Digitale Veiligheid gemeenten: *Chefsache!*

De verantwoordelijkheid voor digitale veiligheid raakt bij gemeenten meerdere domeinen, die elk hun eigen risico's genereren en om verschillende oplossingen vragen. Ten eerste dragen gemeenten 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 – vanuit de verantwoordelijkheid voor openbare orde en veiligheid – een rol bij de bestrijding van digitale criminaliteit. In dit artikel beschrijven we welke meervoudige bestuurlijke verantwoordelijkheid gemeentebesturen hier in hebben, welke handelingsruimte de bestuurder al heeft en welke fundamentele vragen nu onderzocht worden.

Meervoudige bestuurlijke verantwoordelijkheid

Zowel binnen als buiten gemeentehuizen is het denken over digitale veiligheid aan het verbreden. Zo roept de ontwikkeling van 'slimme steden' nieuwe vragen op. Bijvoorbeeld wie vanuit welke rechtmatigheid online inwoners mag volgen, gegevens mag verzamelen of over hoe de burger beschermd kan worden tegen privacy schending of tegen onveilige technologie. Technologie kan er ook toe leiden dat een stad juist onveiliger of minder democratisch wordt. Bestuurders worden aangesproken op hun verantwoordelijkheid bij uitval en verstoring van de digitale samenleving. De openheid die de bestuurders van Lochem[1] en Hof van Twente[2] hebben laten zien, maakt duidelijk dat een incident hun verantwoordelijkheid direct raakt. Het waarborgen van de digitale veiligheid van de gemeente vraagt van de gemeentebestuurders inzet op meerdere terreinen[3].

Eigen huis op orde, blijft belangrijk

Een betrouwbare en veilige overheid vraagt om gedegen informatieveiligheid en privacybescherming van de gemeentelijke informatiehuishouding. Het 'eigen huis op orde' krijgen en houden blijft noodzakelijk. Zo zal de gemeente zelf voldoende weerbaar moeten blijven tegen steeds nieuwe digitale dreigingen. Het dreigingsbeeld van de Informatie BeveiligingsDienst (IBD) 2021[4] van de VNG; het cybersecuritybeeld Nederland[5] en de steeds pregnantere ransomware-aanvallen zoals bij Hof van Twente maken dat duidelijk. Gemeenten werken aan het continue verbeteren van die digitale weerbaarheid en hebben zich hier unaniem over uitgesproken in de resolutie Digitale Veiligheid in februari 2021[6]. Ze zien ook, dat het nog wel het een en ander vraagt van bestuur, ambtelijke organisatie, IT voorzieningen, leveranciers en ook in de samenwerking tussen gemeentelijke partners en afstemming tussen de diverse bestaande digitale en reguliere veiligheidsstructuren. Het risicomanagement bij de gemeenten zal in lijn moeten liggen met deze digitale risico's en de risico's van ketenpartners moeten in beeld zijn. Voor de gemeenten en overheidsorganisaties in de keten geldt de Baseline Informatieveiligheid Overheid (BIO) als basis voor informatieveiligheid en privacybescherming, zowel in de eigen organisatie, als ook in de samenwerking en gegevensuitwisseling in gemeenschappelijke regelingen, met andere ketenpartners en bij uitbestede privaatrechtelijke taken of diensten. Dit vereist inzicht in de mate waarin de dienstverlening van de eigen organisatie, leverancier of ketenpartner kwetsbaar is voor inbraak of verstoring op het koppelvlak en vraagt om openheid over en weer. De InformatieBeveiligingsDienst (IBD) is voor de gemeenten het sectorale Computer Emergency Response Team (CERT) [7] met een gespecialiseerd

[1] https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553
[2] https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/03/artikel/hof-van-twente-cyber-hack-stevige-les-voor-ons-1872
[3] https://vng.nl/sites/default/files/2021-01/08_resolutie_digitale_veiligheid.pdf
[4] https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2021-2022/
[5] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021
[6] https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten
[7] https://www.informatiebeveiligingsdienst.nl/ibd-cert/

team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. De IBD ondersteunt gemeenten bij hun informatiebeveiliging, zowel met adviezen, waarschuwingen over kwetsbaarheden, als ook door een rol als een ondersteunende 'digitale brandweer' in de eerste response bij incidenten[8].

