VeiligheidsAlliantie
regio Rotterdam

REGIONAAL Introductiedossier

Digitale veiligheid

'Samenwerken aan digitale veiligheid'

Versie 2026

Inleiding

De toenemende digitalisering van de samenleving maakt het voor kwaadwillende makkelijker om criminele delicten te plegen, zoal in de vorm van digitale criminaliteit en online norm-overschrijdend gedrag. Dit veroorzaakt aanzienlijke schade, variërend van economische verliezen tot bedreigingen voor de nationale veiligheid.

In 2024 waren er in Nederland bijna 2.4 miljoen slachtoffers van online criminaliteit (Meer mensen slachtoffer van online criminaliteit in 2024 | CBS). De impact op slachtoffers is groot. Mensen en bedrijven lijden financiële schade, maar het tast ook het vertrouwen in elkaar aan. En het beïnvloedt het vertrouwen in de digitale infrastructuur. De impact van slachtoffers van online fraude blijft niet beperkt tot financiële schade. Uit verschillende onderzoeken blijkt dat de impact van online criminaliteit niet onderdoet voor die van traditionele criminaliteit en in sommige opzichten zelfs groter is.

De afgelopen jaren werkten politie, Openbaar Ministerie, VeiligheidsAlliantie regio Rotterdam (VAR), gemeenten en het Platform Veilig Ondernemen (PVO) samen met publiek-private partijen aan een integrale aanpak veelvoorkomende gedigitaliseerde criminaliteit.
Vanuit het Regionaal Veiligheidsoverleg (RVO) is burgemeester Marco Oosterwijk regionaal portefeuillehouder op dit onderwerp. Hij wordt hiervoor ondersteunt vanuit de VAR.
De regionale portefeuille is onder te verdelen in vier subthema's:

1. Eigen huis op orde
2. Cybercrisis en cyberincidenten
3. Gedigitaliseerde criminaliteit
4. Online aangejaagde ordeverstoringen

Online aangejaagde ordeverstoringen valt onder de portefeuille Maatschappelijk Ongenoegen. Informatie hierover is terug te vinden in het introductiedossier Maatschappelijk Ongenoegen. Deze is te vinden op de kennisbank.

De VAR heeft een regionaal netwerk digitale veiligheid met diverse werkgroepen en organiseert jaarlijks diverse fysieke en digitale bijeenkomsten op uitéénlopende onderwerpen. Daarnaast houden we landelijke ontwikkelingen en *best practises* in de gaten, delen we interventies en praktische documenten op de kennisbank. Maandelijks verstuurt de VAR een nieuwsbrief waar o.a. het thema digitale veiligheid aan bod komt.

Rolverdeling

Gemeenten, OM, Politie en andere maatschappelijke organisaties hebben in de verschillende subthema's elk een eigen rol in preventie en repressie die bijdragen aan een integrale aanpak. Dat vraagt om een intensieve regionale samenwerking.

Brede bestrijding van cybercrime draait om opsporing en vervolging, maar ook om het tegenhouden van criminaliteit (verstoring), het beperken van schade en het voorkomen van dader- en slachtofferschap (preventie). Er zijn veel publieke en private partijen actief op het thema digitale veiligheid. De verantwoordelijkheid voor de opsporing en vervolging van strafbare feiten ligt bij de Politie en het OM. De burgemeester is verantwoordelijk voor de openbare orde en veiligheid. De gemeenten hebben een rol bij bewustwording en preventie en nazorg van slachtoffers.

Regionaal accounthouder Digitale Veiligheid VAR:
Dave van den Berg dj.vandenberg1@rotterdam.nl

Definities

Definitie gedigitaliseerde criminaliteit
Misdrijven waarbij criminelen ICT als middel inzetten om traditionele vormen van criminaliteit te plegen. Zoals bijvoorbeeld hulpvraag-fraude, aan-en verkoopfraude.

Definitie Cybercriminaliteit
Computercriminaliteit, cybercriminaliteit of cybercrime is criminaliteit met ICT als middel én doelwit. Zoals hacking, DDoS-aanvallen en ransomware.

