Focusblad

Digitale Veiligheid

Inhoudsopgave

Colofon

Deze publicatie is gerealiseerd door BMC Advies en Management, in opdracht van de Vereniging van Nederlandse Gemeenten (VNG).

Tekst/inhoud: Jasper van Gaalen (BMC)
Begeleiding: Kato Vierbergen (VNG), Shanna Fontaine (VNG)
Grafisch ontwerp: Simpel is slim

Inleiding

Dit Focusblad Digitale Veiligheid is gekoppeld aan het Kernbeleid Veiligheid, de VNG-methode voor lokaal integraal veiligheidsbeleid. Regelmatig worden belangrijke veiligheidsvraagstukken, die nog niet of niet volledig zijn opgenomen in het Kernbeleid Veiligheid apart uitgewerkt in een zogenaamd focusblad. Het doel van dit focusblad is om gemeenten handvatten te bieden voor een goede verwerking van het thema digitale veiligheid in het lokaal Integraal Veiligheidsplan (IVP). Daarnaast kunnen gemeenten het focusblad gebruiken om het thema zowel operationeel als bestuurlijk te borgen.

Het focusblad beschrijft de te onderscheiden veiligheidsrisico's, de rol van de gemeente rond deze risico's en het aanbevolen pad voor de uitwerking in het IVP. In dit veiligheidsplan worden vraagstukken integraal vormgegeven en de rollen en instrumenten van verschillende domeinen in samenhang gebracht. Dit geeft een stevige basis voor de benodigde aanpak van digitale veiligheid

Digitale veiligheid is een onderwerp dat zich blijft ontwikkelen en de betrokken partijen (waaronder gemeenten) staan voor belangrijke uitdagingen. Gemeenten hebben zich via de Resolutie Digitale Veiligheid unaniem voor intensivering van de gemeentelijke inzet op dit thema uitgesproken. De Agenda Digitale Veiligheid van de VNG schetst hoofdlijnen van de aanpak en vormt mede het kader van dit focusblad.

In dit focusblad wordt ingegaan op:
1. De urgentie van het thema en van positiebepaling door de gemeente
2. De te onderscheiden risico's en onderdelen van de aanpak
3. De te zetten stappen voor de verwerking in het IVP

Dit focusblad is in samenwerking met gemeenten, de politie, de veiligheidsregio's, de Informatiebeveiligingsdienst (IBD) en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) tot stand gekomen.

1 Digitale veiligheid – prioriteit voor gemeenten

Digitalisering brengt veel goeds, onder meer efficiëntie, communicatie, sociale verbindingen, effectiviteit van ketens en innovatie. Daartegenover staan echter stevige veiligheidsrisico's. Groeiende afhankelijkheid van systemen heeft als keerzijde dat een hapering grote gevolgen kan hebben, zowel digitaal als in de fysieke leefomgeving.
Informatie in systemen kan in verkeerde handen terechtkomen, gemanipuleerd worden, onbereikbaar worden of 'kwijt' raken met alle gevolgen van dien. Berichtgeving en uitwisseling via internet kan maatschappelijke onrust veroorzaken, denk aan polariserende 'posts' op social media of nepnieuws. Verder kunnen inwoners, bedrijven en overheden slachtoffer worden van oplichting, diefstal, bedreiging en andere online criminaliteit.

Publieke partijen hebben een bijzondere positie bij het aanpakken en beheersbaar houden van deze risico's. Enerzijds kunnen zij zelf slachtoffer worden van systeemverstoring, datalekken en gedigitaliseerde criminaliteit.
Anderzijds hebben publieke partijen veiligheidstaken rond deze risico's en moeten zij de kans van maatschappelijke verstoring en slachtofferschap en de gevolgen daarvan, verkleinen. Waar deze twee sporen samenkomen wordt het ingewikkeld. Want hoe kan je een digitale crisis in de samenleving bestrijden als je er zelf ook door bent getroffen?

