Teksten over digitale veiligheid in gemeentelijke Integrale Veiligheidsplannen (IVP's)

Neem deze onderstaande tekst, net als andere gemeenten, op in het integraal veiligheidsplan (IVP). Hiermee zorgen we voor een uniforme taal en focus op dit thema.

"Wij geven prioriteit aan een digitaal weerbare gemeente. We zetten ons in om te voorkomen dat (1) inwoners en (2) bedrijven slachtoffer worden van cybercrime en gedigitaliseerde criminaliteit. Ook zorgen we ervoor dat de (3) informatiebeveiliging van de gemeente op orde is en dat we goed voorbereid zijn op cybercrises en (4) online aangejaagde ordeverstoringen. Dat doen we door […]".

Neem een kijkje in de IVP's van andere gemeenten om te zien hoe zij digitale veiligheid borgen in hun gemeentelijk beleid. In dit document staan voorbeelden van gemeente Dordrecht, Breda, Amersfoort en het samenwerkingsverband Noord-Holland Samen Veilig. Voor de volledige plannen verwijzen we je naar de bronnen die erbij staan weergegeven. Heb je vragen? Neem contact op met CCV-adviseur Sten Meijer, via sten.meijer@hetccv.nl

DORDRECHT

Bron: https://www.magazinedordrecht.nl/integraal-veiligheidsplan/

Een betrekkelijk nieuw fenomeen is de digitale criminaliteit (cybercriminaliteit). Voorbeelden hiervan zijn het gebruik van ransomware (gijzelsoftware), DDoS aanvallen en hacks. Daarnaast is er digitale criminaliteit, waarbij ICT een rol speelt, zoals internetoplichting, cyberpesten en phishing (nepwebsites). De zorgen over de effecten van digitale ondermijnende criminaliteit in wijken en buurten nemen steeds verder toe. De maatschappelijke weerbaarheid tegen deze effecten blijft achter bij de groeiende dreiging van digitale criminaliteit. Burgers, overheid en bedrijven hebben allemaal een eigen verantwoordelijkheid op dit gebied. Onze gezamenlijke uitdaging is de stad weerbaar te maken tegen cybercriminaliteit. Dordtse ondernemers krijgen bijvoorbeeld een training om te voorkomen dat zij het slachtoffer worden van deze vorm van criminaliteit.

- Verdere afname van vermogens- en geweldscriminaliteit in Dordrecht.
- Vergroten van de maatschappelijke weerbaarheid tegen de digitale dreiging.
- Inzicht krijgen in de knelpunten en risico's van voorzieningen (onder andere elektriciteitsvoorzieningen, bruggen en ziekenhuizen) die cruciaal zijn voor onze stad op het gebied van digitale veiligheid.

Zo kunnen zij preventieve maatregelen nemen om te voorkomen dat hun eigendom wordt gestolen en kunnen zij de politie helpen bij het opsporen van strafbare feiten, via bijvoorbeeld een Whatsapp-groep en Burgernet.

Wat gaan we doen:

- inzicht krijgen in de aard en omvang van digitale criminaliteit;
- bewustwording van medewerkers van de gemeente;
- het trainen van Dordtse ondernemers om te voorkomen dat zij slachtoffer worden van cybercriminaliteit;
- Dordtse bewoners bewust maken van de gevaren van de digitale samenleving en concrete adviezen op dit gebied geven;
- onderzoek naar knelpunten en risico's van de vitale infrastructuur en kwetsbare bedrijven in de stad (onder andere elektriciteitsvoorzieningen, bruggen, ziekenhuizen) en op basis daarvan verdere acties ondernemen.

