Actieprogramma

Veilig Ondernemen 2023 t/m 2026

Nationaal Platform Criminaliteitsbeheersing (NPC)

Inleiding

Binnen het Actieprogramma Veilig Ondernemen 2019-2022 van het Nationaal Platform Criminaliteitsbeheersing (NPC) is de afgelopen vier jaar door overheid en bedrijfsleven intensief samengewerkt om criminaliteit te voorkomen en terug te dringen. Het NPC[1] stimuleert deze publiek-private samenwerking op nationaal, regionaal en lokaal niveau. Daarbij ligt de focus op de aanpak van criminaliteit *tegen* het bedrijfsleven en het (on)bewust *faciliteren* van criminaliteit door het bedrijfsleven. Het NPC doet dat door criminaliteitsvraagstukken te agenderen die het bedrijfsleven raken en gezamenlijk aan de slag te gaan met passende interventies en mogelijke oplossingen.

Om deze publiek-private aanpak verder te brengen presenteert het NPC dit Actieprogramma Veilig Ondernemen 2023-2026. Dit actieprogramma schetst de geprioriteerde thema's voor de publiek-private aanpak van de komende jaren en biedt concrete maatregelen waar overheid en bedrijfsleven gezamenlijk mee aan de slag gaan. Naast het actieprogramma lopen nog tal andere samenwerkingsvormen, pilots en initiatieven om criminaliteit tegen te gaan en waarbij publiek- private samenwerking van essentieel belang is. Dit actieprogramma moet in samenhang met de andere initiatieven gelezen worden en deze dienen complementair aan elkaar te zijn.

Het Actieprogramma Veilig Ondernemen 2023-2026 is tot stand gekomen door het actief ophalen van ervaringen, behoeften en voorstellen vanuit zowel de publieke als de private sector. Tijdens het Ondernemersdiner 2022 zijn de minister van Justitie en Veiligheid en de minister voor Rechtsbescherming samen met hun topambtenaren in gesprek gegaan met de top van het Nederlandse bedrijfsleven. Het congres *Eén front tegen criminaliteit*, waar publiek-private samenwerking tegen criminaliteit centraal stond, inspireerde en gaf deelnemers de mogelijkheid met elkaar in gesprek te gaan. Op die manier werden ook ideeën opgehaald voor de toekomstige gezamenlijke aanpak.

In opdracht van het NPC heeft Bureau Beke het onderzoek *Samen criminaliteit bestrijden* uitgevoerd, een belangrijke bouwsteen voor dit actieprogramma. Bijna 300 ondernemers zijn in dit onderzoek gevraagd naar de vormen van criminaliteit waar zij mee geconfronteerd worden. Met een deskresearch en panelgesprekken met stakeholders is een compleet en actueel overzicht gemaakt van de criminaliteitsvormen die het bedrijfsleven het meest raken.

De betrokkenheid van tal van publieke en private partijen, alsook de wetenschap, zorgt dat dit actieprogramma zich richt op de actuele veiligheidsopgaves en dat het kan rekenen op breed draagvlak van de publiek-private partners. Er komen enkele thema's naar voren waar de afgelopen jaren al op is ingezet, maar ook nieuwe vraagstukken komen aan bod.

1 In het NPC zijn - onder voorzitterschap van de minister van Justitie en Veiligheid - vertegenwoordigd: VNO-NCW en MKB-Nederland, Transport en Logistiek Nederland, BOVAG, Koninklijke Horeca Nederland, Raad Nederlandse Detailhandel, Nederlandse Vereniging van Banken, Verbond van Verzekeraars, politie, Openbaar Ministerie, Vereniging Nederlandse Gemeenten en het ministerie van Economische Zaken en Klimaat.