Gemeenten hebben een belangrijke rol, met globaal dezelfde tweedeling. Binnen de gemeentelijke organisatie zijn zij verantwoordelijk voor weerbare systemen en de veiligheid van informatie in die systemen (- 'beschikbaarheid, integriteit en vertrouwelijkheid').
Daarnaast heeft de gemeente een rol in het weerbaar maken van de inwoners en ondernemers om slachtoffer- en daderschap te voorkomen. Ook het voorkomen van digitale ontwrichting en online aangejaagde ordeverstoringen zijn hierbij relevante aspecten. Daarbij kan het voorkomen dat meerdere aspecten zich tegelijk aandienen.

Zowel de veiligheidsrisico's, beschikbare tools én de te hanteren uitgangspunten zijn nog verre van uitgekristalliseerd. Toch is *koersbepaling in digitale veiligheid* als gemeente nu cruciaal vanwege de groeiende veiligheidsrisico's. Het is van belang in positie te komen, de beschikbare tools te operationaliseren en samen met publieke- en private partners de risico's te beheersen.

2 Risico's en hoofdlijn aanpak

Het Kernbeleid Veiligheid maakt systematisch onderscheid tussen *veiligheidsrisico's* enerzijds en de aanpak daarvan anderzijds. Dit onderscheid is cruciaal om tot een trefzekere aanpak te komen. Ook in dit focusblad wordt dit onderscheid consequent doorgevoerd, ten behoeve van een effectief stramien voor beleidsontwikkeling rond digitale veiligheid. Zowel wat betreft de risico's als de in te zetten maatregelen op het vlak van digitale veiligheid is het beeld divers en complex. In verschillende kaders en programma's wordt met verschillende ordeningen gewerkt. Toch is hier een rode draad in te vinden. In de basis worden *vier soorten risico's (risicoclusters)* en *zes hoofdbestanddelen van de aanpak* onderscheiden. De opzet wordt hieronder schematisch weergegeven. In de rechterkolom is de relatie met de veel gehanteerde Cyberwegenkaart van het CCV gemarkeerd. Vier van de zes te onderscheiden bestanddelen van de aanpak zijn opgenomen in de Cyberwegenkaart. Vanwege het toenemende belang van de overige twee worden ze in dit focusblad toch stevig gepositioneerd.

Hierna worden deze risicoclusters en onderdelen van de aanpak toegelicht. Er wordt telkens ingegaan op manieren waarop de risico's zich kunnen manifesteren, de specifieke risico's voor de gemeente, aanpak/tools van de gemeente, regelgeving/wettelijk kader, partners en dilemma's in de aanpak. NB Dit betreffen nadrukkelijk géén uitputtende opsommingen. De beschrijving is – in de geest van het Kernbeleid Veiligheid – schetsmatig en bedoeld om voldoende houvast te geven voor de verdere ontwikkeling van een lokale maatwerk aanpak rond de kernpunten van digitale veiligheid.

Risicocluster 1: **Kwetsbaarheid van informatie** *Diefstal, verlies, aantasting van informatie*	**Voorbeelden, modaliteiten, modus operandi:** • datalekken • bedrijfsspionage, diefstal technologie • risico's als gevolg van leveranciers in de cloud • via onder meer ransomware, phishing, verkeerd geadresseerde e-mails • evt. door statelijke partijen • kwaadwillende (ex-)medewerker	**Risico's gemeente:** • uitval dienstverlening/bedrijfsvoering door hersteloperaties • hoge herstelkosten • uitlekken vertrouwelijke gegevens • manipulatie gegevens • aantasting privacy inwoners • maatschappelijke onrust • imagoschade, boetes en schadeclaims
Risicocluster 2: **Kwetsbaarheid van systemen** *Digitale ontregeling, ontwrichting, blokkades van systemen*	**Voorbeelden, modaliteiten, modus operandi:** • uitval websites/portalen • uitval voorzieningen, infrastructuur • verstoring bestuurlijke/maatschappelijke processen/dienstverlening • risico's van 'internet of things' • via onder meer hacken, ransomware, malware, DDoS via botnets • aanvallen bij leveranciers • evt. door statelijke partijen	**Risico's gemeente:** • uitval dienstverlening/bedrijfsvoering en aantasting continuïteit • openbare orde effecten door niet-functionerende voorzieningen of ketens (noodzaak interventies) • 'eigen' slachtofferschap i.c.m. bredere cybercrisis (hoe crisis effectief te managen?) • hoge herstelkosten • uitvallen belangrijke voorzieningen binnen gemeentegrenzen • imagoschade, boetes en schadeclaims