BREDA

Bron: https://hetccv.nl/onderwerpen/veiligheid-en-zorg/praktijkvoorbeelden/breda-meerjarenprogramma-veiligheid/

Op dit moment is de politie de meest actieve partij binnen de veiligheidsketen op het gebied van cybercriminaliteit. Zij geven aan dat zij een landelijke verschuiving zien van traditionele delicten naar digitale delicten. Waar de traditionele criminaliteit al jaren daalt, neemt de geregistreerde digitale criminaliteit toe. Deze trend geldt ook voor Breda

De aanpak van cybercriminaliteit bestaat uit drie onderdelen: preventie, verstoring en repressie. Op dit moment zet de Gemeente Breda nog niet actief in op preventie van cybercriminaliteit. Verschillende teams binnen de politie zijn actief op het gebied van repressie van digitale criminaliteit. Deze repressie is echter om verschillende redenen een enorme uitdaging:

- Door het gebruik van internet zijn geldstromen niet langer rechtstreeks herleidbaar.
- Door de vluchtigheid van gegevens verdwijnen sporen snel.
- Het internet kent verschillende manieren om te anonimiseren.
- Cybercrime kent geen begrenzing in tijd of plaats. Het is voor cybercriminelen relatief eenvoudig om in korte tijd veel slachtoffers te maken en veel geld te verdienen.

Uit onderzoek blijkt dat twee doelgroepen het vaakst slachtoffer zijn van digitale delicten: jongeren en MKB-bedrijven. Jongeren, die veel actief zijn op internet, hebben relatief vaker te maken met cybercriminaliteit. Deze groep verdient dan ook bijzondere aandacht. Verder komen inbraken op de digitale bedrijfsvoering van ondernemers veel voor. De Nederlandse economie lijdt jaarlijks 10 miljard euro schade door cybercriminaliteit, waarvan een groot deel voor rekening komt van ondernemers. Veilig ondernemen kan niet langer los worden gezien van het digitale domein. Daarnaast moeten we aandacht hebben voor de vitale infrastructuur. We hebben op dit moment nog geen duidelijk beeld van de grootste vitale risico's van cybercriminaliteit voor Breda.

De omvang en ernst van digitale dreigingen in Nederland is significant en neemt in de toekomst alleen maar toe.

Jongeren
Voor hedendaagse jongeren is de digitale wereld een deel van hun leven. Als we hen willen helpen om optimaal en veilig gebruik te maken van de digitale wereld, moeten we continu aandacht hebben voor skills, eigen verantwoordelijkheid en veiligheid. Kinderen kunnen zelf niet altijd voor een veilige online omgeving zorgen of voldoende digitaal weerbaar zijn. Zij hebben hiervoor hulp nodig van hun ouders, hun school en ketenpartners zoals de gemeente, de politie, de GGD, Halt en het CJG. Het is belangrijk dat jongeren mediawijs worden en leren om zorgvuldig en verstandig om te gaan met (privé-)informatie op internet. Hun school is de ideale plek om risico's van internet en sociale media te bespreken. Daarbij moet duidelijk worden wat de gevolgen kunnen zijn van online wangedrag, waar jongeren terecht kunnen met signalen en hoe zij zelf weerbaar kunnen worden.

Ondernemers
Bredase ondernemers zijn verantwoordelijk voor hun eigen veiligheid. De Gemeente Breda heeft hierin een faciliterende rol door hen te informeren en concrete tips te bieden. We willen meer bewustzijn creëren voor de risico's en vormen van digitale criminaliteit. Daarbij moeten ondernemers concrete handvatten krijgen om hun eigen digitale veiligheid te verbeteren.

Bewoners
Ook op het gebied van cybercriminaliteit kunnen we bewoners betrekken, net als bij de preventie van woninginbraak. Dankzij het uitgebreide bewonersnetwerk van Buurtpreventie Breda (met 17.000 aangesloten adressen en 2000+ actieve vrijwilligers) kunnen we veel Bredanaars bereiken, ook op het gebied van cyberpreventie. Het doel is om buurtbewoners actief te betrekken bij het thema en de

buurtpreventen probleemeigenaar te maken. De buurtpreventen kunnen op hun beurt als ambassadeurs optreden door hun straatgenoten bewust te maken en te informeren.

Vitale infrastructuur
We willen als gemeente een duidelijk beeld hebben van de grootste risico's op het gebied van cybercrime. Door deze risico's in kaart te brengen, kunnen we gericht preventieve acties inzetten. Dit pakken we samen op met de Veiligheidsregio.

