optreden
   (zie Actielijn 2, pagina 9).
3. Gemeenten oefenen met digitale incidenten en -crises. Met de eigen organisatie en met alle ketenpartners die samenwerken bij lokaal cruciale processen
   (zie Actielijn 3, pagina 10).

GOVERNANCE

4. Gemeenten versterken de samenwerking tussen het college van B en W en raad op het onderwerp digitale veiligheid. De digitale veiligheid is vooral een lokale aangelegenheid en alleen op specifieke onderdelen leggen gemeenten verantwoording af aan ministeries
   (zie Actielijn 4, pagina 11).
5. De VNG werkt aan het verbeteren van de OOV-bevoegdheden van lokale bestuurders die in de praktijk niet altijd passen bij digitale incidenten en -crises. Ook zonder formele bevoegdheden kan al veel voortgang geboekt worden
   (zie Actielijn 5, pagina 12).

RISICOGERICHT HANDELEN

6. Gemeentebestuurders bepalen welke met (lokale) ketenpartners uitgevoerde maatschappelijke processen cruciaal zijn voor het functioneren van de gemeente. De digitale veiligheid voor deze ketens is (naast die van de eigen organisatie) een expliciet aandachtspunt voor het college.
   (zie Actielijn 6, pagina 13).
7. In lokaal cruciale processen zijn alle ketenpartners samen verantwoordelijk voor de digitale veiligheid. De gemeente treedt krachtig op als initiatiefnemer en spreekt zo nodig ketenpartners aan op hun (mede-)verantwoordelijkheid
   (zie Actielijn 7, pagina 14).
8. Gemeenten werken, in nauwe afstemming met de veiligheidsregio, aan een lokale digitale risicokaart waarin ook de domino-effecten (en zelfs cascade-effecten) van digitale incidenten en -crises duidelijk worden. Dit is een regulier onderdeel van de jaarlijks verplichte regionale risicoplannen.
   (zie Actielijn 8, pagina 15).

EÉN OVERHEID/ SAMEN ORGANISEREN

9. Gemeenten werken aan het versterken van de eigen digitale weerbaarheid. Zij worden daarbij ondersteund door de Informatiebeveiligingsdienst voor gemeenten (IBD). De IBD ontwikkelt zich verder als expertise- en ondersteuningsdienst en ondersteunt de organisatie met handreikingen, adviezen, en operationele diensten. De IBD coördineert bij incidenten en is hét expertisecentrum op het gebied van digitale veiligheid voor gemeenten.
   (zie Actielijn 9, pagina 16).
10. De VNG werkt voor gemeenten aan harmonisatie en professionalisering van relevante digitale veiligheidsprocessen met departementen en collega-brancheorganisaties (veiligheidsregio's)
    (zie Actielijn 10, pagina 17).

Inhoud

Voorwoord

Digitalisering heeft een grote impact op de levens van onze inwoners. We leven in een informatie- en netwerksamenleving die steeds complexer wordt. Dorpen en steden ontpoppen zich tot 'smart cities' waar digitale kansen volop worden benut. De overheid is in transitie naar een digitaal georiënteerde dienstverlening en bedrijfsvoering. Traditioneel beschikt de overheid over privacy- en concurrentiegevoelige datasets over en voor inwoners en ondernemers. De afgelopen jaren heeft de overheid zich ingespannen om vooral de beveiliging daarvan naar een hoger plan te tillen.
Gemeenten hebben hier al mooie stappen in gemaakt. Het bestuurlijk bewustzijn rondom informatiebeveiliging is enorm toegenomen. De VNG-visitatiecommissie Informatieveiligheid onderschrijft in haar rapport "Durven Leren" dat het belang van het onderwerp niet meer ter discussie staat. De overheid investeert veel om de informatieveiligheid in de gemeentelijke organisatie goed in te bedden. Desondanks verschilt het niveau van gerealiseerde informatieveiligheid per gemeente. De Informatieveiligheidsdienst voor gemeenten (IBD) ondersteunt gemeenten met het programma Verhogen Digitale Weerbaarheid. De IBD adviseert op techniek, proces en governance om digitale weerbaarheid blijvend te verbeteren. Digitalisering is allang geen ICT-vraagstuk meer, maar vraagt ook bestuurlijke keuzes om publieke waarden te borgen.

Kwetsbaarheden en dreigingen in het digitale domein nemen toe, met verstrekkende gevolgen in de samenleving. Dit vraagt om extra inspanningen en initiatieven om de digitale weerbaarheid en het herstelvermogen van de samenleving te versterken. Immers, digitalisering en de beveiliging ervan, gaan ook over onze organisatiegrenzen heen. Dit realiseren alle overheidslagen zich. Dit betekent dat alle overheden – ook gemeenten- overgaan tot het implementeren van de gezamenlijke baseline Informatieveiligheid Overheden (De BIO).

Door de toenemende belangstelling voor digitale veiligheid nemen diverse overheidsorganisaties initiatieven ter versterking van de digitale weerbaarheid. Dit varieert van een nationale aanpak door organisaties als de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Center (NCSC), tot de sectorale aanpak door organisaties als het Instituut Fysieke Veiligheid (IFV), de Nederlandse Vereniging van Ziekenhuizen en natuurlijk de VNG.

Het wordt tijd dat er ook een gemeentelijke agenda komt die bestuurlijke handvatten biedt. Daarom presenteert de VNG de Agenda Digitale Veiligheid 2020 - 2024 waarin gemeenten gezamenlijk vastleggen wat hun standpunten zijn en wat hun actieplan is om het vertrouwen van inwoners en ondernemers in hun digitale veiligheid te vergroten en vast te houden. Deze Agenda Digitale Veiligheid is verbonden met de Meerjarenvisie van de VNG, met de daarin benoemde transities op het gebied van energie, economie én informatiesamenleving. Deze transities zijn alleen te realiseren met een goed functionerende én veilige informatievoorziening. Dat betekent dat de Agenda Digitale Veiligheid ook op termijn verbinding moet leggen met meerdere beleidsterreinen.
Met deze Agenda Digitale Veiligheid 2020 - 2024 hopen we een toekomstperspectief te bieden voor gemeentebestuurders, zodat zij kunnen werken aan een lokaal krachtige digitale overheid.