Foto: Martijn Beekman

In dit Actieprogramma Veilig Ondernemen 2023-2026 zijn de volgende thema's opgenomen:

- **Aanpak preventie cybercrime voor het bedrijfsleven:** ondernemers krijgen steeds vaker te maken met cybercrime. Eén op de vijf ondernemers heeft jaarlijks met een cyberaanval te maken. In coronatijd heeft cybercrime een verdere vlucht genomen: tussen 2019 en 2021 is een toename van 200% zichtbaar wat betreft cybercrime gerelateerde incidenten. Daarnaast groeit de afhankelijkheid van IT bij ondernemers alsmaar verder. De private sector en deskundigen noemen cybersecurity dan ook als prioriteit en het blijft de komende jaren van groot belang om op dit thema in te zetten bij de gezamenlijke aanpak. Grotere ondernemingen dan wel ondernemers die behoren tot de zogenaamde 'vitale sectoren' lijken het meest weerbaar tegen cybercriminaliteit. Zij hebben een belangrijke voortrekkersrol om het minder weerbare MKB mee te nemen in de broodnodige preventieve stappen.

- **Aanpak georganiseerde ondermijnende criminaliteit:** ondermijning kenmerkt zich door een verwevenheid tussen onder- en bovenwereld. Voorbeelden zijn intimidatie, afpersing, het witwassen van geld in de horeca, drugscriminaliteit en opslag en vervoer van andere goederen, personen of geld. Ook hier heeft de coronatijd – maar ook de stijgende energiekosten – ondernemers kwetsbaarder gemaakt voor criminelen door groeiende financiële zorgen. Georganiseerde, ondermijnende criminaliteit zorgt in bedrijfstakken voor forse economische, fysieke en psychische schade en bemoeilijkt ondernemerschap. Het tast het vestigings- en investeringsklimaat in Nederland aan. Deze combinatie van factoren maakt dat ondernemers dit onderwerp opnieuw als prioriteit beschouwen.

- **Gebiedsgerichte aanpak (vermogens)criminaliteit:** gesprekken met private partijen tonen aan dat er sterke behoefte is om criminaliteitsproblemen beter inzichtelijk te maken en de afstand tussen de ondernemer en de overheid te verkleinen. Om de veiligheid van het bedrijfsleven te waarborgen en de uitdagingen waar zij voor staat het hoofd te bieden, is de gebiedsgerichte aanpak van (vermogens)criminaliteit de komende jaren een belangrijk thema voor de publiek-private partners. Onderwerpen als diefstal en agressie kwamen ook in het onderzoek onder ondernemers prominent naar voren en vinden in dit actieprogramma een plaats.

Bij de uitwerking van bovenstaande inhoudelijke thema's is speciaal aandacht besteed aan een aantal strategische invalshoeken, die als rode draad door het actieprogramma lopen: wederkerigheid, innovatieve oplossingen, informatie- en gegevensdeling, onderlinge verbanden tussen de thema's, branchegerichte aanpak en enerzijds kansen voor pilots en anderzijds borging van initiatieven.

Het overgrote deel van de acties in dit programma is preventief van aard. De acties richten zich op het versterken van de weerbaarheid tegen criminaliteit om zo slachtofferschap, schade en ongewilde facilitering van criminaliteit te voorkomen. Preventie en repressie gaan echter nadrukkelijk hand in hand. De acties uit het actieprogramma sluiten onder andere aan bij de prioriteiten uit de Veiligheidsagenda[2]. De Veiligheidsagenda 2023 t/m 2026 beschrijft de inzet van politie en Openbaar Ministerie op onder meer cybercrime en georganiseerde ondermijnende criminaliteit. De agenda's in samenhang beziend wordt zowel preventief als repressief opgetreden. Daarnaast wordt onder diverse acties in het programma op operationeel niveau samengewerkt waarbij preventie en repressie elkaar versterken. Ook zijn de publieke en private partijen belangrijke partners in de integrale samenwerking op lokaal niveau, onder meer via de Platforms Veilig Ondernemen. De politie zet daarnaast in op een fenomeengerichte aanpak. Hierbij wordt gekeken naar alle interventies die er beschikbaar zijn om slachtofferschap en daderschap te voorkomen en criminele activiteiten te verstoren. Bij deze aanpak wordt gewerkt volgens het barrièremodel, crimescript of soortgelijke modellen om inzicht te verkrijgen in het criminele proces en hier barrières op te werpen. Deze barrières kunnen bestaan uit preventieve maatregelen die door overheid of ondernemers genomen kunnen worden of op interventies vanuit de overheid waarbij belangrijke actoren van een crimineel proces tegengehouden of ontmoedigd worden. Daarbij is de politie één van de partners, maar hebben ook andere publieke en private partners een belangrijke rol.