A1 Eigen huis op orde

Aanpak/tools gemeente
- doorvoering Baseline Informatiebeveiliging Overheid (BIO), interne trainingen en diverse awareness-tools, inwerken nieuwe medewerkers en borging bij leidinggevenden;
- bovenlokale afstemming met (CISO's/PO's) van andere gemeenten;
- preparatie op incidenten, inclusief proactieve afstemming met strategische actoren en oefenen;
- risicokaart cyber opstellen;
- 'blijven herhalen';
- logging en monitoring van informatie;
- incidentresponsplan en -organisatie;
- PPS, voorlichting aan ondernemers/ bedrijven.

Dilemma's, overwegingen
- awareness en handelen rond risico's zit niet in DNA gemeente;
- gemeenten werken te compliance-gericht;
- belang van strategische positionering bij gemeentesecretaris;
- benodigde versus beschikbare capaciteit/ middelen.

Regelgeving/wettelijk kader
- Algemene Verordening Gegevensbescherming;
- Baseline Informatiebeveiliging Overheid;
- Gemeentewet;
- Nationale crisisstructuur/ Nationaal Crisisplan Digitaal;
- Domeinwetten;
- Eisen stelselhouders.

Partners
- Informatiebeveiligingsdienst (IBD);
- veiligheidsregio;
- regiogemeenten;
- ketenpartners/leveranciers;
- politie.

A2 De keten op orde

Aanpak/tools gemeente

- samenwerking/afstemming met (CISO's/PO's van) ketenpartners (fysiek en sociaal domein);
- ontwikkeling gezamenlijk cyber-risicobeeld en monitoring-systematiek.

Dilemma's, overwegingen

- benodigde vs. beschikbare capaciteit/ middelen;
- prioritering/selectie ketens/partners.

Regelgeving/wettelijk kader

- Algemene Verordening Gegevensbescherming;
- Baseline Informatiebeveiliging Overheid;
- Nationale crisisstructuur/ Nationaal Crisisplan Digitaal.

Partners

- Informatiebeveiligingsdienst (IBD);
- veiligheidsregio;
- regiogemeenten;
- ketenpartners;
- politie;
- leveranciers.

A3 Preparatie op cyberincidenten en -crises

Aanpak/tools gemeente

- brede preparatie op incidenten en crises, inclusief proactieve afstemming met strategische partners, inventarisatie kwetsbare systemen binnen gemeente, crisisstructuur en -oefeningen en continuïteitsplannen;
- vaste check op cyberrisico's bij gemeentelijke planvorming/nieuwe ontwikkelingen;
- bij vergunningen, subsidies en aanbestedingen eisen stellen aan partijen (o.m. ISO 27002);
- PPS, voorlichting aan ondernemers/ bedrijven.

Dilemma's, overwegingen

- risico's bij strategische partners – publiek en privaat (o.m. waterschappen, bedrijven die met gevaarlijke stoffen werken, mainports);
- belang van strategische positionering bij gemeentesecretaris;
- benodigde versus beschikbare capaciteit/ middelen.

Regelgeving/wettelijk kader

- Wet Veiligheidsregio's;
- Nationale crisisstructuur/ Nationaal Crisisplan Digitaal.

Partners

- Informatiebeveiligingsdienst (IBD);
- veiligheidsregio;
- regiogemeenten;
- Nationaal Cyber Security Centrum (NCSC).