Het Cybersecurity Woordenboek legt zo'n 780 cybersecurity termen uit in begrijpelijke taal.

Cijfermatig inzicht in digitale criminaliteit

Er zijn diverse middelen beschikbaar om inzicht te verkrijgen in de lokale en regionale cijfers rondom gedigitaliseerde criminaliteit en cybercriminaliteit.

- Lokale aangiftebeelden: Deze door de politie gegenereerde beelden bieden inzicht in slachtoffercategorieën binnen diverse vormen van online fraude. De politie adviseert deze cijfers lokaal op te vragen bij het basisteam van de betreffende gemeente.
- Gezamenlijk Veiligheidsbeeld - Veiligheidsalliantie Rotterdam: In opdracht van het Regionaal Veiligheidsoverleg (RVO) verschijnt deze monitor tweemaal per jaar. Het rapport bundelt cijfers van de politie, het OM, Veiligheidshuizen (Rotterdam-Rijnmond en Zuid-Holland-Zuid), het RIEC, Burgernet, Enver, Jeugdteams ZHZ en Halt. Om het jaar worden ook de cijfers van de landelijke VeiligheidsMonitor in de rapportage opgenomen.
- Zicht op Online Criminaliteit: Dit dashboard biedt analyses van zowel slachtoffers als daders. Hoewel het dashboard in november 2025 is gelanceerd, bevat het momenteel nog data tot en met 2023. Het doel is om deze gegevens via regelmatige updates structureel te actualiseren.

1. Eigen huis op orde

Rol gemeente

Gemeenten zijn verantwoordelijk voor het goed functioneren van de eigen digitale systemen (hardware en software) en digitale informatievoorzieningen, zodat de dienstverlening en bedrijfsvoering in goede orde verloopt en de beschikbare informatie bij de gemeente goed beveiligd is.

Deze taakvoering is belegd bij de Chief Information and Security Officer (CISO). De CISO houdt zich in het kader van informatiebeveiliging bezig met beleid en strategie, risico- en incidentbeheersing, bewustwording en training van medewerkers en compliance en audits. De VAR organiseert 4 keer per jaar een regionaal overleg voor alle CISO's. In dit regionale overleg bespreken zij actualiteiten, knelpunten en tips and tricks.

Inbedding in de organisatie

Het op orde krijgen van de informatiebeveiliging vraagt om een integrale aanpak binnen de organisatie. Alle medewerkers moeten zich bewust zijn van de risico's in de omgang met digitale systemen.

Daarnaast is de gehele bedrijfsvoering afhankelijk van goedwerkende digitale systemen. Om continuïteit te kunnen borgen is het noodzakelijk om de vitale processen per afdeling in kaart te brengen. Wanneer er bestuurlijk voldoende aandacht is voor het belang van dit onderwerp, klinkt dat door in de gehele organisatie.

Aanbod landelijke partners

- Handreiking verhogen bewustzijn informatiebeveiliging is een document opgesteld door de Informatiebeveiligingsdienst van de VNG. Dit document biedt gemeenten duidelijke handvatten voor een structurele aanpak van het verhogen van het bewustzijn binnen de organisatie.
- Handreiking incident- en responsemanagement geeft de CISO handvatten voor het inrichten van het proces rondom incident en responsemanagement.
- Handreiking Information Security Management (ISMS) is een nadere uitwerking, geschreven door de VNG, van wat er voor gemeenten zoodzakelijk is voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging conform BIO2.
- Handreiking Cybersecurity voor de bestuurder neemt de bestuurder mee in het beleggen van cybersecurity in de eigen organisatie met daarbij een checklist welke helpt de organisatie weerbaar te maken. De handreiking is geschreven door de cyber security raad.

Partners

- De Informatiebeveiligingsdienst (IBD) is een belangrijke partner in het op orde brengen van het eigen huis. Zij heeft op haar website een hele reeks documenten ter beschikking gesteld die ondersteuning kunnen bieden in het beveiligen van de eigen informatiehuishouding.