Inleiding

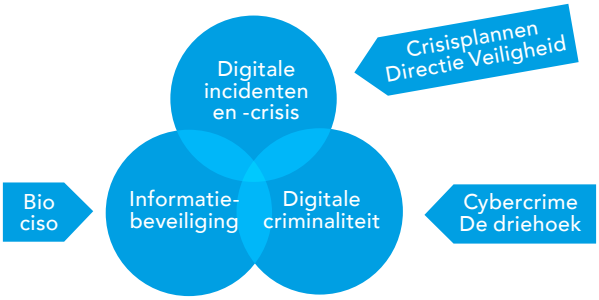
De positieve ontwikkelingen in de informatiesamenleving gaan gepaard met toenemende risico's en onderlinge afhankelijkheden. Die risico's beperken zich niet meer tot de grenzen van de gemeentelijke organisatie, maar doen zich des te meer voor in lokale ketens en netwerken. De verantwoordelijkheid voor de digitale veiligheid van zo'n keten als geheel is nog onontgonnen terrein. Dat is risicovol omdat bij een digitale ontwrichting de maatschappelijke effecten groot kunnen zijn. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) onderschrijft dit in haar rapport 'Voorbereiden op digitale ontwrichting'. Met 'digitale ontwrichting' doelt de WRR op de ernstige verstoringen van het maatschappelijke leven met zowel digitale als fysieke dimensies. Denk bijvoorbeeld aan de gevolgen van de ransomware aanval op een Oekraïens boekhoudsysteem die in 2017 ook de Rotterdamse haven trof of de landelijke uitval van het noodnummer 112 als gevolg van een KPN-storing in 2019.

Digitale ontwrichtingen weerspiegelen het belang van slagkracht van bedrijven en instellingen in de gemeente om deze kwesties het hoofd te kunnen bieden. Overheid en bedrijfsleven zijn verantwoordelijk voor een basis 'fitheid' wat betreft digitale veiligheid en een hoge weerbaarheid wanneer zich onverhoopt toch een incident voordoet. Zij moeten onverminderd doorwerken aan het op orde brengen van de eigen digitale weerbaarheid. De IBD ondersteunt gemeenten met een daarop gericht programma.

De recente 'hack' in de gemeente Lochem drukt ons weer met de neus op de feiten. Een op het oog niet opvallende hack blijkt grote consequenties te hebben voor de continuïteit van de bedrijfsvoering. Daarnaast waren de financiële implicaties omvangrijk. Beide consequenties raken de bestuurlijke verantwoordelijkheid. In de analyse naar aanleiding van deze 'hack' wezen diverse betrokkenen op de noodzakelijke 'fitheid' van de informatievoorziening. Zijn de gebruikte processen en systemen up- to-date? Wordt voldaan aan de basiseisen voor digitale weerbaarheid? Is de organisatie voldoende alert op verstoringen en weten ze wat te doen?

Waarom een Agenda Digitale Veiligheid?

Wat is je legitimering als bestuurder om te handelen bij een digitale ontwrichting? Hoe neemt een bestuurder daarin positie? Hoe werken de overheid en het lokale bedrijfsleven samen? Bestuurders worden op drie manieren geconfronteerd met digitale veiligheid. Ten eerste dragen zij zorg voor de continuïteit van de gemeentelijke dienstverlening en bedrijfsvoering (informatiebeveiliging). Ten tweede worden zij geconfronteerd met incidenten in de openbare ruimte die voortvloeien uit digitale ontwrichting. Ten derde vervullen zij een rol bij de bestrijding van digitale criminaliteit vanuit de verantwoordelijkheid voor openbare orde en veiligheid.

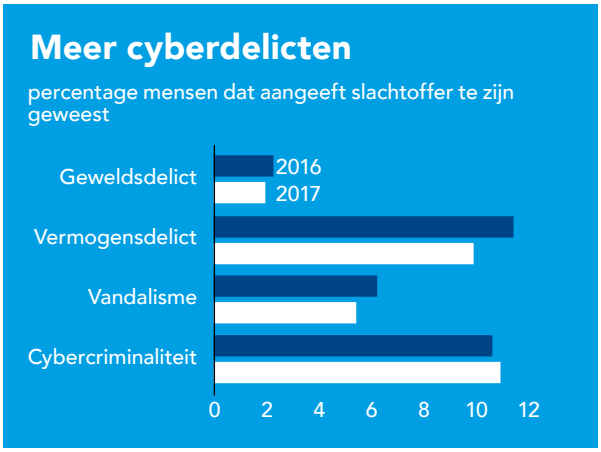


De afgelopen jaren hebben gemeenten vooral geïnvesteerd in de interne organisatie op basis van de resolutie 'informatieveiligheid randvoorwaarde voor een professionele gemeente'. De daarin verwoorde uitgangspunten hebben gemeenten voortvarend opgepakt. Zij hebben onder andere de BIG (Baseline Informatiebeveiliging Gemeenten) geïmplementeerd; er is sprake van stroomlijning van de verantwoordingsplicht aan departementen en er is gewerkt aan een transparante rapportage over informatieveiligheid aan de gemeenteraden. Het

werk is echter niet af. Gemeenten moeten zich blijven inzetten voor het op orde brengen van de gemeentelijke digitale weerbaarheid. De IBD ondersteunt gemeenten hierbij.