Risicocluster 3:

Gedigitaliseerde criminaliteit

Voornamelijk vermogens- en gewelds-criminaliteit ondersteund door internet

Voorbeelden, modaliteiten, modus operandi:

- oplichting via internet
- factuurfraude bedrijven of publiek orgaan
- sexting/sextortion
- geldezel-problematiek
- ransomware
- algemeen: verschuiving van criminaliteit van offline naar online

Risico's gemeente:

- groeiend criminaliteitsvraagstuk
- onveiligheidsgevoelens onder inwoners/ ondernemers
- beperkte zichtbaarheid en daardoor beperkte beheersbaarheid fenomenen
- ambtelijk en bestuurlijk onvoldoende kennis aanwezig

B1 Inzet op weerbaarheid van inwoners, bedrijven, instellingen

Aanpak/tools gemeente

- inzetten op vergroten digitale weerbaarheid inwoners en ondernemers;
- doelgroepgerichte preventiecampagnes inzetten (jongeren, senioren, laaggeletterde en ondernemers). Zowel oog hebben voor slachtoffer- als daderpreventie. Denk bij daderpreventie aan bijvoorbeeld een interventie op geldezels of projecten waarbij jongeren met IT-talent wordt geleerd hoe zij die talenten op een goede manier kunnen inzetten;
- agenderen aanpak gedigitaliseerde criminaliteit in de lokale driehoek;
- nauwe samenwerking met veiligheidspartners en platforms als Platform Veilig Ondernemen;
- bevorderen meldings- en aangiftebereidheid.

Dilemma's, overwegingen

- interne borging/samenwerking met andere domeinen (sociaal domein);
- belang van maatwerk per doelgroep;
- meebewegen met innovatie aan daderzijde;
- ontbreken van voldoende kennis bij gemeente (ambtelijk en bestuurlijk) en publieke partners;
- benodigde versus beschikbare capaciteit/ middelen.

Regelgeving/wettelijk kader

- Algemene wet bestuursrecht;
- Wetboek van Strafrecht.

Partners

- Politie (Cybercrime teams, COPS, digitale wijkagenten, het Landelijk Meldpunt Internet Oplichting (LMIO));
- jongerenwerk;
- Bureau HALT;
- welzijns- en onderwijsinstellingen;
- Openbaar Ministerie;
- Centrum voor criminaliteitspreventie en Veiligheid (CCV);
- Digital Trust Centre (DTC);
- Nationaal Cyber Security Centrum (NCSC).

B2 Ontwikkeling interventies/repressie

Aanpak/tools gemeente

- inzetten bestaande landelijk ontwikkelde methoden die wetenschappelijk zijn onderzocht. Het CCV heeft een database met lokale cyberprojecten aangelegd en jaarlijks kunnen gemeenten en samenwerkingsverbanden projecten indienen bij de Citydeal Lokale weerbaarheid en cybercrime;
- daders van cyberdelicten aanpakken via de Persoonsgerichte aanpak of Top-X aanpak;
- lokale uitwerking van een daderinterventie zoals de geldezel-aanpak;
- maatwerkprojecten die kwaliteiten van cyberdaders centraal stellen;
- impulsen aangiftebereidheid en kwaliteit aangifteproces (t.b.v. fenomeenbeelden);

Dilemma's, overwegingen

- benodigde versus beschikbare capaciteit/ middelen;
- gevarieerd en veranderlijk beeld qua kwetsbaarheden dadergroepen (o.m. op het financiële vlak);
- innovaties qua modus operandi.

Regelgeving/wettelijk kader

- Wetboek van Strafrecht.

Partners

- Politie (Cybercrime teams, COPS, digitale wijkagenten, Het Landelijk Meldpunt Internet Oplichting (LMIO));
- jongerenwerk;
- Bureau HALT;
- welzijns- en onderwijsinstellingen;
- Openbaar Ministerie;
- Centrum voor criminaliteitspreventie en Veiligheid (CCV);
- Digital Trust Centre (DTC);
- Nationaal Cyber Security Centrum (NCSC).

Risicocluster 4:

Online aangejaagde ordeverstoring

Polarisatie/maatschappelijke onrust ondersteund door internet

Voorbeelden, modaliteiten, modus operandi:

- escalatie van demonstraties, maatschappelijk protest
- inzet nepnieuws voor maatschappelijke onrust
- 'pedo-jagers'
- escalatie van hetzes tegen ambtenaren/ bestuurders/politici
- desinformatie en ondermijning openbaar gezag
- evt. (indirect) door statelijke partijen

Risico's gemeente:

- verstoring openbare orde door escalaties
- dreiging van verschillende geweldsdelicten (ook tegen lokaal bestuur)
- maatschappelijke onrust, onveiligheidsgevoelens
- verhoogd veiligheidsrisico voor de gemeentelijke organisatie/gemeentehuis
- problematische verkeersdoorstroming, hinder hulpdiensten

C Ontwikkeling en implementatie preventie-, signalerings- en responsketen

Aanpak/tools gemeente

- uitwisseling online signalen met partners als politie en jongerenwerk
- preventieve afstemming met veiligheidspartners;
- opstellen lokaal protocol online monitoring;
- binnen de crisisstructuur oefenen op grootschalige ordeverstoring;
- bewaken van openbare orde en veiligheid door benodigde interventies (communicatief, bestuurlijk, juridisch) in te zetten. Een voorbeeld van een communicatieve interventie: delen van een online tegengeluid via bestaande communicatiekanalen.

Dilemma's, overwegingen

- grijs gebied van mogelijke bestuurlijke bevoegdheden
- online monitoring moet goed afgebakend zijn
- ook ethische vraagstelling: oppassen voor controlestaat
- benodigde versus beschikbare capaciteit/ middelen
- veel signalen/relevante informatie is 'gewoon' te verkrijgen via de gebruikelijke offline werkvormen, netwerken en contacten.

Regelgeving/wettelijk kader

- illegale content: Wetboek van Strafrecht, Algemene wet bestuursrecht
- onrechtmatige content: Burgerlijk Wetboek
- Algemene Verordening Gegevensbescherming
- Artikel 172 Gemeentewet, de burgemeester is belast met handhaving van de openbare orde
- Artikel 7 Grondwet vrijheid van meningsuiting
- Artikel 10 Europees Verdrag voor de Rechten van de Mens vrijheid van meningsuiting.

Partners

- politie;
- jongerenwerk;
- Openbaar Ministerie;
- Centrum voor criminaliteitspreventie en Veiligheid (CCV);
- veiligheidsregio;
- regiogemeenten.

Overstijgende inzet

Bij de aanpak van de risico's zijn slimme verbindingen mogelijk in de vorm van maatregelen die risico's binnen meerdere risicoclusters tegelijk raken. Dit soort maatregelen heeft zeker een 'streepje voor', want ze zorgen immers voor extra rendement. Aan te bevelen is hier expliciet oog voor te hebben bij het ontwikkelen van de aanpak. Enkele voorbeelden van maatregelen/inzet die effect hebben op meerdere risicoclusters:

	1	2	3	4
Regionale afstemming en samenwerking met andere gemeenten (IV-ers en CISO's) en Veiligheidsregio inzake systeemstabiliteit (risicobeheersing) en crisisbeheersing bij ontwrichting (preparatie), impulsen beveiliging (bovenlokale) ketenpartners, ontwikkeling risicobeelden, kwetsbare ontwikkelingen binnen gemeenten, preventie en preparatie maatschappelijke onrust, uitwisseling risicobeelden online-opruiing, inzet (tools, structuren) weerbare inwoners en bedrijven.	•	•	•	•
Voorlichting/communicatie voor inwoners over preventie en follow-up slachtofferschap van gedigitaliseerde criminaliteit, hoe te handelen bij grote verstoringen, risico's en preventie (incl. eigen rol) van online-agressie/-polarisatie.		•	•	•
Voorlichting/communicatie voor ondernemers over risico's en preventie van informatiediefstal, preventie en follow-up systeemverstoring, hoe te handelen bij grote verstoringen, preventie en follow-up slachtofferschap gedigitaliseerde criminaliteit.	•	•	•	
Voorlichting/communicatie voor instellingen (zoals onderwijs, welzijn, zorg) over risico's en preventie informatiediefstal, preventie en follow-up systeemverstoring, hoe te handelen bij grote verstoringen, risico's en preventie (incl. eigen rol) online-agressie/-polarisatie, preventie en follow-up slachtofferschap gedigitaliseerde criminaliteit.	•	•	•	•
Bij gemeentelijke subsidies, aanbestedingen, vergunningen eisen stellen met betrekking tot informatiebeveiliging en systeemstabiliteit (o.m. ISO 27002). Publieke en private partners zo verder in positie brengen. Vastleggen in generieke kaders, zoals subsidieverordening en aanbestedingsbeleid.	•	•		
In scenario's van crisisoefeningen (OTO) **meerdere digitale verstoringen/risico's combineren.** Bijvoorbeeld: scenario evenement binnenstad waarbij via social media berichten over naderend zwaar weer worden verspreid en tegelijk vluchtroutes geblokkeerd worden via hack van brugsystemen.	•	•		•