2. Cyberincidenten en cybercrisis

Definitie Cyberincident
Volgens de Wet- beveiliging netwerk- en informatiesystemen (Wbni) is een incident een gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

Definitie Cybercrisis
Een cybercrisis is een crisis die betrekking heeft op de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen met daaraan gerelateerde cascade- en gevolgeffecten in het fysieke domein/openbare orde en veiligheid.

Rol gemeente

Cyberincidenten en cybercrisis die ontstaan bij bedrijven, instellingen en belangrijke voorzieningen binnen de gemeentegrenzen, kunnen een impact hebben op de samenleving. Vaak kan het bedrijf of instelling het incident zelf oplossen, maar soms kan het ook zijn weerslag hebben op de lokale samenleving waardoor de gemeente betrokken raakt.

Met name als het om semipublieke voorzieningen (wegen, bruggen, sluizen, scholen, ziekenhuizen, culturele instellingen, verzorgingshuizen, etc.) gaat, zal de bevolking naar de gemeente en specifiek naar de burgemeester kijken. Goed voorbereide gemeenten weten hoe zij zelf (in de lokale driehoek) of samen met andere gemeenten en/of de Veiligheidsregio kunnen handelen om de cyberincidenten en -crisis beheersbaar te maken en af te wikkelen.

In deze context zijn er vaak verschillende functies die een rol bekleden in de voorbereiding en afhandeling van de crisis. In onderstaande tabel zijn die rollen beschreven.

Teams	Omschrijving	Aanspreekpunt
Gemeentelijk calamiteitenteam (of soortgelijke benaming)	Effectbestrijding en herstellen van een cyberincident of -crisis in het kader van de gemeentelijke bedrijfscontinuïteit.	**Ambtelijk**: CISO/ Gemeentesecretaris **Bestuurlijk**: portefeuillehouder ICT
Lokale driehoek	Bepalen inzet van opsporingsbevoegdheden en bestuurlijke noodbevoegdheden, gezamenlijk met officier van justitie en teamchef van politie.	**Ambtelijk**: Adviseur OOV/ crisisbeheersing **Bestuurlijk**: burgemeester
Gemeentelijk Beleidsteam (GBT)	Bestuurlijke advisering over (nood) bevoegdheden, strategische besluiten in het kader van openbare orde en veiligheid, bijstandsaanvragen, afwegen maatschappelijke impact, bestuurlijke afstemming (externe) partijen, scenariodenken en het bepalen van de communicatiestrategie.	**Ambtelijk**: Adviseur crisisbeheersing **Bestuurlijk**: burgemeester

Inbedding in de organisatie

Cyberincidenten en -crises kunnen grote gevolgen hebben voor de continuïteit van gemeentelijke processen en zelfs impact hebben op de openbare orde en veiligheid. Daarom is het essentieel dat de organisatie deze dreiging omarmt. Dit begint met het integreren van cybercrisismanagement in de

bestaande crisisplannen. Het is daarbij belangrijk dat het huidige crisisteam wordt uitgebreid zodat deze ook beschikt over kennis en procedures om adequaat te handelen bij cyberaanvallen, datalekken of verstoringen van vitale systemen.

Aanbod

- Handreiking hulp bij digitale ontwrichting legt per fase van een cybercrisis of incident uit welke afwegingen er moeten worden gemaakt en door wie. De handreiking is geschreven door de VNG en bedoeld voor adviseurs crisisbeheersing van gemeenten en bestuurders.
- Handreiking bestuurlijke bevoegdheden cyber van het Nederlands Instituut Publieke Veiligheid (NIPV) is een verkenning naar bevoegdheden en interventiemogelijkheden van burgemeesters bij (dreigende) digitale incidenten;
- Handreiking: cybergevolgbestrijding (koude fase) focust op de gevolgbestrijding van een cybercrisis. Dit betekent dat in kaart wordt gebracht op welke manier cybergevolgbestrijding afwijkt van gevolgbestrijding bij rampen en crises zoals beschreven in het crisisplan van de veiligheidsregio's of het Continuïteitsplan van de G4-gemeenten. Deze handreiking is geschreven door Berenschot.
- Handreiking cybergevolgbestrijding (warme fase) is bedoeld om tijdens een digitale verstoring snel inzicht te krijgen in de verstoring en het mogelijk maatschappelijk effect daarvan. Deze handreiking is geschreven door Berenschot.
- De IBD biedt een cyberoefenpakket aan. Met dit oefenpakket kan uw gemeente en desgewenst in aansluiting met partners zelfstandig een interactieve cyberoefening organiseren en uitvoeren.