Maar er is een verbreding gaande. En daar moeten we naartoe, in het denken over digitale veiligheid binnen en buiten de grenzen van het gemeentehuis. De samenleving wordt steeds meer afhankelijk van digitale technologie. Bestuurders staan nu voor de uitdaging om samen met lokale bedrijven sturing te geven aan de beheersing van risico's die met digitalisering samenhangen. Er moeten nog stappen worden gezet om ze daarin regie te laten nemen. In de fysieke veiligheidsketen is dat al 'chefsache' voor de bestuurder:

> "De vergelijking met brandveiligheid dringt zich op. We weten met elkaar dat brand (ondanks alle preventiemaatregelen) niet te voorkomen is. Wat we daar geleerd hebben, is dat we een afweging gemaakt hebben van risico's op het ontstaan van brand en een bestuurlijke afweging hebben gemaakt om te investeren in het voorkomen daarvan. We weten wat te doen als er brand is; we hebben de adequate gereedschappen en we zijn snel ter plaatse. We weten ook waar de verantwoordelijkheden liggen van andere betrokken bestuurders en professionals en we trainen op snelle en doelgerichte communicatie."



Doelstelling Agenda Digitale Veiligheid 2020 - 2024

De Agenda Digitale Veiligheid beoogt een handelingsperspectief voor de lokale bestuurder bij vraagstukken rondom digitale veiligheid te bieden. Daarnaast bevat deze agenda de ambities om te komen tot digitaal veilige gemeenten en de daarbij behorende onderwerpen. Deze worden in de komende maanden verder uitgewerkt in activiteitenplannen.

Leeswijzer

De volgende paragraaf bevat vier uitgangspunten die zijn gebruikt bij het verder uitwerken van de deze agenda digitale veiligheid.
Ketenverantwoordelijkheid, risicomanagement en het aansluiten bij bestaand structuren zijn daar de kernbegrippen. De daarop volgende paragraaf werkt de tien actielijnen in de samenvatting inhoudelijk verder uit. Die actielijnen zijn gerubriceerd naar vier herkenbare samenhangende thema's.

Uitgangspunten

1. Vanuit het maatschappelijke vraagstuk

Gezien de huidige ontwikkelingen voldoet een bestuurlijke focus op alleen de informatiebeveiliging van het gemeentehuis niet langer.
Datalekken, digitale verstoringen, incidenten en digitale criminaliteit zijn dagelijkse realiteit.
Dergelijke incidenten tonen aan dat (digitale) verstoringen ook elders tot ontwrichtende effecten kunnen leiden. Digitale ontwrichting; iedereen krijgt het op zijn of haar bord. Bestuurders worden daarom niet alleen geconfronteerd met de eigen bedrijfsvoering, maar óók met digitale criminaliteit en digitale incidenten in de samenleving.
Het maakt dat het thema 'digitale veiligheid' een thema is dat periodiek thuishoort op de bestuurstafel en niet meer uitsluitend een bedrijfvoeringsvraagstuk is.

2. Aansluiten bij de leefwereld van de bestuurder

Vanuit bestuurlijk perspectief zijn al instrumenten om grip te krijgen op het complexe werkveld digitale veiligheid. In deze paragraaf benoemen we er twee.

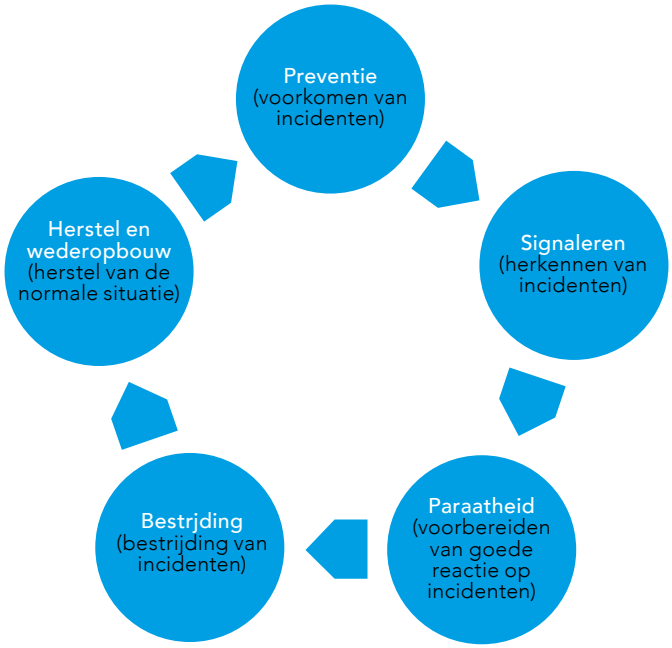
2.1. De BIO en Tien bestuurlijke principes
Een van de belangrijke uitgangspunten van de Baseline Informatieveiligheid Overheden is een bestuurlijk risicomanagement voor informatievei-

ligheid. De (gemeentelijk) bestuurders spelen daarin een belangrijke rol. Om die rol in te vullen, zijn tien bestuurlijke principes geformuleerd. Deze principes maken onderdeel uit van het besluit van VNG om de BIO gemeentebreed te implementeren. Deze principes gelden als uitgangspunt voor de digitale agenda 2020-2024:

1. Bestuurders bevorderen een veilige cultuur;
2. Informatiebeveiliging is van iedereen;
3. Informatiebeveiliging is risicomanagement;
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. Informatiebeveiliging is een proces;
7. Informatiebeveiliging kost geld;
8. Onzekerheid dient te worden ingecalculeerd;
9. Verbetering komt voort uit leren en ervaring;
10. Het bestuur controleert en evalueert.

2.2. Een digitale veiligheidsketen

Digitale veiligheid is een redelijk nieuwe dimensie in de belevingswereld van bestuurders, maar het thema kent nauwe raakvlakken met de voor de bestuurder bekende veiligheidsketen. In de fysieke veiligheidsketen heeft de bestuurder een duidelijk handelingsperspectief. Denk aan brandoefeningen en andere fysieke incidenten. Door aan te sluiten bij de bekende veiligheidsketen kan er worden doorgepakt. Instrumenten voortvloeiend uit deze agenda sluiten daar dan zoveel mogelijk op aan.