Uitgangspunten aanpak

Belangrijke, generieke uitgangspunten voor de gemeentelijke inzet op digitale veiligheid zijn:

- *Iedereen heeft invloed* op de digitale veiligheid. Dit vloeit logisch voort uit integrale digitalisering van het dagelijkse werk. Communiceer en operationaliseer dit statement consequent – ambtelijk en bestuurlijk, intern en extern, publiek en privaat.
- *Werk bij alle risico's/risicoclusters integraal vanuit de veiligheidsketen.* Voorkom waar mogelijk verstoringen en slachtofferschap, maar geeft ook invulling aan de preparatie van incidentbestrijding, crisisbeheersing en gevolgafhandeling.
- *Brede scope*. Ook verstoringen bij private partijen, publieke partners en binnen de vitale infrastructuur kunnen lokaal stevig door werken en handelen van de gemeente vereisen.
- Investeer in *ketenweerbaarheid*. Dus ook die van publieke partners en private partijen. Ook hier geldt: de keten is zo sterk als de zwakste schakel.
- *Onderhoud consequent de verbinding met de verschillende gemeentelijke beleidsdomeinen* op dit cruciale onderwerp. Houd het op de agenda, op het netvlies, ferm verankerd in het dagelijkse werk.
- *Tandem Veiligheid/OOV-CISO*, zeker ook richting de interne partners. Beide taakgebieden zijn nadrukkelijk complementair in de aanpak van de geschetste risico's.
- *Wees precies*. Maak concreet waar de aangrijpingspunten zitten voor beleidsdomeinen. Reik tools op maat aan voor de private partijen waar ze echt iets mee kunnen. Blijf zo weg van plechtige beloften, maar biedt handelingsperspectief!

- *Zorg voor blijvende awareness en betrokkenheid bij gemeentesecretaris, MT, burgemeester, college en raad.* Werk aan draagvlak op strategisch niveau.
- *Leg de prioriteiten, aanpak en rollen van verschillende domeinen en randvoorwaarden strategisch vast* in het IVP en in andere beleidskaders. Borg de aanpak zo voor langere tijd.
- *Onderken je rol én kwetsbaarheid als gemeente in geval van een grote cybercrisis.* Prepareer je op situaties waarin de samenleving verstoord is, maar ook de gemeentelijke organisatie. Ook dan moet de crisisbeheersing functioneren.
- *Begin dichtbij:* Eigen huis op orde. Dat is de basis!

3 In het IVP

Overwegingen

Een robuuste en consequente inzet op digitale veiligheid, ook door gemeenten, is nodig. Hierboven is ingegaan op de risico's en de hoofdlijnen van de gemeentelijke aanpak. Het is nu van belang deze inzet ook strategisch te borgen in gemeentelijk beleid. Een plausibel kader is het IVP. Enkele overwegingen:

- De genoemde risico's en benodigde inzet hebben vrijwel alle stevige raakvlakken met het taakveld Veiligheid/OOV (waaronder ook crisisbeheersing valt).
- De onderdelen *A1: Eigen huis op orde* en *B1: Weerbaarheid inwoners/bedrijven/instellingen* zijn al onderdeel van het IVP conform *Kernbeleid Veiligheid*.
- Belangrijke aspecten van de inzet op digitale veiligheid zoals publiek-private samenwerking, maatschappelijke weerbaarheid en ketenaanpak zijn ook vaste waarden in het IVP.
- De IVP-cyclus is solide politiek-bestuurlijk ingebed en daarmee een 'betrouwbaar' vehikel voor strategische borging van inzet op digitale veiligheid.
- Het IVP is daadwerkelijk *integraal*, óók in de zin van het leggen van verbindingen tussen verschillende beleidsdomeinen met opgaven en tools rond dit vraagstuk. De verschillende beleidsdomeinen komen zo samen en afzonderlijk accuraat in positie.
- De *veiligheidsrisico's* zijn actueel, significant en worden alleen maar groter. Borging ervan in veiligheidsbeleid is hoe dan ook opportuun.