Daarnaast schetst dit actieprogramma de inzet op de doorontwikkeling van de **Platforms Veilig Ondernemen** en de **aanpak fraude**. Het programma sluit af met een hoofdstuk over **governance, monitoring en middelen**. In de bijlagen zijn de resultaten van het vorige actieprogramma opgenomen en de acties van het nieuwe programma kort op een rij gezet.

Het uitgangspunt is dat de genoemde thema's en acties in dit programma voor focus en samenhang zorgen zonder de benodigde flexibiliteit te verliezen. We hanteren een lerende en adaptieve werkwijze.

2 Volgend uit artikel 18 van de Politiewet 2012 stelt de minister, gehoord het College van Procureurs-Generaal en de regioburgemeesters, ten minste eenmaal in de vier jaar de landelijke beleidsdoelstellingen vast ten aanzien van de taakuitvoering van de politie.

Foto: Rutger Rog

Aanpak preventie cybercrime voor het bedrijfsleven

Sinds 1991 is Bert[3] trotse eigenaar van een drogisterij. De drogisterij is goed beveiligd tegen cybercrime. Tenminste, dat dacht hij. Op de een of andere manier hadden cybercriminelen toegang gekregen tot de pc van Bert en alle bestanden versleuteld. De criminelen eisten vele Bitcoins om de boel te ontgrendelen. Op de pc draaide onder andere het kassasysteem en het voorraadbeheer.

Bert besloot het losgeld niet te betalen: "Ik werk keihard voor m'n centen, ik gun het ze niet. En straks betaal ik wel, en komen ze later weer terug. Of ik betaal, en dan ontgrendelen ze m'n bestanden toch niet". Gevolg was wel dat Bert al zijn bedrijfsbestanden en het vertrouwen van zijn klanten kwijt was: "Mensen gaan ergens anders iets kopen als je winkel dicht is. Het plezier in het werk gaat eruit".

Steeds meer bedrijven krijgen te maken met cybercrime. De gevaren van phishing, ransomware of computervirussen zijn bekend bij ondernemers. Desalniettemin worden er dagelijks bedrijven slachtoffer van bekende en minder bekende vormen van cybercrime. Deze vorm van criminaliteit is gevaarlijk, richt schade aan en werkt enorm ontwrichtend. Waar digitalisering en automatisering ons als samenleving veel bieden, kent de toenemende afhankelijkheid van digitale infrastructuur ook nadelen en kwetsbaarheden. Cybercrime legt die kwetsbaarheid soms pijnlijk bloot.

De afgelopen jaren zijn verschillende activiteiten ondernomen om de cyberweerbaarheid van ondernemers - vooral in het midden- en kleinbedrijf (mkb) - te vergroten. De eerste jaren is, onder andere met bijeenkomsten en congressen, ingezet op bewustwording bij ondernemers. In 2020 is gestart met de City Deal "Lokale weerbaarheid Cybercrime" waarbij ingezet wordt op het stimuleren van gedragsverandering door ondernemers meer handelingsperspectief te bieden via betrouwbare lokale en regionale kanalen. Er zijn mooie resultaten geboekt, maar de problematiek is hier niet mee opgelost.

Nog steeds wanen veel ondernemers zich ten onrechte veilig, omdat ze denken dat bij hen betrekkelijk weinig te halen valt. Tegelijkertijd neemt de bedreiging van cybercrime de afgelopen jaren alleen maar toe. In het Cybersecuritybeeld Nederland (2022) wordt opnieuw aangegeven dat bedrijven veel te vrezen hebben van cybercrime en in het bijzonder van ransomware en cyberaanvallen op leverancierssketens. Ondanks de risico's slaan ondernemers nog onvoldoende acht op het nemen van (basale) veiligheidsmaatregelen[4].