3. In de keten

Vaak zal de gemeente samenwerken met ketenpartners waardoor de formele invloed op ketenpartners (en dus ook op de veiligheid van de gehele keten) beperkt is. Toch kan het gemeentebestuur ter verantwoording geroepen worden bij digitale verstoringen. Gemeentebestuurders worden opgeroepen initiatieven te nemen en de ketenpartners aan te spreken vanuit de maatschappelijke verantwoordelijkheid voor de (digitale) veiligheid en continuïteit van lokaal vitale processen.

4. Met de partners

In 2018 is de Nederlandse Cybersecurity Agenda (NCSA) gepubliceerd onder verantwoordelijkheid van het ministerie van Justitie & Veiligheid. Deze landelijke agenda zet de noodzakelijke stap om de digitale veiligheid te versterken en de vitale belangen van Nederland beter te beschermen. Ook binnen de veiligheidsregio's is het thema 'digitale ontwrichting' actueel. Voor dit thema werkt het Veiligheidsberaad aan een bestuurlijk routeboek. Het doel van 'Bestuurlijk routeboek digitale ontwrichting' is om te komen tot een betere informatiepositie en een handelingsperspectief voor de besturen van veiligheidsregio's. Onderdeel hiervan is het verhelderen van de rol van veiligheidsregio's bij digitale ontwrichting en het bieden van kaders hiervoor. Digitale weerbaarheid vraagt met nadruk om een ketenbenadering, waar de veiligheidsregio's onderdeel van uit maken.

Agenda Digitale Veiligheid 2020 – 2024

De tien actielijnen zoals gepresenteerd in de samenvatting worden in deze paragrafen uitgewerkt. Om de leesbaarheid en samenhang van die actielijnen te benadrukken, hebben we ze in deze agenda gerubriceerd in vier overkoepelende thema's. Het betreft 'Awareness', Governance, Risicogericht Handelen en tot slot 'Eén overheid/Samen Organiseren.

AWARENESS

Actielijn 1: Bewustzijn vergroten

Het delen en verbinden van informatie tussen overheid en inwoner is niet meer weg te denken in de gemeentelijke dienstverlening. Persoonlijke en gevoelige gegevens van inwoners worden toevertrouwd aan de lokale overheid. Inwoners en ondernemers moeten erop kunnen vertrouwen dat die informatie bij de lokale overheid in veilige handen is. Het is van essentieel belang dat lokale overheden interne bewustwording creëren over het belang van privacybescherming van privacygevoelige data van inwoners en de impact als deze data op straat komen te liggen. Het delen van kennis, ervaringen en vaardigheden met relevante partners draagt bij aan bestuurlijke bewustwording en handelingsperspectief. Samen met het Nederlands Genootschap van Burgemeesters (NGB), de Wethoudersvereniging en de Vereniging van gemeentesecretarissen (VGS) ontwikkelt de VNG handvatten voor het College van B en W en haar gemeentesecretaris om digitale veiligheid adequaat te besturen. De VNG zoekt hier de samenwerking met het Veiligheidsberaad en het instituut voor Fysieke Veiligheid.

Bewustwording geldt voor iedereen

Het vergroten van het kennisniveau rondom digitale veiligheid geldt niet alleen voor bestuurders, maar ook voor het gehele ambtelijke apparaat én inwoners. De snelheid waarmee digitale criminaliteit zich ontwikkelt, is nauwelijks bij te benen. Het begint echter wel met menselijk falen en kwetsbaarheden; slechte wachtwoorden, een ondoordachte klik of onvoldoende controle op de eigen veiligheid. Het vergroten van bewustzijn onder digitale kwetsbare doelgroepen is een onderdeel van het preventiebeleid. Ook hier geldt dat we als gemeenten aansluiten op eerdere interbestuurlijke initiatieven.

VNG Cybergame

De VNG-cybergame is een gesimuleerd spel waarbij een digitaal incident met een fysieke uitwerking in het domein van de openbare orde en veiligheid centraal staat. Doel is om onder bestuurders én ambtenaren (CISO's, adviseurs openbare orde en veiligheid) bewustzijn op het gebied van digitale veiligheid te vergroten.

IBD Crisisgame

De IBD-crisisgame is een gesimuleerd spel dat wordt gebruikt om te oefenen met een informatiebeveiligingscrisis. De crisisgame is vooral gericht op de interne organisatie en bedoeld voor medewerkers die belast zijn met het onderwerp informatiebeveiliging (CISO's, adviseur informatiebeveiliging). Het doel van deze game is het vergroten van bewustzijn rondom informatiebeveiliging binnen de eigen gemeente.

Actielijn 2: Weerbare organisatie

De traditionele benadering van informatiebeveiliging, waarbij aan de buitenkant van de organisatie muren werden opgetrokken om het kwaad buiten te houden, is niet meer houdbaar. We moeten ervan uit gaan dat onze digitale muren doordringbaar zijn. Wij zullen dan ook het accent van de veiligheidsmaatregelen verschuiven van het steeds hoger maken van de muren (weerbaarheid) naar de capaciteit veerkrachtig op te kunnen treden. Om te bepalen hoe en waar deze muren aanpassing behoeven, is het noodzakelijk een inschatting te maken van de risico's die daarbij komen kijken. De actielijnen zes, zeven en acht in deze agenda werken dat thema verder uit. Het signaleren en bestrijden van incidenten is van het grootste belang om passend en voortvarend te handelen wanneer de gemeente geconfronteerd wordt met in- of externe bedreigingen. Het kan betekenen dat we terug moeten vallen op analoge processen.
We moeten ons ervan bewust zijn dat we in toenemende mate afhankelijk zijn van (buitenlandse) bedrijven. Samenwerking met ketenpartners en/of andere gemeenten voor de oprichting van een 'digitale brandweer' (inclusief de hiervoor benodigde bevoegdheden) in combinatie met inzet van leveranciers kan soelaas bieden. Het verlaagt die afhankelijkheid en verandert de machtsbalans. GGI veilig en IBD spelen op dit punt een belangrijke rol.
Het toegroeien naar een weerbare organisatie vraagt om een daarbij passend budget, zowel bij gemeenten als bij VNG/IBD. Om de verantwoordelijkheid voor informatieveiligheid adequaat te kunnen invullen is het noodzakelijk dat daarvoor gemeentelijk budget wordt gealloceerd. De hoogte van dat budget is afhankelijk van de uitkomst van een gemeentelijke risicoanalyse die bestuurlijk is geaccordeerd. Dit budget moet zichtbaar zijn in de gemeentelijke begroting.