De gemeenten worden ondersteund in hun verantwoording over digitale veiligheid, de BIO en diverse overheidsbrede normatiek met een Eenduidige Normatiek Single Information Audit (ENSIA).[9] Ook provincies, waterschappen en enkele onderdelen binnen de rijksoverheid gebruiken ENSIA om zich te verantwoorden. De rapportages over de staat van informatiebeveiliging vormen een goede basis voor een periodiek gesprek van bestuur en management met de eigen Chief Information Security Officer (CISO). Dit helpt om steeds beter grip te krijgen op digitale veiligheid en de wijze waarop digitale weerbaarheid en het herstelvermogen is ingericht.

Voorkomen van digitale ontwrichting[10]

Naast de verantwoordelijkheid voor de veiligheid en continuïteit van de eigen gemeentelijke processen en ketenprocessen zijn gemeentebestuurders ook verantwoordelijk voor de eventuele maatschappelijk ontwrichtende consequenties van digitale onveiligheid. Zij zijn samen met (sociale) partners betrokken in diverse maatschappelijk relevante processen waarvan de uitval of verstoring kan leiden tot maatschappelijke ontwrichting. Gemeenten hebben een belang bij het ongestoord voortgang vinden van deze processen, maar zijn niet voor alle aspecten verantwoordelijk. Ze kunnen eisen stellen ten aanzien van de digitale veiligheid bij vergunningplichtige evenementen en bedrijfsmatige activiteiten. Daarbij is het relevant dat de gemeente weet, hoe hierop te handhaven en hoe ze samen met de organisatie of met ander gemeenten en/of de veiligheidsregio kunnen handelen om een cyberincident en/of -crisis beheersbaar te maken en af te wikkelen. Dit werd duidelijk tijdens de hack bij Senzer[11] en IJmond werkt![12], werkbedrijven die voor de arbeidsmarktregio's de participatiewet uitvoert voor meerdere gemeenten, waaronder het uitbetalen van de bijstandsuitkeringen en de tijdelijke overbruggingsregeling voor zelfstandig ondernemers (Tozo) in gevaar komt. Behalve dat een bedrijf of de instelling het incident in eerste instantie misschien zelf kan oplossen, kan het kan ook zijn weerslag hebben op de sociale leefomgeving, waardoor de gemeente(n) betrokken raakt(raken). Naast continuïteit van dienstverlening en communicatie naar betrokkenen vanuit de getroffen organisatie, kan het verder beperken van de impact één van de taken van de gemeente zijn. Al met al overstijgt digitale veiligheid de verantwoordelijkheid van de gemeentelijke CISO en is het naar zijn aard een bestuurlijk issue.

Gaat de analogie met fysieke veiligheid overal op?

Deze meervoudige verantwoordelijkheid brengt een complexe governance met zich mee. Het vraagt een andere blik op bestaande bestuurlijke verantwoordelijkheden, om vanuit het digitale veiligheidsperspectief deze maatschappelijk relevante processen met de daarbij relevante (keten)partners te identificeren.

In de fysieke veiligheidsketen zijn industriële sectoren als water, transport, energie nu aangewezen als vitale sectoren. Daar is de koppeling met beveiliging van digitaal aangestuurde operationele techniek en meet- en regelsystemen al gelegd. Hier komen 'safety' en 'security' bij elkaar en zijn al *Chefsache*.

[8] In 2019 heeft BZK/DGOO/DO onder de noemer Gemeenschappelijk Overheid Security Operations Center (GOV-SOC) de opbrengsten van hun verkenning overgedragen aan de bestuurslagen die de uitkomsten benutten om de incident response capaciteit van hun eigen bestuurslaag te versterken.
[9] https://www.vngrealisatie.nl/ensia
[10] het WRR-rapport 'Voorbereiden op digitale ontwrichting' van 20 maart 2020: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.
[11] https://www.senzer.nl/netwerkinbraak
[12] https://www.ijmondwerkt.com/2021/10/04/uitbreiding-veelgestelde-vragen-30-9/

