

Focusblad Digitale Veiligheid

VAR - 26 september 2022

- Kernbeleid Veiligheid
- Verschuiving van traditionele criminaliteit, naar digitaal
- Onvoldoende aandacht en budget

- <u>Momentum:</u>
  - Nieuwe IVP’s 2023
  - Verkiezingen

Aanleiding

VNG Resolutie Digitale Veiligheid 2021

Unaniem voor intensivering van de gemeentelijke inzet

Prioriteit

Doel

Beschrijft:

- De veiligheidsrisico’s binnen digitale veiligheid
- De rol van de gemeenten
- Het aanbevolen pad van uitwerking

Risico's	Aanpak	Cyberwegenkaart CCV
Risicocluster 1: **Kwetsbaarheid van informatie** *Diefstal, verlies, aantasting van informatie*	**A1 Eigen huis op orde** *Veiligheid van informatie en systemen binnen de gemeentelijke organisatie*	→ **Eigen huis op orde**
Risicocluster 2: **Kwetsbaarheid van systemen** *Digitale ontregeling, ontwrichting, blokkades van systemen*	**A2 De keten op orde** *Veiligheid van informatie en systemen bij ketenpartners van de gemeente*	
	A3 Preparatie op cyberincidenten en -crises *Digitale ontwrichting, met mogelijk fysieke impact bij publieke en private partijen*	→ **Cyberincidenten en -crises**

Risico's

Risicocluster 3:
Gedigitaliseerde criminaliteit
Voornamelijk vermogens- en gewelds-criminaliteit ondersteund door internet

B1 Inzet op weerbaarheid van inwoners, bedrijven, instellingen

B2 Ontwikkeling interventies/ repressie

→ **Cybercrime en gedigitali-seerde criminaliteit**

Risicocluster 4:
Online aangejaagde ordeverstoring
Polarisatie/maatschappelijke onrust ondersteund door internet

C Ontwikkeling en implementatie preventie-, signalerings- en responsketen

→ **Online aangejaagde ordeverstoring**

Risico's

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

Risico's

A1 Eigen huis op orde

Aanpak/tools gemeente

- doorvoering Baseline Informatie-beveiliging 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.

Aanpak

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 cyber-crisis (hoe crisis effectief te managen?)
- hoge herstelkosten
- uitvallen belangrijke voorzieningen binnen gemeentegrenzen
- imagoschade, boetes en schadeclaims

Risico's

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.

Aanpak

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).

Aanpak

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

Risico's

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).

Aanpak

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).

Aanpak

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

Risico's

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;

Aanpak

Focusblad biedt hulp bij het uitwerken:

- Aanpak die meerdere punten raakt →
  X regionale afstemming
  X communcatie inwoners/ondernemers
  X gecombineerde crisisoefeningen met meerdere digitale verstoringen

Uitwerking

- Focusblad: https://vng.nl/publicaties/focusblad-digitale-veiligheid

- In het verlengde hiervan:
  - 5 Cyber Sessions
  - Bestuurlijke gesprekken

Praktische informatie

Vragen?

Neem contact op via

Shanna.fontaine@vng.nl

Vervolg