Wat is nodig om daar te komen?
De aanpak van cybercriminaliteit in Breda staat nog in de kinderschoenen. Voor een succesvolle aanpak moeten we investeren in kennis en in samenwerking met onder meer het CJG, de GGD, Halt, de politie, de Veiligheidsregio, scholen, ondernemers (verenigingen) en bewoners. Een hogere cyberweerbaarheid in Breda is een gezamenlijke verantwoordelijkheid. Opsporing en vervolging van cybercriminaliteit zijn van oudsher een taak van de politie en het Openbaar Ministerie. Preventie is meer de taak van gemeenten. Willen we succes boeken, dan is een integrale aanpak nodig, met oog voor elkaars taken en verantwoordelijkheden. Hoewel cybercrime niet gebonden is aan grenzen, heeft deze vorm van criminaliteit ook zijn raakvlakken in de 'echte' wereld. Op deze raakvlakken liggen kansen voor een effectieve integrale aanpak. Verder kan de beperkte mogelijkheid om aangifte te doen van digitale delicten een barrière zijn: bij cybercriminaliteit is de keuze van het soort delict beperkt (slechts één delictklasse). De verwachting is dat de aangiftebereidheid toeneemt als er meer mogelijkheden zijn om cybercriminaliteit als delict op te geven. Met een projectplan geven we invulling aan een eenduidig preventiebeleid met concrete maatregelen op het gebied van cybercriminaliteit. Hierin is aandacht voor de verschillende aspecten: jongeren, buurtbewoners, ondernemers en de vitale infrastructuur in de stad.

Analyseren
Informatie omtrent cybercriminaliteit wordt geïnventariseerd en vervolgens geanalyseerd om een beeld te krijgen van omvang, Modus Operandi en slachtofferschap. Gezien het globale karakter van cybercriminaliteit is het niet altijd makkelijk om een lokaal veiligheidsbeeld te schetsen, maar landelijke trends kunnen vertaald worden naar de Bredase situatie. Op basis van de beschikbare informatie wordt een veiligheidsanalyse gemaakt die voor Breda relevant is.

Anticiperen
Cybercriminaliteit is net als het internet zeer dynamisch en continu in ontwikkeling. Het is daarom belangrijk om trends en ontwikkelingen nauwlettend in de gaten te houden en met deze trends mee te bewegen. Dit vraagt om een flexibele, snelle aanpak waarbij we als gemeente meebewegen met de trends en ontwikkelingen die we signaleren op het gebied van cyberveiligheid. We nemen de stakeholders - waaronder jongeren, ondernemers en bewoners - mee in deze flexibele aanpak en informeren hen tijdig. Wanneer nieuwe vormen van digitale criminaliteit de kop opsteken, worden deze direct meegenomen in de preventie aanpak.

Activeren
In een participerende samenleving zijn bewoners en ondernemers partners in veiligheid, zo ook op het gebied van cybercriminaliteit. Het verbeteren van de digitale weerbaarheid van de stad is een gezamenlijke taak. De gemeente heeft hierin een activerende en faciliterende rol door bewoners en ondernemers te informeren, bewust te maken over wat er speelt en concreet handelingsperspectief te bieden op gebied van cyberveiligheid.

AMERSFOORT

Bron: https://www.amersfoort.nl/web/file?uuid=ff98645b-2a9f-4328-8fbb-d5dc8b5d27dc&owner=a46adc0b-3fdf-46de-afba-c11e346680c1&contentid=10456

De samenleving digitaliseert. Steeds vaker regelen inwoners, ondernemers en publieke instellingen hun zaken en diensten online. De online wereld biedt veel mogelijkheden en kansen, maar er zijn ook risico's. Criminaliteit en overlast verschuift in de vorm van cybercrime en gedigitaliseerde criminaliteit steeds vaker naar het cyberdomein. In Amersfoort wordt jaarlijks circa een op de negen inwoners slachtoffer van cybercrime. De impact van cybercrime is groot. Slachtoffers kunnen naast financiële schade soms ook jaren online de gevolgen ondervinden van hun slachtofferschap. Ook rampen en crises met een digitale oorzaak kunnen de samenleving langdurig ontwrichten. Samen met politie, het Openbaar Ministerie en onze lokale en regionale ketenpartners richten we ons op het digitaal weerbaar maken van onze stad. We doen dat door ons eigen huis op orde te brengen en onze ondernemers en inwoners bewuster te maken van de online risico's, zodat slachtoffer- daderschap kan worden voorkomen.