Stappenplan

Het *Kernbeleid Veiligheid* bevat een stappenplan met zes hoofdstappen voor het voorbereiden, vaststellen en in uitvoering brengen van het IVP. De veiligheidsvelden en –thema's die binnen 'integrale veiligheid' vallen (zie volgende kopje), worden hierbij alle systematisch meegenomen. Voor de hand ligt het thema Digitale Veiligheid op dezelfde wijze in het beleidsproces te integreren. De analyse en beleidsontwikkeling concentreren zich dan rond de hiervoor behandelde risicoclusters en bestanddelen van de aanpak. In schema:

Risicoclusters	Bestanddelen aanpak
1. Kwetsbaarheid van informatie **2. Kwetsbaarheid van systemen**	A1: Eigen huis op orde A2: De keten op orde A3: Preparatie op cyberincidenten – en crises
3. Gedigitaliseerde criminaliteit	B1: Inzet op weerbaarheid inwoners, bedrijven, instellingen B2: Ontwikkeling interventies/repressie
4. Online aangejaagde ordeverstoring	C: Ontwikkeling en implementatie v/e preventie-, signalerings- en responsketen

De te zetten stappen zijn:

Hoofdstappen IVP	Uitvoering/deelstappen t.b.v. verwerking Digitale veiligheid in IVP
1. Opstart IVP-proces	• beknopte ambtelijke 'preview' door Veiligheid/OOV, CISO, PO, Communicatie van: - risicobeeld digitale veiligheid > actualiteit ten aanzien van de vier risicoclusters; - huidige inzet op risico's/vormgeving van zes bestanddelen van de aanpak; - wenselijke *programmatische* uitwerking aanpak digitale veiligheid: met welke partners/ wanneer/in welke vorm/…?; - evt. benodigd specifiek onderzoek e.d. t.b.v. effectieve uitwerking digitale veiligheid in traject IVP; - te betrekken partijen bij uitwerking digitale veiligheid in IVP; - wenselijke vertegenwoordiging digitale veiligheid in brede IVP-werkgroep; • verwerking in startnotitie IVP (ter bestuurlijke vaststelling); • samenstellen IVP werkgroep incl. vertegenwoordiging digitale veiligheid; • startbijeenkomst werkgroep.
2. Veiligheidsanalyse	• nadere inventarisatie en analyse van: - aard en omvang risico's; - huidige inzet op risico's en omissies/verbeterpunten daarin; - prioritair karakter van thema digitale veiligheid/deelthema's daarvan.
3. Prioritering	• afweging en 'tussenbesluit' over prioritaire status in het IVP van digitale veiligheid (of deelthema's daarvan); • in gesprek met de raadsleden; • indien niet prioritair: opnemen als strategisch thema in het IVP.
4. Opstellen IVP	• beleidsmatige uitwerking digitale veiligheid (als prioriteit of strategisch thema): - afbakening/deelthema's; - doelstellingen; - hoofdlijnen aanpak; - partners. • inclusief markering eventuele integrale programmatische uitwerking > lokale *Agenda Digitale Veiligheid*.
5. Opstellen Uitvoeringsplan	• concretisering uit te voeren acties/in te zetten tools; • inclusief rolverdeling, tijdpad, begroting; • schets governance/P&C-systematiek (bijvoorbeeld: ambtelijke coördinatiegroep en stuur-groep digitale veiligheid).
6. Van beleid naar uitvoering	• voorbereidingsstappen eventuele integrale programmatische uitwerking > lokale *Agenda Digitale Veiligheid*; • implementatie governance/P&C-systematiek; • consequente doorvoering vastgestelde inzet/acties.

Een extra 'veiligheidsveld'?