Stroppenpot als hulpmiddel

De financiële afwikkeling van schade kan moeizaam verlopen. Er is nog weinig inzicht in de risico's en de bijbehorende schade. Ook verzekeraars zijn terughoudend bij het compenseren van schade ten gevolge van wereldwijde cyberaanvallen omdat deze beschouwd worden als terrorisme en/of een gewapend conflict.
Gemeentebesturen zullen met ketenpartners dan ook gezamenlijk afspraken moeten maken over de dekking van onverzekerde schade. Een gezamenlijke 'stroppenpot' is een belangrijk hulpmiddel bij het herstel van lokaal vitale processen.

Actielijn 3: De digitale brandoefening

Uit het Cybersecuritybeeld Nederland 2019 blijkt onder meer dat analoge alternatieven en back-up systemen langzaam verdwijnen. De afhankelijkheid van digitale netwerken in de samenleving is daardoor zodanig groot geworden dat aantasting kan leiden tot digitale ontwrichting. Hoewel in veel gevallen de impact van digitale incidenten en –crisis beperkt blijft tot de eigen bedrijfsvoering, kunnen deze ook gevolgen hebben voor de fysieke omgeving. In de fysieke veiligheid zijn er talloze oefendraaiboeken, uitgebreide crisisorganisaties, wettelijke regels en voorzieningen om de risico's te managen en fysieke incidenten beheersbaar te krijgen. De vergelijking met brandveiligheid dringt zich vaak op. Bestuurders weten waar de verantwoordelijkheden liggen van diverse partijen en er wordt volop geoefend, waardoor crisiscommunicatie een tweede natuur wordt. Een dergelijke bestuurlijke organisatie zou ook voor de digitale veiligheid moeten gelden. Het betekent overigens ook dat de medewerkers die bij de oefeningen zijn betrokken in zowel de 'reguliere informatieveiligheid' als de 'fysieke veiligheidsketen' adequaat opgeleid moeten zijn om dit type oefening effectief te laten zijn.

Integrale aanpak

De noodzaak om te oefenen met digitale noodscenario's ter voorbereiding op daadwerkelijke incidenten zou integraal onderdeel moeten zijn van het bedrijfscontinuïteitsplan van iedere gemeente. Ook wordt samenwerking met de veiligheidsregio in de fase 'preparatie' noodzakelijk. Dit betekent dat de kennis en capaciteit van de veiligheidsregio op het thema 'digitale ontwrichting' als nieuw domein georganiseerd moeten worden. Het gemeentebestuur zal in samenspraak met het bestuur van de veiligheidsregio hiervoor middelen vrij moeten maken.

VNG Cyberoefening

De VNG Cyberoefening is een pakket waarmee gemeenten op relatief eenvoudige wijze zelf kunnen oefenen met het doorleven van een cyberincident met impact op de eigen dienstverlening en op de omgeving in het domein van openbare orde en veiligheid. De oefening moet gemeenten en betrokkenen inzicht geven in de werking van de eigen organisatie (opschaling) bij een digitale ontwrichting en handelingsperspectief bieden om de bijzonderheden te herkennen en de crisis goed te managen.

GOVERNANCE

Actielijn 4: Decentrale verantwoording waar kan, centraal toezicht waar moet

Gemeenten zijn zelf verantwoordelijk voor informatieveiligheid. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties draagt de stelselverantwoordelijkheid voor informatieveiligheid. Stelselverantwoordelijkheid betekent dat alle overheidsorganisaties medeverantwoordelijkheid dragen voor het stelsel als geheel en dat elk van hen daarop kan worden aangesproken. Op het gebied van informatieveiligheid zijn wettelijke taken in medebewind bij de gemeente neergelegd waardoor de rijksoverheid zich terughoudend opstelt. Gemeenten nemen die rol serieus en organiseren zich individueel en collectief.

Decentraal verantwoording waar dat kan

De rijksoverheid hanteert het basisprincipe dat gemeenten zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Dit noemen we ook wel horizontaal toezicht omdat via de lokale planning en control-cyclus verantwoording wordt afgelegd aan de gemeenteraad. In de verantwoording geeft het College van B en W aan hoe het informatieveiligheidsbeleid is gerealiseerd, welke afwijkingen er zijn, de risicoafweging daarbij en de verbeteringen die worden doorgevoerd. Zo kan de gemeenteraad zijn rol innemen als toezichthouder en tegelijk aanleiding geven voor een dialoog over informatieveiligheid en de gewenste wijze van communiceren hierover Een groot aantal gemeenten heeft de afgelopen jaren stappen gezet om het onderwerp te behandelen op de collegetafel en in raadsvergaderingen. Dat blijkt niet eenvoudig. We blijven inzetten op het beter toerusten van college en raad om hier als verantwoordelijk bestuur en controlerend orgaan in te handelen. Dat versterkt de kracht van het lokale horizontale toezicht. Overigens geldt dat voor bestuurders en raadsleden specifieke op de rol toegesneden informatie moet worden ontwikkeld.

Centraal toezicht waar dat moet

De Rijksoverheid heeft aangegeven dat voor enkele processen wel interbestuurlijke verantwoording moet plaatsvinden. Dit heet verticaal toezicht, waarbij gemeenten op die processen aan de rijksoverheid verantwoording afleggen. Concrete voorbeelden van verticaal toezicht op het gebied van informatieveiligheid zijn op dit moment de gemeentelijke ENSIA rapportages aan het Ministerie van Binnenlandse Zaken (BZK) voor DigiD en aan de Inspectie Sociale Zaken en Werkgelegenheid in het kader van het opvragen van persoonsgegevens door gemeentelijk sociale diensten via SUWInet.
Het uitgangspunt is dat verticaal toezicht dienend is aan de ministeriële verantwoordelijkheid en kan daarom niet enkel worden vervangen door decentrale verantwoording. In het kader van de ministeriële verantwoordelijkheid kan de minister of toezichthouder ook gebruik maken van de resultaten van het horizontale toezicht. Hierbij is het van belang dat de gemeenteraad voldoende opgeleid wordt tot controlerend orgaan.