Ambitie
We dringen het slachtofferschap van cybercrime terug door inzicht te krijgen in de aard en omvang, het weerbaar maken van onze inwoners en ondernemers en door barrières op te werpen voor daders en dadergroepen. We streven naar een daling van slachtofferschap en een stijging van meldingsbereidheid. We hebben het eigen digitale huis op orde en bereiden ons voor op een crisis met digitale oorzaak.

Cybercrime bestaat uit meerdere digitale delicten, waarvan een aantal - zoals hacken en internetfraude - inmiddels al vaker voorkomt dan fietsendiefstal. Jongeren in de leeftijd van 12-25 jaar zijn in het bijzonder kwetsbaar. Zij worden het vaakst slachtoffer van cybercrime omdat zij vaker online zijn en op het web meer experimenteren dan andere leeftijdsgroepen. Ook ondernemers hebben flink last van cybercrime. Jaarlijks kampt meer dan de helft van de ondernemers met ICT-veiligheidsincidenten en het aantal slachtoffers van cybercrime is één op de vijf. De totale maatschappelijke schade wordt geschat op circa 10 miljard euro ieder jaar opnieuw. Desondanks blijft de melding- en aangiftebereidheid van slachtoffers betrekkelijk laag. Iets meer dan een kwart van de cyberincidenten wordt gemeld, waarvan slechts 13% bij de politie. Het vergroten van bewustwording en investeren in de preventie van slachtofferschap is dus van groot belang.

De gemeente Amersfoort is óók vatbaar voor cybercrime. Amersfoort verleent tal van diensten aan inwoners. Wanneer deze processen worden verstoord, kan dat grote gevolgen hebben. Daarnaast is de gemeente Amersfoort verantwoordelijk voor de rampen- en crisisbeheersing van de stad. Wanneer rampen en crises een digitale oorzaak kennen, moeten we daar goed op voorbereid zijn. Dit kunnen we niet alleen. De Veiligheidscoalitie Midden-Nederland heeft daarom samen met de 39 aangesloten gemeente afgesproken dat het thema cyberveiligheid en digitale weerbaarheid één van de regionale speerpunten voor 2019-2023 is. We zoeken samen naar nieuwe manier om de digitale weerbaarheid van onze regio te vergroten.

Het digitaal weerbaar maken en houden van de stad vraagt om beleid dat vanuit verschillende invalshoeken is ingestoken. Samen met onze ketenpartners richten we ons op vier punten:

- Inzicht in de aard en omvang van slachtofferschap cybercrime
- Eigen huis op orde
- Preventie en bewustwording kwetsbare groepen in de stad
- Cybergevolgenbestrijding

Wat is cybercrime?
Cybercrime is criminaliteit dat met behulp van ICT-apparatuur (computers, tablets, smartphones) gepleegd is, gericht op ICTapparatuur. Vormen van cybercrime zijn hacking, ransomware en bijvoorbeeld virussen of wormen. Naast cybercrime is er ook steeds vaker sprake van gedigitaliseerde criminaliteit.

Dat zijn ‘klassieke’ delicten in een ‘digitaal’ jasje zoals online identiteitsfraude, internetoplichting, sexting en online afpersing.

Inzicht aard en omvang
De aandacht voor cybercrime en digitale veiligheid is nog betrekkelijk nieuw. Er is hierdoor weinig bekend over slachtofferschap van cybercrime in de gemeente Amersfoort. Om ons beleid optimaal in te richten is meer inzicht in de aard en omvang nodig. Hierdoor weten we beter welke behoeften inwoners en ondernemers hebben en welke trends er zijn. We doen dat door digitale veiligheid op te nemen in de tweejaarlijkse monitor Leefbaarheid en Veiligheid en door het Amersfoort-Panel te bevragen op het thema digitale veiligheid. Daarnaast willen ze inzicht in het verhaal achter de cijfers. Het cyberdomein verandert vliegensvlug, we willen daarom weten wat er in de stad leeft en speelt zodat we kunnen inspelen op de actualiteit. Hieraan