Wat willen we bereiken met publiek-private samenwerking ter preventie van cybercrime in het (niet-vitale) bedrijfsleven?

Cyberweerbaarheid is en blijft in de basis een verantwoordelijkheid van de ondernemer zelf. Overheid en private partijen, zoals de brancheverenigingen, hebben een gezamenlijke rol in het faciliteren van ondernemers door:

1. Bewustwording vergroten door voorlichting te geven over de risico's en gevaren van cybercrime;

3 Dit is een fictieve naam.

4 Cybersecurity monitor 2021, CBS.

2. Gedragsverandering te stimuleren door ondernemers te voorzien van (begrijpelijke en eenvoudige) informatie en instrumenten om deze risico's af te wegen en de nodige maatregelen (zoals het toepassen van de vijf basisprincipes[5] van het DTC) te treffen.

Om het Nederlandse ondernemersklimaat digitaal veiliger te maken en de ondernemer hulp van een betrouwbare partner en "dicht bij huis" te bieden, blijft publiek-private samenwerking de komende jaren essentieel. De focus in de aanpak ligt bij het mkb. Daarnaast is er aandacht voor het bredere (niet-vitale) bedrijfsleven[6]. De vitale infrastructuur krijgt al bijzondere aandacht voor de digitale veiligheid.

Hoe gaan we dat bereiken?[7]

Door het Digital Trust Center[8], als landelijk aanspreekpunt, breder onder de aandacht te brengen en informatie en instrumenten via een betrouwbare partner en "dicht bij huis" aan de ondernemer aan te bieden. Ondernemers hebben behoefte aan eenvoudige, begrijpelijke, niet-tijdrovende en betaalbare ondersteuning van betrouwbare en bekende partners. Lokale en regionale samenwerkingsverbanden, zoals gemeenten, de Platforms Veilig Ondernemen en brancheorganisaties spelen hier een belangrijke rol in.

Voor de verdere uitwerking wordt ook het verband gelegd met de Nederlandse Cyber Securitystrategie en de Veiligheidsagenda 2023 t/m 2026 waarin afspraken worden gemaakt over opsporing en vervolging en interventies zoals voorkomen en verstoren.

Acties

Voorlichtingsactiviteiten Digital Trust Center (1)

De komende jaren wordt dit thema sterker onder de aandacht gebracht. Dit doet het DTC bijvoorbeeld met een campagne over phishing. Het DTC gaat activiteiten ondernemen om het aantal bezoekers op de website te verhogen en het aanbod van instrumenten die de ondernemer helpen passende maatregelen te nemen voor cyberveiligheid uitbreiden. Daarnaast gaat het DTC het informeren van individuele bedrijven over concrete dreigingsinformatie via de daartoe ingerichte informatiedienst opschalen.

Meest betrokken partij: EZK/DTC.

Stimuleren gedragsverandering via samenwerkingsverbanden (2)

Om de ondernemer hulp van een betrouwbare partner en "dicht bij huis" te bieden werken lokale, regionale en sectorale partners samen om ondernemers te faciliteren. Onderstaande samenwerkingsverbanden illustreren dit.

- *Nationaal: Brancheorganisaties*
  Het platform Samen Digitaal Veilig, van VNO-NCW en MKB-Nederland, is een praktische tool gebaseerd op de vijf basisprincipes van het DTC om (veelal mkb-) bedrijven en medewerkers op te leiden in digitale veiligheid. Kennis en bewustwording bij medewerkers is cruciaal in de strijd tegen cybercrime. Medewerkers worden getraind via korte opleidingsvideo's en vragen. Via een automatische uitvraag ziet de ondernemer of zijn IT-leverancier de zaken goed heeft geregeld. BOVAG is betrokken geweest bij de ontwikkeling en de eerste branche die het platform onder haar leden uitrolt. Het uiteindelijke streven is om, na een gedragsonderzoek, de tool te verspreiden onder 100+ participerende branchevereniging. Via het samenwerkingsverband van de brancheorganisaties wordt beoogd de branches een effectief middel te bieden om de bewustwording en kennis van leden te vergroten.