Bestuurlijke mindmap ‘informatiebeveiliging’

Er moet meer bestuurlijke aandacht komen voor informatieveiligheid, met een hechtere verbinding tussen bestuurder en de Chief information security officer (CISO). Dat concludeerde de Visitatiecommissie Informatieveiligheid in 2017. Naar aanleiding hiervan heeft de VNG een bestuurlijke mindmap ‘informatiebeveiliging’ ontwikkeld om de leefwereld van de bestuurder en CISO dichter bij elkaar te brengen. De mindmap biedt inzicht in de rol van het gemeentebestuur en kaart de belangrijkste onderdelen aan die van belang zijn in de gesprekken tussen de bestuurder en CISO.

Actielijn 5: OOV bevoegdheden en rollen voor de lokale bestuurders

Op het gebied van openbare orde en veiligheid zijn er talloze 'fysieke' veiligheidsincidenten die de gemeente raken en waar de burgemeester als lokale veiligheidsbestuurder een wettelijke verantwoordelijkheid in heeft. Rampen, branden en huiselijk geweld zijn een kleine greep uit het veiligheidsdomein die de diversiteit van de problematiek weerspiegelen. Niet alleen de burgemeester is belast met de handhaving van de openbare orde en veiligheid, maar ook het hele college van B en W hebben een rol in het integraal veiligheidsbeleid.
De VNG actualiseert om de vier jaar het Kernbeleid Veiligheid. De rol van het gemeentebestuur op digitale veiligheid krijgt hierin ook een plek. Steeds meer gemeenten geven hun regierol op digitale criminaliteit een plek in hun Integraal Veiligheidsbeleid.
Wat preventie betreft, gaat het om het vergroten van bewustzijn, het vergroten van inzicht in de materie en het meenemen en aanspreken van veiligheidspartners op hun rollen en verantwoordelijkheden (bijv. politie: vergroten aangiftebereidheid en aandacht voor opsporing).

Voorbeelden:

- Gemeente Breda is bezig met digitale buurtambassadeurs voor digitale veiligheid in de eigen buurt of wijk;
- Diverse gemeenten zijn bezig met bewustzijn voor bepaalde doelgroepen als MKB en jeugd, bijvoorbeeld via het spel Cyber 24;
- Diverse gemeenten hebben de regie in het ontwikkelen van een lokaal cyberweerbaarheidsbeeld.

Verantwoordelijkheden en ordebevoegdheden zijn op een rij gezet in het 'zakboek 'openbare orde en veiligheid' voor burgemeesters (uitgave van het Nederlands Genootschap voor Burgemeesters). Dit zakboek is tot nu toe gericht op de fysieke aspecten van veiligheid, waarin termen als 'informatieveiligheid', 'cyber' of 'digitaal' niet worden genoemd.
Bestuurlijke bevoegdheden op het gebied van openbare orde en veiligheid zijn niet altijd goed toepasbaar bij digitale veiligheid, deels omdat deze bevoegdheden gebaseerd zijn op de fysieke wereld. Op dit moment onderzoeken diverse onderwijsinstellingen digitale interventies en de toepassing van bestuurlijke bevoegdheden.[1]
Bij de toepassing van offline bevoegdheden op online vraagstukken spelen fundamentele vraagstukken, zoals de inbreuk op grondrechten bij (preventief) ingrijpen of grensoverschrijdende bevoegdheden. Op dit moment is er beperkte steun vanuit de wet en ontwikkelingen rondom wetgevingen zijn tijdrovend.[2] Tegelijkertijd vraagt het toepassen van offline bevoegdheden op online vraagstukken wel om bestuurlijke actiebereidheid om binnen de huidige bevoegdheid en maatschappelijke verantwoordelijkheid te handelen op het moment dat digitale incidenten zich voordoen.

1) Burgemeesters in cyberspace, Programma Politie & Wetenschap, 2018
2) a. Wet beveiliging netwerk- en informatiesystemen maakt onderscheid in vitale en niet-vitale processen;
b. Wet Digitale Overheid verankert taken, verantwoordelijkheden en bevoegdheden met betrekking tot de voorzieningen voor de generieke digitale infrastructuur (GDI);
c. Wet computercriminaliteit III geeft het Openbaar Ministerie duidelijke bevoegdheden bij de opsporing en vervolging van computercriminaliteit;
d. In de Algemene Verordening Gegevensbescherming worden maatregelen van verwerkers van persoonsgegevens gevraagd inclusief het toezicht door de verwerkingsverantwoordelijke hierop.

RISICOGERICHT HANDELEN

Actielijn 6: Lokale vitale processen bepalen vanuit maatschappelijke taken

Vanwege de digitale veiligheid is de afbakening van de nationale vitale infrastructuur momenteel onderwerp van gesprek. Denk daarbij aan drinkwater, elektriciteit, luchthavens maar ook aan de basisregistraties. De wet "Wet beveiliging netwerk- en informatiesystemen (Besluit beveiliging netwerk- en informatiesystemen)" onderscheidt vitale en niet-vitale processen. Het Nationaal Cyber Security Center (NCSC) werkt samen met de betrokken organisaties aan de bescherming van deze vitale infrastructuren tegen cyberdreigingen. Maar gemeenten maken hier vooralsnog geen onderdeel van uit, hierdoor moeten gemeenten de digitale veiligheid zelf organiseren.