Tot dusverre definieert het Kernbeleid Veiligheid (edities 2003 t/m 2021) 'integrale veiligheid' aan de hand van vijf veiligheidsvelden, met daarbinnen telkens meerdere veiligheidsthema's (zie hieronder). Dit spectrum vormt het vertrekpunt voor de beleidsontwikkeling, kader voor de veiligheidsanalyse en toets voor de integraliteit van het IVP. Dit dient immers, na de lokale 'maatwerkordening' van thema's (prioriteiten en strategische thema's) in stap 3 en verder van het stappenplan, nog steeds de vijf veiligheidsvelden effectief en integraal te bestrijken. Het thema Informatieveiligheid is ondergebracht in het vijfde veiligheidsveld: *Integriteit en veiligheid*.

Veilige woon- en leefomgeving	Bedrijvigheid en veiligheid	Jeugd en veiligheid	Fysieke veiligheid	Integriteit en veiligheid
1.1 Sociale kwaliteit	2.1 Veilig winkelgebied	3.1 Jeugdoverlast	4.1 Verkeersveiligheid	5.1 Polarisatie en radicalisering
1.2 Fysieke kwaliteit	2.2 Veilige bedrijven-terreinen	3.2 Jeugdcriminaliteit/ individuele probleem jongeren	4.2 Brandveiligheid	5.2 Georganiseerde/ ondermijnende criminaliteit
1.3 Objectieve veiligheid/ veel voorkomende en 'high impact'-criminaliteit	2.3 Veilig uitgaan	3.3 Jeugd, alcohol en drugs	4.3 Externe veiligheid/ Omgevingsveiligheid	5.3 Weerbare overheid/ weerbaar bestuur
1.4 Subjectieve veiligheid	2.4 Veilige evenemen-ten	3.4 Veilig in en om de school	4.4 Rampenbestrijding en crisisbeheersing	5.4 Informatie-veilig-heid
	2.5 Veilig toerisme			5.5 Ambtelijke en bestuurlijke integriteit

Gezien de omvang, actualiteit én dynamiek van risico's op het vlak van digitale veiligheid, lijkt toevoeging van een extra, zesde, veiligheidsveld Digitale Veiligheid gepast. Prominente positionering als separaat veiligheidsveld in Kernbeleid Veiligheid markeert het belang van deze vraagstukken en faciliteert effectieve uitwerking en operationalisering in het lokale beleidsproces, inclusief de dwarsverbanden met veiligheidsthema's binnen andere velden. Bij de eerstvolgende herijking van het Kernbeleid Veiligheid wordt bepaald of en hoe deze aanpassing van de systematiek kan worden vormgegeven.

Veilige woon- en leefomgeving	Bedrijvigheid en veiligheid	Jeugd en veiligheid	Fysieke veiligheid	Digitale veiligheid	Integriteit en veiligheid
				5.1 Kwetsbaar-heid van informatie	
				5.2 Kwetsbaar-heid van systemen	
				5.3 Gedigitali-seerde criminali-teit	
				5.4 Online aangejaagde ordeverstoring	

Documentatie

- Berenschot, Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten (mei 2020).
- CCV, Cybercrime.
- CCV, Database lokale cyberprojecten.
- CCV, Lokale Cyberwegenkaart (juni 2020).
- Cybersecurity Alliantie, Cyberkompas voor Ondernemend Nederland.
- Gemeente Amsterdam, Agenda Digitale Veiligheid (juni 2020).
- Gemeente Den Haag, Agenda Digitaal Veilig Den Haag (oktober 2021).
- IFV, Bestuurlijke netwerkkaarten crisisbeheersing.
- IFV, Whitepaper digitale ontwrichting en cyber (september 2019).
- Noord-Holland Samen Veilig, Jaarplan cyber 2022 (2022).
- Stol, W., Bantema, W., Lokaal bestuur in een digitaliserende samenleving (oktober 2021).
- VNG, Agenda Digitale Veiligheid (2020).
- VNG, Resolutie Digitale Veiligheid (december 2020).
- VNG, CCV, Inventarisatie cyberveiligheid (2017).
- NCSC, Nationaal Crisisplan Digitaal (februari 2020).

Meer weten over digitale veiligheid? Check het dossier op de website van de VNG:

Vereniging van
Nederlandse Gemeenten

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

info@vng.nl

mei 2022

vng.nl