Eigen huis op orde
Amersfoort verzamelt en verwerkt persoonsgegevens en beheert tal van processen met behulp van ICT-systemen. Onze inwoners en ondernemers mogen van ons verwachten dat we daar zorgvuldig mee omgaan en dat onze dienstverlening beschikbaar is en blijft. De systemen waar wij mee werken moeten veilig zijn ingericht zodat potentiele indringers buiten de deur worden gehouden. Belangrijker nog dan de systemen zijn de human factors. Als het toch misgaat is het zaak dat onze medewerkers digitale gevaren (zoals phishingmails, malware en malafide websites) herkennen en die adequaat weten af te handelen. Bewustwordingscampagnes en herhaaldelijke eLearning modules zijn daarin onmisbaar.

Preventie en bewustwording kwetsbare groepen in de stad
De online wereld ontwikkelt zich in een rap tempo. Niet iedereen is zich bewust van de risico’s die zij dagelijks online lopen. Slachtoffers van cybercrime doen vaak geen melding bij de politie of betrokken instanties. Samen met de bij de Veiligheidscoalitie aangesloten partners investeren we in het bewust maken van inwoners, ondernemers en instellingen over digitale veiligheid en op welke wijze zij hun kans op slachtofferschap kunnen verkleinen. We besteden in het bijzonder aandacht aan onze jongeren en onze kleine- en middelgrote ondernemers omdat hier de urgentie, kennis en middelen om zichzelf effectief te beschermen kan ontbreken. We doen dit samen met onderwijsinstellingen, kennisinstituten en de reeds bestaande netwerken (zoals het Keurmerk Veilig Ondernemen) om zo dicht mogelijk bij de behoeftes van onze inwoners en ondernemers aan te sluiten.

Cybergevolgenbestrijding
De vitale infrastructuur (elektriciteit, schoonwatervoorziening, noodnummers e.d.) is steeds vaker gedigitaliseerd. Wanneer deze systemen worden verstoord, kan dat de stad ontwrichten. We zien steeds vaker dat rampen en crises daardoor een digitale hoopt de speciaal aangestelde digitale wijkagent een bijdrage te leveren. oorzaak hebben. Om in dergelijke gevallen terug te keren naar de ‘normaalsituatie’, zijn andere vaardigheden nodig dan bij klassieke rampen en crises. Het is om die reden nodig dat de cybergevolgenbestrijding wordt opgenomen in de plannen van de crisisorganisatie. Dit wordt samen met de Veiligheidsregio Utrecht vormgegeven.

NOORD HOLLAND SAMEN VEILIG

Bron: https://nh-sv.nl/action/?action=jvdownload&id=45 en jaarplan: https://jp.nh-sv.nl/thema/cyber/

Ons leven is voor een groot deel digitaal. De problemen waarvoor we als overheid staan ook. Want inwoners van de 32 gemeenten in onze eenheid in Noord-Holland worden slachtoffer van cybercrime. Het is al lang niet meer de vraag óf maar wanneer en met welke impact. De openbare orde en veiligheidsproblematiek kent een digitale component die steeds groter wordt. Ook in de troonrede staat dat digitale criminaliteit en veiligheid meer investeringen vragen, omdat de wereldwijde dreigingen op tal van manieren toenemen.

De politie ziet het totaal aantal meldingen en aangiften in de eenheid Noord-Holland in de eerste helft van 2021 35 procent stijgen ten opzichte van deze periode in 2020. Het totaalbedrag dat met cybercrime in de eenheid Noord-Holland is buitgemaakt in de eerste helft van 2021 is € 8.995.472,24. Dat is een toename van € 5.024.362,24 vergeleken met een jaar eerder. De totale schade is 126,5% gestegen. Deze doorgaande stijging is al een aantal jaren zichtbaar, waardoor we inmiddels spreken over veelvoorkomende criminaliteit (VVC). De impact is soms dusdanig dat het ook kenmerken van high impact crime (HIC) vertoont. Dit zijn delicten waarvan de impact groot is voor het slachtoffer, te denken valt aan woninginbraken, overvallen en straatroven. In 2021 is er onder de vlag van Noord-Holland Samen Veilig (NHSV) hard gewerkt om in gemeenten het aantal slachtoffers en daders te verminderen. Iedere gemeente deed op zijn minst aan één van de vier cyberprojecten (‘Geldezels’, ‘re_B00TCMP’, ‘het slachtoffer spreekt’, ‘Online Orde’) mee.