Gemeentebestuurders zullen binnen de eigen gemeente met stakeholders een vergelijkbaar gesprek moeten voeren: welke lokale vitale processen kennen wij? Wat is de impact bij digitale ontwrichting? Hoe waarborgen we de continuïteit bij cyberincidenten en -crises? Welke bindende afspraken maken wij? Veiligheid is immers nooit vrijblijvend.
Hierbij kun je denken aan de bedreiging van de verkeersveiligheid bij een aanval op hun besturingssystemen, of aan het stilvallen van de uitbetaling van uitkeringen of het niet kunnen verstrekken van de WMO-zorg bij een cyberincident bij de gemeente.
Een dergelijke risicoanalyse is overigens al 'verplicht' vanuit het perspectief van de implementatie BIO waarbij bedrijfscontinuïteit aan de orde is. De daar gehanteerde principes kunnen gemeenten ook inzetten voor de hier bedoelde analyse.

Actielijn 7: Krachtige partner in de keten

In een netwerksamenleving staat iedere organisatie niet op zichzelf. In ketens en netwerken zijn afhankelijkheden ontstaat en zijn organisatieprocessen en informatiesystemen vervlochten geraakt. Gemeenten dragen steeds meer (uitvoerende)taken over aan andere organisaties met als gevolg dat informatie(systemen) en data meer over de deze ketens verspreid raken.
Tegelijkertijd is iedere organisatie in de ketensamenwerking of samenwerkingsverband zelfstandig verantwoordelijk voor de informatiebeveiliging en bedrijfscontinuïteit. Hierbij maakt iedere organisatie afwegingen op basis van belangen, risico's en beschikbare middelen. Ook gebruiken organisaties verschillende normenkaders en zijn er verschillen in juridische verantwoordelijkheden. Als vanzelfsprekend zullen onderlinge verschillen in volwassenheid tussen deze ketenpartners ontstaan en is de digitale weerbaarheid van lokale samenwerkingsstructuren niet gegarandeerd. De uitdaging ligt vooral in het verkennen van de raakvlakken, wederzijdse afhankelijkheden en bijbehorende risico's in de keten.

Niet eenmalig maar regelmatig
Bij de voorbereiding van iedere samenwerking zullen risicoanalyses en maatregelen, gericht op het voorkomen van cyberincidenten, een integraal onderdeel moeten vormen. Bij de uitvoering van die werkzaamheden zijn de CISO en beleidsadviseurs openbare orde en veiligheid geëigende adviseurs. Dit brengt het bestuur en management in positie hierover verantwoordelijkheid te nemen.

Als logisch vervolg hierop moeten gemeenten adequaat toezicht houden op ketenpartners en leveranciers. Bijvoorbeeld door het verder vergroten van de doelgroep van ENSIA (Eenduidige Normatiek Single Information Audit), waaronder omgevingsdiensten, veiligheidsregio's en belastingsamenwerkingen.

Samenwerken is ook informatie delen
Uitwisseling van informatie over cyberdreigingen en incidenten is tussen ketenpartners niet vanzelfsprekend. Het gevolg kan zijn dat signalen niet of te laat bij de juiste partijen terechtkomen en dat er geen totaalbeeld ontstaat. Dit maakt vervolgens het adequaat optreden bij de crisisorganisatie onmogelijk. Onderlinge communicatie tussen ketenpartners binnen de wettelijke mogelijkheden is dan ook cruciaal. We moeten uitwerken hoe we deze informatie-uitwisseling effectief inrichten.
Pas wanneer de beschikbare informatie samen komt, kan een patroon zichtbaar worden; bijvoorbeeld dat criminelen systematisch inbraken hebben gepleegd bij meerdere organisatie in de keten. Het verzamelen en delen kennis is dus noodzakelijk om de ernst van incidenten te kunnen vaststellen, om invloed uit te kunnen oefenen op de wijze waarop een digitale ontwrichting zich voltrekt en om tijdens een crisis de juiste beslissingen te kunnen nemen. Om die analyse te maken is de rol van IBD cruciaal.
De IBD verzorgt de informatie-uitwisseling met andere vergelijkbare organisaties in andere branches zoals zorg en veiligheidsregio's om dreigingsinformatie en maatregelen onderling uit te wisselen.

Actielijn 8: Risicomanagement geeft focus

Het bepalen van ketenafhankelijkheden, gevolgd door gezamenlijke risicoafwegingen, biedt houvast bij het prioriteren en plannen van maatregelen. Hierbij spelen niet alleen domino-effecten, maar zelfs ook cascade effecten, waardoor een 'digitale risicokaart' noodzakelijk is voor daadkrachtig handelen. De nadruk ligt vooral op het waarborgen van de bedrijfscontinuïteit van lokale vitale processen.

Voorbeeld van een cascade-effect is digitale ontwrichting in de Rotterdamse haven, waardoor de afhandeling van goederen stilvalt, waardoor opstoppingen ontstaan op de aanvoerroutes in de regio of zelfs daarbuiten, waardoor de bereikbaarheid voor hulpdiensten afneemt. Ook in de scheepvaart en het railvervoer ontstaan stremmingen, waardoor een trein met chemische lading stil komt te staan in stedelijk gebied, etc. Een ander voorbeeld is een fysieke of digitale aanval op een groot internetknooppunt of een gelijktijdige aanval op enkele telefonieproviders, waardoor communicatieverbindingen uitvallen, waardoor chaos ontstaat in de openbare ruimte, mensen 112 slecht kunnen bereiken, communicatie tussen hulpdiensten wordt bemoeilijkt, etc. Kortom, een waterval aan effecten.

