



Achtergrondinformatie Digitale Veiligheid voor gemeentelijke IVP's

Datum: 15-10-2026

Doel van dit document

Deze notitie biedt achtergrondinformatie en onderbouwing voor gemeenten die digitale veiligheid willen opnemen in hun Integraal Veiligheidsplan (IVP). De notitie is bedoeld als verdieping op de documentatie '**IVP-bouwstenen Digitale Veiligheid**'. Gemeenten kunnen de bouwstenen rechtstreeks gebruiken in hun IVP en deze aanvullen met elementen uit deze achtergrondnotitie die aansluiten bij de lokale situatie.

Wat zien we?

Ontwikkelingen

- Meer dan 40% van alle criminaliteitsslachtoffers in Nederland is het gevolg van online criminaliteit, en naar verwachting zal dit blijven stijgen. Daarnaast zien we dat digitale middelen in toenemende mate worden ingezet bij traditionele delicten. Volgens professionals in Midden-Nederland bevat inmiddels de helft van de aangiften bij politie een online component, en zal dit aandeel over vijf jaar zelfs 85% zijn.
- Ook zijn complete criminele software zoals botnets en ransomware met één druk op de knop beschikbaar zonder dat diepgaande technologische kennis nodig is. Deze drempelverlaging wordt verder ondersteund door de brede toegankelijkheid van AI.
- De digitalisering van de samenleving gaat onverminderd door, maar we zijn nog onvoldoende voorbereid om inwoners en ondernemers weerbaar te maken tegen online criminaliteit. De verwachting is dat burgers, bedrijven en overheid de komende jaren steeds vaker getroffen worden door online criminaliteit, en Europol voorspelt dat online fraude andere vormen van zware en georganiseerde misdaad gaat overtreffen. Het is daarom essentieel dat de gemeente reageert op deze ontwikkelingen en verdere escalatie tegengaat.
- Online criminaliteit neemt niet alleen toe in omvang, maar ontwikkelt zich ook voortdurend. Vormen zoals phishing, bankhelpdeskfraude, sextortion, beleggingsfraude en ransomware treffen een steeds grotere en bredere groep slachtoffers. Hierdoor is sprake van massaal slachtofferschap. Ook binnen gemeenten worden inwoners, ondernemers en maatschappelijke organisaties dagelijks geconfronteerd met deze risico's.

Impact online criminaliteit slachtofferschap

- Uit onderzoek is meermaals gebleken dat online criminaliteit slachtofferschap minstens zo ingrijpend is als slachtofferschap van traditionele criminaliteit, als dan niet ingrijpender. Mensen kunnen niet alleen financiële schade leiden, maar ze kunnen ook te maken krijgen met emotionele en sociale consequenties zoals stress, schaamte en "*victim blaming*". Daarnaast zien we dat het vertrouwen van slachtoffers in de overheid en andere organisaties afneemt wanneer zij geen passende begeleiding en nazorg krijgen. De impact van online criminaliteit raakt daarmee verder dan het individuele slachtoffer en raakt ook het vertrouwen in de samenleving als geheel.
- Deze gevolgen onderstrepen het belang van een gemeentelijke aanpak waarbij niet alleen aandacht is voor preventie, maar ook voor het herkennen, ondersteunen en doorverwijzen van slachtoffers.

Grenzeloosheid online criminaliteit in thematiek

- Digitale veiligheid is al lang geen losstaand thema meer, maar raakt alle onderdelen van het veiligheidsbeleid. De online en offline leefwereld zijn steeds sterker met elkaar verweven. Hierdoor verschuiven ook bestaande veiligheidsvraagstukken steeds vaker naar de digitale context.
- Delictsvormen zoals ondermijning, oplichting, radicalisering en geweld kennen steeds vaker een online component. Digitale veiligheid is daarmee niet langer een afzonderlijk veiligheidsthema, maar een randvoorwaarde voor een veilige en weerbare samenleving.

- Deze ontwikkeling vraagt van gemeenten een integrale benadering. Digitale veiligheid raakt niet alleen openbare orde en veiligheid, maar ook jeugdbeleid, zorg, onderwijs, dienstverlening en economische ontwikkeling. De urgentie voor gemeenten om hun rol te pakken bij het vergroten van digitale weerbaarheid, het vroegtijdig signaleren van online criminaliteit, en het ondersteunen van slachtoffers wordt dan ook benadrukt door minister Van Weel van Justitie en Veiligheid.
- Daarnaast zijn signalen, meldingen en informatie over daders vaak verspreid over verschillende organisaties. Slachtoffers van online fraude kunnen bijvoorbeeld terechtkomen bij politie, banken, de Fraudehulpdesk en andere instanties. Deze versnippering maakt het moeilijk om een volledig beeld van het probleem te verkrijgen en snel en effectief te handelen.