Met het uitwerken van maatschappelijk relevante processen zal het denken over digitale veiligheid verder geïntegreerd moeten worden met de reguliere denkbeelden rond veiligheid. Vanuit de beleidsdepartementen van Jusitie en Veiligheid (JenV) en Binnenlandse Zaken en Koninkrijksrelaties (BZK) wordt met de VNG onderzoek gedaan naar de belangrijkste lokale processen die cruciaal zijn bij maatschappelijke ontwrichting[13]. In het verlengde van de beelden rondom de vitale sectoren wordt een gemeentelijk beeld uitgewerkt van maatschappelijk relevante processen, mogelijke effecten van digitale ontwrichting, de mogelijke (digitale) interventies en het handelingsperspectief dat daarbij past. Dit levert een top 10 van de belangrijkste maatschappelijk relevante processen waar gemeenten belang bij hebben, maar misschien niet verantwoordelijk zijn voor de uitvoering. Gericht op mogelijke incidenten in die processen kan een (bestuurlijk) adequate crisisrol[14] met aanpak uitgewerkt worden. Voor gemeentelijke verantwoordelijkheid in de gevolgbestrijding zal een optimale aansluiting moeten worden gezocht op het Nationaal Crisisplan Digitaal (NCP-Digitaal)[15]. Het NCP-Digitaal biedt snel inzicht en overzicht in mogelijke gevolgen en maatregelen, rollen, taken en bevoegdheden op nationaal niveau ten tijde van een digitale crisis. Een aantal gemeenten heeft een zogeheten ‘resilience officer’ aangesteld. De samenwerken met het Instituut Fysieke Veiligheid (IFV) en de Veiligheidsregio’s als professionals in crisisbeheersing en gevolgbestrijding[16] is belangrijk, zodat voor het gemeentelijk digitale domein een relevant en actueel oefenprogramma afgestemd kan worden, vanuit beide verantwoordelijkheden ingericht. Oefenen is een beproefd middel om vast te stellen of incident- en crisismanagement goed ingeregeld zijn. In het fysieke domein is dit een ‘no brainer' en reguliere praktijk; in het digitale domein zal eerst uitgewerkt moeten worden wánneer lokaal en regionaal wélke specifieke digitale crisisstructuur noodzakelijk wordt.

Digitale openbare orde en veiligheid

Een echt nieuwe ontwikkeling is de aandacht voor online aangejaagde ordeverstoringen[17], waarbij via sociale media oproepen worden gedaan en mensen zich snel kunnen organiseren om de openbare orde te verstoren. Desinformatie wordt actief verspreid met als doel mensen tegen elkaar op te zetten, de informatie van de overheid in twijfel te trekken en zo de democratische waarden onder druk te zetten. Online lijken mensen minder te beseffen dat ze strafbare feiten plegen. Ook komen inwoners online sneller in contact met radicale groepen en vinden er ‘hate crimes’ plaats in de digitale wereld met hun effecten in de fysieke werkelijkheid, zoals in Bodegraven[18].

Inwoners en bedrijven begeven zich tegelijkertijd meer en meer online. Verschillende vormen van criminaliteit vinden vooral online plaats, van bankfraude tot kindermisbruik. Dit vraagt ook aandacht voor de veiligheid en handhaving zodat inwoners zich ook online veilig kunnen voelen. Het Rathenau Instituut geeft in hun onderzoek naar schadelijk en immoreel gedrag online aan, dat online gedrag dat niet direct illegaal is, wel schadelijk en immoreel kan zijn.[19] Zij pleiten voor een meer proactieve overheid. *“Een overheid die niet alleen reageert wanneer gedrag al is ontspoord, maar die ook proactief ingrijpt in de*

[13] Onderzoek toegezegd door minister JenV in de kabinetsreactie op het WRR-rapport ‘Voorbereiden op digitale ontwrichting’ https://www.digitaleoverheid.nl/document/kabinetsreactie-op-het-rapport-voorbereiden-op-digitale-ontwrichting-wrr/ .

[14] In 2020 heeft de directie Digitale Overheid van BZK de *Quickscan voorbereiding op digitale ontwrichting* uitgevoerd. https://www.rijksoverheid.nl/documenten/rapporten/2021/01/31/quick-scan-voorbereiding-op-digitale-ontwrichting#:~:text=Gemeenten%2C%20waterschappen%2C%20provincies%20en%20veiligheidsregio's,dat%20eind%202020%20is%20uitgevoerd. Voorbereiding op digitale ontwrichting is hierin gedefinieerd als: *‘Voorbereid zijn op het bestrijden van de gevolgen van een ernstige ‘lokale’ verstoring van maatschappelijke kernprocessen, die samenhangt met cyberincidenten waarbij continuïteit van dienstverlening en/of crisisbeheersing onder verantwoordelijkheid valt van lokale overheden in aansluiting op bestaande crisisstructuren’*.