EÉN OVERHEID/SAMEN ORGANISEREN

Actielijn 9: Versterken gemeentelijke weerbaarheid

Het verbeteren van de digitale weerbaarheid van gemeenten blijft in deze agenda een belangrijk uitgangspunt. De Informatiebeveiligingsdienst (IBD) van de VNG biedt gemeenten een programma versterken digitale weerbaarheid waarmee gemeenten worden ondersteund om die digitale basis 'op orde' brengen. De IBD moet de informatiebeveiliging van gemeenten borgen. Zij is het sectorale Computer Emergency Response Team voor alle Nederlandse gemeenten. Daarnaast ondersteunt de IBD gemeenten bij de implementatie van de Baseline Informatiebeveiliging Overheid (BIO) en vertegenwoordigt de gemeentelijke belangen bij het beheer van de BIO, is het schakelpunt met het Nationaal Cyber Security Centrum (NCSC) en geeft regelmatig kennisproducten uit. De IBD heeft onder andere een gemeentelijk dreigingsbeeld 2019/2020 uitgebracht dat tweejaarlijks verschijnt om de digitale weerbaarheid van gemeenten te verhogen. Gemeenten krijgen hierdoor inzicht in de belangrijkste risico's voor de eigen organisatie. Hierin lezen bestuurders een handelingsperspectief aangeboden, bestaande uit een bestuurlijke risicoanalyse en prioriteitstelling. Dat ziet er zo uit:

- Zet informatiebeveiliging op de agenda van het college en zorg dat lijnmanagers verantwoordelijkheid kunnen nemen. De top van de organisatie moet doordrongen zijn van het belang van informatiebeveiliging en heeft een voorbeeldfunctie.
- Breng de basis op orde, want de basale beveiligingsprocessen en maatregelen zijn belangrijk om de digitale weerbaarheid van de gemeente te verhogen.
- Versterk de menselijke schakel, want technologie alleen is niet de oplossing. Informatiebeveiliging begint bij de bewuste medewerker.
- Versterk de positie van de CISO. Een CISO moet de ruimte en middelen krijgen en investeren in kennis en kunde om de gemeente weerbaarder te maken tegen huidige en toekomstige digitale dreigingen.
- Verbeter het inzicht in de risico's van nieuwe technologieën. Maak de juiste mensen verantwoordelijk voor deze ontwikkelingen en betrek vanaf het beginstadium de CISO en de verantwoordelijke lijnmanagers.

Het blikveld van de IBD is de afgelopen jaren vooral gericht op preventie, signaleren, coördineren en ondersteunen. Vanwege de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) is er nu ook meer aandacht voor netwerk-monitoring, voor het bewaken van dataverkeer op het eigen organisatienetwerk en voor respons op eventuele aanvallen. Hierbij ligt de focus vooralsnog op de digitale weerbaarheid van de eigen gemeentelijke organisatie. De komende jaren zal de Gemeentelijke Gemeenschappelijke Infrastructuur nog verder uitgebouwd moeten worden om gemeenten te helpen bij het weerbaar maken van hun digitale infrastructuur.
Gezien alle ontwikkelingen en de toenemende risico's op digitale ontwrichtingen buiten de gemeentelijke organisatie is het nodig ons te oriënteren op verbreding en versterking van het takenpakket van de IBD en de rol die de VNG daarin heeft. Daarbij zal beter aansluiting gevonden moeten worden met sector overstijgende partners. Het Nationaal Respons Netwerk is daarbij een mogelijk vertrekpunt waar kennis en capaciteiten van verschillende publieke en private partners geïntensiveerd kunnen worden.
We zetten ook in op de vorming van een gemeentelijk respons netwerk. Dit netwerk bestaat uit elkaar ondersteunende gemeenten in tijden van crises. De IBD coördineert deze ontwikkeling en stuurt GRN aan in voorkomende gevallen.

Actielijn 10: Eén overheid

De overheid is inmiddels een complex netwerk van gespecialiseerde organisaties die intensief en liefst zo efficiënt mogelijk met elkaar samenwerken. Het college van Dienstverleningszaken zoekt samen met de Taskforce "Samen Organiseren" steeds naar manieren om bij de lokale overheid succesvolle initiatieven op te schalen. Inmiddels omvat dit een breed palet van specifiek voor de lokale overheid ontwikkelde (ICT-)voorzieningen en -diensten die gemeenten digitaal veiliger maken. We roepen gemeenten op hier zoveel mogelijk gebruik van te maken.

Ook overheidsbreed is er beweging. Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt verschillende normenkaders voor de verschillende geledingen van de overheid. Hiermee ontstaat één gezamenlijke taal voor alle overheidsorganisaties: helder, eenduidig en veilig. Het vereenvoudigt niet alleen onderling toezicht, maar ook de samenwerking en kennisdeling.
De VNG ziet het als haar taak om met andere brancheorganisaties (zoals het Instituut Fysieke Veiligheid, regioburgemeesters, BIJ12, Nederlandse vereniging van Ziekenhuizen) samen te werken aan afstemming, kennisuitwisseling en verdere professionalisering.

BEGRIPPENKADER [3]

- **Digitale Veiligheid:** situatie waarin je geen schade hebt of krijgt door verstoring of uitval van ICT.
- **Cyberweerbaarheid:** de veerkracht van een organisatie en haar digitale systemen en processen. Wordt uitgedrukt in de snelheid en effectiviteit waarmee een organisatie zich weet te herstellen na een incident.
- **Informatiebeveiliging:** alles wat je doet om ervoor te zorgen dat informatie steeds toegankelijk is, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Informatiebeveiliging zorgt ervoor dat de gevolgen van problemen met informatie zoveel mogelijk beperkt worden.
- **Digitale criminaliteit:** criminaliteit waarbij iemand een computersysteem aanvalt of misbruikt voor criminele activiteiten. Er zijn twee types: 1) gedigitaliseerde criminaliteit in brede zin. Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, racisme en belediging. 2) cybercriminaliteit in enge zin. Hierbij zijn informatiesystemen en computers niet alleen middel, maar ook doelwit. Bijvoorbeeld: computers beschadigen, spamaanvallen, DDoS-aanvallen, virussen verspreiden.
- **Digitale incidenten en –crises:** digitale of fysieke incidenten met een digitale oorsprong die kunnen leiden tot crises in de eigen organisatie en zelfs tot maatschappij ontwrichtende situaties in het domein van de openbare orde en veiligheid.

3) De eerste vier begrippen zijn afkomstig van het online Cybersecurity Woordenboek van Cyberveilig Nederland (2019).

Vereniging van
Nederlandse Gemeenten
Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93
info@vng.nl
januari 2020