Grenzeloosheid online criminaliteit (geografisch)

- Online criminaliteit is niet beperkt door gemeentegrenzen. Vanuit landen over de hele wereld kunnen cybercriminelen en fraudeurs opereren en daarbij ook Nederlandse burgers en organisaties ontwrichten. Dit maakt de opsporing van criminelen uitdagend en vraagt om een sterke samenwerking tussen partners.
- De digitale aard van deze criminaliteit zorgt ervoor dat slachtoffers, daders en relevante signalen zich vaak over meerdere gemeenten en regio's verspreiden. Hierdoor beschikt geen enkele gemeente zelfstandig over een volledig beeld van de problematiek. Effectieve preventie en bestrijding vragen daarom om regionale samenwerking, kennisdeling en gezamenlijke duiding van signalen en ontwikkelingen. Door samen op te trekken vergroten gemeenten hun informatiepositie, versterken zij elkaars aanpak en kunnen zij sneller inspelen op nieuwe dreigingen en fenomenen.

Kunstmatige Intelligentie als katalysator van online criminaliteit

- Kunstmatige Intelligentie (AI) verlaagt de drempel om digitale delicten te plegen, en verhoogt daarmee het tempo en de schaal van incidenten. Bestaande dreigingen zoals phishing, malware en online geweld worden sneller, goedkoper, toegankelijker en overtuigender uitgevoerd. Computertechnische vaardigheden zijn dan ook al lang niet meer vereist om online criminaliteit uit te voeren.
- Hoewel AI online criminaliteit niet fundamenteel verandert, zorgt het er wel voor dat bestaande fenomenen zich sneller ontwikkelen. Bij sextortion kunnen criminelen bijvoorbeeld gebruikmaken van AI om realistisch beeld- en videomateriaal te genereren, waardoor chantage geloofwaardiger wordt en de impact op slachtoffers verder toeneemt.
- Deze ontwikkelingen benadrukken het belang van digitale weerbaarheid, bewustwording en actuele kennis bij inwoners, ondernemers en professionals.

Hoog gehalte aan niet-geregistreerde criminaliteit

- In 2025 werden er ongeveer 2,5 miljoen Nederlanders slachtoffer van online criminaliteit. Tegelijkertijd is het "dark number", de hoeveelheid niet-geregistreerde criminaliteit, nog altijd hoog. In 2025 deed 15% van alle slachtoffers aangifte bij de politie. Deze lage hoeveelheid aan aangiftes maakt het lastig om een volledig beeld te krijgen van de aard, omvang en ontwikkeling van online criminaliteit. Het werkelijke probleem is daardoor waarschijnlijk aanzienlijk groter dan uit registraties blijkt.
- Dit vraagt om een sterke informatiepositie waarin politiecijsers worden gecombineerd met signalen van partners, maatschappelijke organisaties, ondernemers en inwoners. Alleen door deze informatie samen te brengen ontstaat een vollediger beeld van risico's, doelgroepen en ontwikkelingen.

Waar willen we naartoe?

Weerbaarheid vergroten inwoners

- We zetten in op het vergroten van de digitale weerbaarheid van inwoners en ondernemers. Het voorkomen van slachtofferschap staat daarbij centraal. We informeren inwoners en ondernemers actief over digitale risico's en bieden handelingsperspectief om deze risico's te herkennen en te verkleinen.
- Hierbij richten we ons op verschillende doelgroepen met een aanpak die aansluit op hun specifieke risico's en belevingswereld. Door in te spelen op actuele ontwikkelingen en veelvoorkomende fenomenen vergroten we de effectiviteit van preventieve interventies.

- Samen met maatschappelijke partners, onderwijsinstellingen, ondernemersnetwerken en andere betrokken organisaties versterken we de digitale weerbaarheid van onze gemeenschap. Door kennis, netwerken en capaciteit te bundelen kunnen risicogroepen eerder worden bereikt en bestaande initiatieven beter met elkaar worden verbonden.
- Met behulp van een sterke informatiepositie en een nauwe samenwerking met partners kunnen preventieve acties bovendien gericht worden ingezet via organisaties die dicht bij de doelgroep staan en beschikken over de juiste expertise en netwerken.

Slachtoffers van online criminaliteit krijgen ondersteuning en nazorg

- Slachtoffers van online criminaliteit moeten snel de juiste ondersteuning kunnen vinden. Schaamte, schuldgevoelens en onbekendheid met het beschikbare aanbod kunnen ervoor zorgen dat slachtoffers geen hulp zoeken of geen aangifte doen.
- Daarnaast bestaat er een breed landschap van initiatieven en organisaties, waardoor slachtoffers niet altijd weten waar zij terecht kunnen. Heldere hulproutes en goede doorverwijzing kunnen deze drempels verlagen en ervoor zorgen dat slachtoffers sneller passende ondersteuning ontvangen.
- We zetten daarom in op het versterken van de ondersteuning en nazorg voor slachtoffers. Hiermee beperken we niet alleen de impact van slachtofferschap, maar verkleinen we ook de kans op herhaald slachtofferschap. Mensen die eenmaal slachtoffer zijn geworden, lopen immers een verhoogd risico om opnieuw doelwit te worden.
- Ook professionals die in hun dagelijkse werkzaamheden in contact komen met inwoners spelen hierin een belangrijke rol. Door signalen van online criminaliteit tijdig te herkennen, kunnen zij slachtoffers ondersteunen, begeleiden naar passende hulp en waar nodig stimuleren om melding of aangifte te doen.