Aanpak en prioriteiten
Medewerkers van het project ‘Aanpak cybercrime en gedigitaliseerde vormen van criminaliteit’ ondersteunen de 32 gemeenten, politie en het Openbaar Ministerie (OM) in het gezamenlijk aanpakken van cybercriminaliteit in brede zin. Cyberveiligheid omvat zowel de aanpak van cybercrime als gedigitaliseerde criminaliteit. Het gaat om alle delicten waarbij criminelen ICT als middel inzetten. In 2022 zetten we de koers van een jaar eerder voort. De kern van onze aanpak draait om het vergroten van de cyberweerbaarheid van onze inwoners. Dit sluit aan bij de kaders van het Integraal Meerjarenbeleidsplan Veiligheid Noord-Holland 2019-2022, Pamflet Overleg Cyberburgemeesters Nederland maart 2021, de cyberwegenkaart van het CCV, Cyberwegenkaart Infographic en de digitale veiligheidsagenda 2020-2024 van de VNG.

De ambities voor 2022 moeten worden bijgesteld. Dit is een zorgelijke ontwikkeling omdat de aanpak van cyber en gedigitaliseerde criminaliteit veel meer prioriteit binnen het veiligheidsdomein moet krijgen. Onder cybercrime vallen delicten waarbij ICT het middel en doel is. Hierbij valt te denken aan hacken en ransomware. Bij gedigitaliseerde criminaliteit gaat het om traditionele delicten waarbij ICT als middel wordt ingezet, maar niet het doel is. Te denken valt aan (identiteits-)fraude. De ervaring uit 2021 leert echter dat de uitvoering van de projecten en de bestuurlijke en ambtelijke aandacht voor dit veiligheidsthema meer tijd en capaciteit vragen dan beschikbaar is.

In 2022 werken wij door aan de projecten die in 2021 zijn opgestart. Dit heeft meerdere redenen. In de eerste plaats is de uitvoering en lokale inbedding van de projecten niet aan een kalenderjaar gebonden en vragen die in 2022 nog aandacht. Daarbij komt dat de gemeenten de meerwaarde van de projecten zien en graag meedoen. Ook willen wij in 2022 gemeenten, die in 2021 nog niet meededen, de kans geven aan te haken.

Dit zijn de gemeentelijke taken en verantwoordelijkheden:

- Het eigen huis op orde brengen en houden (informatiebeveiliging).
- De voorbereiding op cyberincidenten- en crises.
- De voorbereiding op online aangejaagde ordeverstoringen.

- Het regisseren van het lokaal veiligheidsbeleid, inclusief de preventieve aanpak van cybercrime en gedigitaliseerde criminaliteit.

In 2020 en 2021 heeft Noord-Holland Samen Veilig via diverse initiatieven de eerste twee punten bij verantwoordelijke functionarissen meer onder de aandacht gebracht en hen geattendeerd op de veiligheidsrisico's die gemeenten kunnen lopen. Gemeentelijke organisaties en Veiligheidsregio's pakken de verantwoordelijkheid verder op. In 2022 werken wij met gemeenten door aan de punten 3 en 4, met drie actielijnen: vergroten van de cyberweerbaarheid, het versterken van de lokale aanpak cybercrime en gedigitaliseerde criminaliteit en het investeren in kennis en vaardigheden. Waar dit kan, doen wij dit in nauwe samenwerking met de Vereniging van Nederlandse Gemeenten (VNG), het Nederlands Genootschap van Burgemeesters (NGB), het ministerie van Justitie en Veiligheid (JenV), het ministerie van Binnenlandse Zaken en Veiligheid (BZK) en de andere regionale samenwerkingsverbanden.