Meest betrokken partijen: VNO-NCW en MKB-Nederland, BOVAG.

- *Lokaal en regionaal: Gemeenten en Platforms Veilig Ondernemen*
  Voortbouwend op de eerste positieve resultaten van lokale en regionale pilots onder de vlag van de City Deal "Lokale weerbaarheid cybercrime" zijn nieuwe, innovatieve mkb-pilots gestart met als doel om naast bewustwording, ondernemers laagdrempelige instrumenten en informatie te bieden om hun weerbaarheid te vergroten. Bijvoorbeeld door het versterken van de keten: de keten is zo sterk als de zwakste schakel. Er wordt, naar het voorbeeld van de Circle of trust (ASML) waarbij groot klein helpt, een methodiek ontwikkeld waarbij de grote bedrijven de kleinere toeleveranciers ondersteunen bij het opschroeven van de informatiebeveiliging. Daar plukken de individuele bedrijven – en daarmee de gehele keten – de vruchten van.

Daarnaast wordt het Keurmerk Veilig Ondernemen Bedrijventerrein (KVO-B) uitgebreid: het cybersecurityniveau meetbaar maken op bedrijfsniveau en hierover naar betrokken bedrijven terugkoppelen.

In samenwerking met het DTC zullen ondernemers verder worden gestimuleerd om passende basismaatregelen voor hun eigen situatie te nemen: een interventie die gericht is op drie van de vijf basisprincipes van veilig digitaal ondernemen (inventariseer kwetsbaarheden, voer updates uit en voorkom malware). Onderdeel

5 Inventariseer kwetsbaarheden, kies veilige instellingen, voer updates uit, beperk toegang en voorkom virussen en andere malware.

6 Alle bedrijven (van zzp tot grootbedrijf) in Nederland die tot de niet-vitale sectoren behoren. Vitale sectoren zijn bijvoorbeeld banken, telecom-, energie- en waterbedrijven.

7 Zie ook Kamerstuk 26643 nr. 907.

8 Het DTC wordt geïntegreerd met het NCSC en CSIRT-DSP, zie ook de Nederlandse Cybersecuritystrategie, Kamerstuk 26643 nr. 925.

van de interventie is het aanbieden van een handelingsperspectief voor deze drie maatregelen.

De pilots binnen de City Deal worden geëvalueerd en beoordeeld op effectiviteit. Succesvolle en effectieve pilots worden landelijk opgeschaald en verspreid via gemeenten, Platforms Veilig Ondernemen en regionale samenwerkingsverbanden Openbare Orde en Veiligheid. Daarmee wordt nadrukkelijk de aansluiting gevonden met een van de strategische invalshoeken binnen dit actieprogramma; de borging van initiatieven.

Gemeenten en regio's bieden hiermee handvatten om ondernemers met concrete instrumenten bij te staan om de cyberweerbaarheid te verhogen. Gemeenten kunnen dit benutten om op termijn de preventie van cybercriminaliteit gericht tegen ondernemers op te nemen in de Integrale Veiligheidsplannen, die iedere gemeente verplicht dient op te stellen. Daarmee wordt het versterken van de mkb-weerbaarheid cybercrime een vast onderdeel van de lokale activiteiten.

Meest betrokken partijen: JenV, BZK, EZK/DTC, VNG en het CCV.

Cyberweerbaarheidsnetwerken (3)

Het DTC zet in op het opzetten en/of versterken van regionale en branchegerichte samenwerkingsverbanden. In een cyberweerbaarheidsnetwerk werken ondernemers samen met andere organisaties aan het vergroten van de cyberweerbaarheid, binnen en tussen niet-vitale branches, sectoren en regio's. Voorbeelden hiervan zijn de samenwerkingsverbanden FERM (haven Rotterdam) en Brainport (technologiesector).