Partners:

- De **IBD** is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).
- De Veiligheidsregio komt in actie wanneer een digitale verstoring ernstige fysieke gevolgen heeft. De eenheid Rotterdam bestaat uit twee veiligheidsregio's. Rotterdam-Rijnmond en Zuid-Holland Zuid.
- Politie is betrokken in het kader van opsporing en vervolging. Zo kunnen digitale rechercheurs proberen digitale sporen veilig te stellen. Ook kan politie helpen bij de duiding van de dreiging/crisis.

3. Gedigitaliseerde criminaliteit

Rol gemeente

Gemeenten dienen de samenleving weerbaar te maken tegen cybercrime en gedigitaliseerde criminaliteit. Om dit te realiseren kan zij verschillende doelgroepen, zoals jeugd, MKB en senioren benaderen om preventieve interventies in te zetten. Omdat criminaliteitsvormen continue veranderen moeten inwoners blijvend worden voorgelicht over de gevaren.

Inbedding in de organisatie

Digitalisering is niet alleen iets van de afdeling veiligheid. De preventieve aanpak om inwoners weerbaar te maken tegen de uitéénlopende vormen van gedigitaliseerde criminaliteit (zoals sextortion, online pesten en online fraude) vereist een organisatiebrede benadering. Het is daarom goed om in de staande organisatie te onderzoeken op welke wijze digitale veiligheid kan worden meegenomen in de verschillende portefeuilles.

Ervaring leert dat het soms lastig is om de doelgroep te benaderen. Daarom is het aan te raden om gebruik te maken van de al bestaande netwerken in de organisatie. Kijk bijvoorbeeld naar bestaande contacten vanuit de afdeling sociaal domein en kijk hoe je samen het onderwerp aan de man kan brengen.

Aanbod

Er zijn in de afgelopen jaren veel interventies ontwikkeld op het gebied van gedigitaliseerde criminaliteit en cybercrime. Onderstaand hebben we een selectie gemaakt van een aantal interventies per doelgroep.

Let op! Dit is niet alomvattend en wellicht zijn er interventies die beter aansluiten op jouw lokale situatie. Een uitgebreider overzicht vind je terug in de database van het CCV.

Wij adviseren om als gemeente aan te sluiten tijdens landelijke campagnes van de Rijksoverheid en actief mee te doen tijdens de Cybersecuritymaand oktober.

Jeugd

- Hackshield is een cybersecurity game voor kinderen tussen de 8 en 12 jaar. Op een speelse manier leren kinderen zich wapenen tegen digitale ervaringen. Kinderen worden dan Junior Cyber Agent en worden gestimuleerd het geleerde ook over te brengen op hun (groot)ouders.
- Mijn cyberrijbewijs is een gratis lesprogramma dat bijdraagt aan de digitale weerbaarheid van leerlingen uit groep 7 en 8 van het primair onderwijs. Aan de hand van illustrerende thema's zoals online hate speech, online fraude, doxing, hacking en sexting leren en ervaren kinderen meer over online slachtoffer- en daderschap. Van kennis, via inzicht naar gedrag met handelingsperspectief.
- De interactieve film LVB is een interventie gericht op mensen met een licht verstandelijke beperking. Met behulp van deze interventie kan het gesprek worden aangegaan over geldezels, cyberpesten en online seksueel geweld. De film wordt in Q1 2026 gepubliceerd en zal beschikbaar worden gesteld via de website van het CCV.
- ReB00tCMP is een interventie gericht op jongeren met IT-vaardigheden die de neiging hebben om online de grens op te zoeken. Deze jongeren worden geworven door middel van een online campagne en gastlessen op het voortgezet onderwijs: mbo, hbo en wo. Als de jongere voldoet aan de vooraf bepaalde score, kan de jongere een uitnodiging verwachten voor de re_B00TCMP. Dit is een event van een dag dat wordt georganiseerd op een aansprekende locatie met een programma voor zowel de jongeren als hun ouders/verzorgers.