Extern samenwerken om online criminaliteit te bestrijden

- Digitale veiligheid vraagt om samenwerking. Geen enkele organisatie beschikt zelfstandig over alle informatie, expertise en bevoegdheden die nodig zijn om online criminaliteit effectief aan te pakken.
- Daarom werken we samen met politie, andere gemeenten, landelijke initiatieven, maatschappelijke organisaties, onderwijsinstellingen en private partners. Door kennis, signalen en ervaringen uit te wisselen vergroten we onze slagkracht en blijven we aangesloten op regionale en landelijke ontwikkelingen.
- Een gezamenlijke aanpak draagt bij aan een digitaal veilige samenleving waarin online criminaliteit wordt voorkomen, slachtoffers worden ondersteund en waar mogelijk daders worden aangepakt.
- Daarnaast zorgen korte communicatielijnen en duidelijke afspraken ervoor dat relevante informatie sneller op de juiste plek terechtkomt. Hierdoor kunnen partners sneller reageren op nieuwe ontwikkelingen en dreigingen.

Potentiële daders worden ontmoedigd

- Naast het voorkomen van slachtofferschap richten we ons ook op het voorkomen van daderschap. Vooral jongeren beschikken vaak over digitale vaardigheden die zowel positief als negatief kunnen worden ingezet.
- Door bewustwording te creëren over de gevolgen van online criminaliteit, het vergroten van normbesef en het bieden van positieve alternatieven, stimuleren we dat digitale talenten op een legale en maatschappelijk waardevolle manier worden ingezet.
- Samen met onderwijsinstellingen en andere partners besteden we aandacht aan de risico's en consequenties van online daderschap en versterken we beschermende factoren die bijdragen aan een positieve ontwikkeling van jongeren.

Hoe willen we dit bereiken?

Versterken informatiepositie

- Een sterke informatiepositie vormt de basis van een effectieve aanpak van online criminaliteit. We bouwen voort op bestaande samenwerkingsverbanden en brengen signalen, kennis en informatie van partners samen. Door ontwikkelingen, fenomenen en risico's gezamenlijk te monitoren en te duiden, ontstaat een beter beeld van de aard en omvang van online criminaliteit binnen onze gemeente en regio.

- Een versterkte informatiepositie stelt ons in staat om risico's eerder te signaleren, ontwikkelingen beter te begrijpen en gerichte maatregelen te treffen. Hierdoor kunnen partners gezamenlijk optreden om slachtofferschap te voorkomen, slachtoffers beter te ondersteunen en waar mogelijk daderschap tegen te gaan.
- Daarbij benutten we zowel kwantitatieve als kwalitatieve informatie. Beschikbare data, zoals politiecijfers, dashboards en landelijke onderzoeken, worden gecombineerd met signalen, casuïstiek en ervaringen vanuit het netwerk. Juist omdat online criminaliteit vaak ondergerapporteerd blijft, is het belangrijk om registraties aan te vullen met signalen van maatschappelijke organisaties, ondernemers, onderwijsinstellingen en inwoners. Op deze manier ontstaat een completer beeld van risico's, doelgroepen en lokale ontwikkelingen.

Domeinoverstijgende samenwerking

- Online criminaliteit raakt de hele gemeente. Daarom pakken we dit als een brede opgave op. Naast OOV betrekken we ook jeugd, onderwijs, het sociaal domein, economische zaken en burgerzaken bij de aanpak. Iedere afdeling vangt immers andere signalen op.

Door informatie, signalen en initiatieven met elkaar te verbinden, bereiken we concrete resultaten:

- We herkennen online criminaliteit en risico's in een vroeg stadium.
- We bereiken risicogroepen tijdig met preventie, waardoor minder mensen de stap naar daderschap zetten.
- We versterken de digitale weerbaarheid van onze inwoners en ondernemers.
- We herkennen slachtoffers sneller en zorgen dat ze meteen de juiste hulp krijgen.

Externe samenwerking

- Online criminaliteit houdt zich niet aan organisatie-, gemeente- of landsgrenzen. Geen enkele organisatie beschikt zelfstandig over voldoende informatie, expertise of bevoegdheden om het vraagstuk effectief aan te pakken. Daarom investeren we in een sterke samenwerking met veiligheidspartners, maatschappelijke organisaties, onderwijsinstellingen, ondernemers, regionale samenwerkingsverbanden, landelijke initiatieven en private partijen.
- Samenwerking stelt ons in staat om kennis en ervaringen te delen, signalen vroegtijdig te herkennen en interventies beter op elkaar af te stemmen. Door duidelijke afspraken te maken over rollen, verantwoordelijkheden en informatiedeling versterken we onze gezamenlijke aanpak.
- Vanuit deze samenwerking werken we aan een digitaal veilige samenleving waarin online criminaliteit zoveel mogelijk wordt voorkomen, slachtoffers passende ondersteuning ontvangen en daderschap wordt ontmoedigd. Door lokale, regionale en landelijke partners met elkaar te verbinden, vergroten we de effectiviteit en duurzaamheid van onze aanpak.