[15] https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

[16] https://www.ifv.nl/kennisplein/Paginas/bestuurlijke-netwerkkaarten-crisisbeheersing.aspx

[17] https://hetccv.nl/onderwerpen/cybercrime/cyberweerbaarheid-gemeenten/online-aangejaagde-ordeverstoringen/

[18] https://www.ad.nl/binnenland/burgemeester-bodegraven-als-het-nodig-is-laten-we-complotverspreiders-gijzelen~a0c62a93/?referrer=https%3A%2F%2Fwww.google.com%2F

[19] Op verzoek van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) deed het Rathenau Instituut onderzoek naar schadelijk en immoreel gedrag online. https://www.rathenau.nl/nl/digitaal-samenleven/online-ontspoord

online omgeving, zodat schade wordt voorkomen en grondrechten van burgers worden beschermd." Voor burgemeesters is het relevant om te weten of na een oproep de openbare orde dan daadwerkelijk in het geding komt en welk handelingsperspectief beschikbaar is om (proactief) in te grijpen bij deze veiligheidsvraagstukken. Het handelingskader digitale veiligheid[20] kan bestuurders helpen bij de voorbereiding op de digitale veiligheidsproblemen.
In de bestrijding van digitale criminaliteit ondersteunt de gemeente kwetsbare inwoners en bedrijven. De parallel met de verantwoordelijkheidsverdeling en handelingsruimte van de gemeentebestuurders in de fysieke wereld wordt ook hier onderzocht. Daarbij houden cybercriminelen zich niet aan gemeentegrenzen. Zij blijven het continue proberen en hebben er veel tijd en geld voor over om gericht digitaal kwetsbare plekken bij de gemeente, de ondernemers en de inwoners aan te vallen. Cybercrime en cyber-enabled crime[21] zijn groeiende zorgen binnen het veiligheidsbeleid in de stad. Het Kernbeleid Veiligheid is in 2021 aangevuld voor 'gedigitaliseerde criminaliteit', 'zorg en veiligheid' en 'informatiepositie'[22]. Van belang is het samenspel van handelingsbevoegdheden tussen politie, Openbaar Ministerie en gemeente telkens scherp te stellen om adequaat te kunnen blijven reageren. De VNG werkt daarom samen met de ministeries, Veiligheidsregio's en politie, het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en IFV aan verschillende cyberweerbaarheidsprojecten in de gemeenten.

Conclusie
Uitval van maatschappelijk relevante processen door digitale incidenten in de gemeentelijke dienstverlening, online aangejaagde ordeverstoringen of digitale criminaliteit kan leiden tot maatschappelijke ontwrichting, mogelijk met een effect in de fysieke ruimte. De burgemeester is verantwoordelijk voor het handhaven van de openbare orde en veiligheid en met de veiligheidsregio voor crisismanagement bij grote incidenten, ook in het digitale domein. Waar de analogie met de handelingsruimte die bestuurders in het fysieke domein kennen, voor digitale veiligheid niet gelijk op gaat, wordt die onderzocht. De verantwoordelijkheid voor die brede digitale veiligheid overstijgt de verantwoordelijkheid van de gemeentelijke CISO. Digitale Veiligheid is een bestuurlijk issue, Chefsache. De meervoudige verantwoordelijkheid brengt een complexe governance met zich mee die, naast het feit dat dit inhoudelijke kennis vraagt, voor bestuurders een lastig onderwerp is om adequaat sturing op te nemen. Digitalisering en cybercriminaliteit zijn grens overstijgend en de complexiteit van het vraagstuk is groter dan elke gemeente op zich kan verwerken.

Aandachtspunten:
- De actualiteit maakt dat thematiek rond digitale veiligheid op verschillende tafels komt, vanuit verschillende beleidsverantwoordelijkheden bij de ministeries van JenV, BZK en Economische Zaken. Vanuit de Agenda Digitale Veiligheid VNG wordt dit gekanaliseerd naar de verschillende relevante gemeentefunctionarissen en reguleert VNG de bestuurlijke drukte. Dit maakt het voor de gemeenten overzichtelijker, zodat het zijn effect in de uitvoering niet mist.
- De capaciteit in NL op OOV en informatiebeveiliging is schaars en het is lastig om geschikte mensen te werven; zowel voor onderzoek, bij beleid, als bij gemeenten. Voor veel beleidsvragen is nog fundamenteel onderzoek noodzakelijk. Door gerichte aansluiting op onderzoeksinitiatieven en het bestuurlijk versterken van coalities die zich richten op onderzoek en vakontwikkeling kan de schaarse capaciteit in dit domein digitale veiligheid optimaal ingezet worden.

Publicatie: Multidisciplinaire aspecten van digital security

[20] https://vng.nl/nieuws/handelingskader-lokaal-bestuur-in-een-digitale-samenleving
[21] Toelichting op het onderscheid in de kamerbrief van de minister van Justitie en Veiligheid: https://www.rijksoverheid.nl/documenten/kamerstukken/2021/06/28/tk-integrale-aanpak-cybercrime
[22] https://vng.nl/artikelen/kernbeleid-veiligheid-2021