Gastsprekers zijn onder andere politiefunctionarissen, specialisten uit de cybersecurity- en gaming industrie, ervaringsdeskundigen en ethical hackers. Het event wordt afgesloten met een hackchallenge waarmee prijzen te winnen zijn.

Senioren

- De interactieve film Echt of nep is een interventie, waarmee gemeenten via ouderenwerk, politie, bibliotheken, enzovoort, het gesprek aan kunnen gaan met senioren over veilig internetgebruik. In de film zitten keuzemogelijkheden waarbij de film wordt stopgezet en aan de senioren wordt gevraagd wat zij in deze situatie zouden doen.
  De film gaat daarna verder met de keuze die gemaakt is. Door te ervaren wat er gebeurt als er een verkeerde keuze wordt gemaakt, blijft de opgedane kennis beter hangen. Onderwerpen die aan bod komen zijn:
  - WhatsApp fraude
  - Phishing
  - Bankhelpdeskfraude
  - Spoofing
  - Aan- en verkoopfraude
  - Relationele beleggingsfraude
  - Stemnabootsing
  - Datingfraude
- E-learning 'Storytelling tegen digitale oplichting' is een training voor professionals die met de doelgroep senioren werken. In de E-learning leren deelnemers hoe ze verhalen kunnen gebruiken om ouderen bewuster en weerbaarder te maken tegen digitale criminaliteit. In de training leren deelnemers wat een goed verhaal maakt, hoe ze hun eigen persoonlijke verhaal over (digitale) oplichting kunnen vormgeven en hoe ze dit kunnen inzetten om het gesprek aan te gaan met ouderen over veilig internetgebruik.
- Serious game cyberweerbaarheid laaggeletterden is een fysiek bordspel voor senioren. In dit fysieke spel komt onder andere naar voren hoe je controleert of een website betrouwbaar is en welke persoons- (of bank)gegevens je wel of niet kunt delen. Senioren zullen eerder geneigd zijn om een fysiek bordspel te spelen dan op de computer te oefenen. Een vrijwilliger speelt als spelbegeleider het spel in een taalhuis, bibliotheek of in een andere organisatie in het sociaal domein. De veilige omgeving van een fysieke game, zonder online component geeft de doelgroep de rust en daarmee de tijd om de situatie te begrijpen en vervolgens goede beslissingen te kunnen maken.

MKB

Voor interventies voor de doelgroep MKB verwijzen we graag naar het Platform Veilig Ondernemen (PVO).

Partners

Het is onmogelijk om de aanpak van gedigitaliseerde criminaliteit geheel zelf te verzorgen. Samenwerking met publieke en private partners is van essentieel belang. Een goed voorbeeld van hoe je een samenwerking vorm kan geven is het Rotterdam Protected model. In dit samenwerkingsverband werken diverse partijen met elkaar aan het verhogen van de cyberweerbaarheid van inwoners. Onderstaand een aantal van die partners geschetst.

- Scholen
- Jeugdwerk
- Sportverenigingen
- Politie
- OM
- Cybersecurity bedrijven
- Algemene Nederlandse Bond voor Ouderen
- SeniorWeb

- KBO-PCOB
- Kerken
- Politie
- Bibliotheken
- Banken
- Telecomproviders
- Interne teams (die bijvoorbeeld goed in contact staan met de doelgroepen)

Voor partners in het MKB verwijzen we je graag door naar het Platform Veilig Ondernemen.

4. Online aangejaagde ordeverstoringen

Online aangejaagde ordeverstoringen wordt binnen de VAR opgepakt vanuit de portefeuilles maatschappelijk ongenoegen en digitale veiligheid. Alles wat je moet weten om je goed voor te bereiden op online aangejaagde ordeverstoringen is terug te vinden in het introductiedossier maatschappelijk ongenoegen. Deze is terug te vinden op de kennisbank.