De komende jaren wordt netwerkvorming van deze samenwerkingsverbanden, in (niet-vitale) sectoren, verder gestimuleerd. Op dit moment zijn er 45 samenwerkingsverbanden bij het DTC aangesloten. Het streven is om dit in 2023 te versterken naar 50 samenwerkingsverbanden. Daarnaast wordt er o.a. intensief samengewerkt met de Kamer van Koophandel – vanwege hun grote bereik bij ondernemers - om via hun kanalen ondernemers te bereiken en te helpen bij het vergroten van hun cyberweerbaarheid.

Doelstelling is het toewerken naar een ecosysteem van cybersecurity-samenwerkingsverbanden tussen branches, sectoren en regio's om de samenwerking in de keten te versterken, "groot-helpt-klein" te stimuleren en synergie te zoeken tussen de verschillende samenwerkingsverbanden.

Meest betrokken partij: EZK/DTC

Verkenning aanvullende acties (4)

Naast voornoemde (lopende) activiteiten zullen aanvullende activiteiten worden verkend. Deze aanvullende activiteiten sluiten aan bij de behoeften van ondernemers en publieke en private partijen, te denken valt aan:

- Handelingsperspectief voor ondernemers nadat zij slachtoffer zijn geworden van cybercrime (respons).
- Normstelling door middel van zelfregulering, bijvoorbeeld via de brancheorganisatie, verzekeraar, keten of "groot-helpt-klein".
- Een agenda voor cyberoefeningen specifiek gericht op niet-vitale bedrijven.
- Stimuleren van aangiftes bij politie.
- Verkennen van een fenomeengerichte aanpak door politie.
- Nader onderzoek naar aard en omvang van cybercrime tegen ondernemers.
- Een blauwdruk voor ketensamenwerking.
- Stimuleren toepassing risicoklasseindeling Digitale Veiligheid.

Meest betrokken partijen: JenV, politie, EZK/DTC, VNO-NCW en MKB-Nederland.

Foto: Bart Maat

Aanpak georganiseerde ondermijnende criminaliteit

Babs[9] werkt al veertien jaar met veel plezier als chauffeur bij hetzelfde transportbedrijf. Op een dinsdag vertrekt zij uit de Rotterdamse haven, nadat zij daar een zeecontainer bij de containerterminal heeft opgehaald. Na vertrek uit de haven wordt ze klemgereden door een auto. Er komt een duo uit de auto. Een van de personen houdt haar onder schot, terwijl de handlanger de container open maakt en er een aantal sporttassen uit haalt. Ze rijden weg, maar het incident blijft Babs nog langere tijd achtervolgen in haar gedachten.

Hoe wisten de criminelen überhaupt welke vrachtwagen te stoppen? Ook daarvoor hebben zij hun criminele tactieken moeten inzetten. Zo kan het zijn dat zij hun informatie hebben gekregen door de transportplanner van het bedrijf, Dylan, te dwingen de informatie op te geven. Als Dylan bij een wegrestaurant op zijn bestelling staat te wachten wordt hij vriendelijk aangesproken door een onbekende die vertelt dat hij wat van hem nodig heeft. Als Dylan aangeeft dat hij de onbekende niet kent en niet wil helpen, wordt de onbekende opeens een stuk minder vriendelijk. Als Dylan naar huis loopt staat wordt hij opgewacht. De onbekende vertelt te weten waar hij woont, waar zijn kinderen naar school gaan en waar zijn partner werkt. Zo wordt Dylan gedwongen om toch de informatie op te geven.

Ook uit andere branches zijn voorbeelden van kwetsbaarheden voor criminele inmenging. Laura heeft een aantal jaar geleden haar fulltime baan opgezegd om een café te starten. Het café liep goed totdat er maatregelen worden ingesteld om corona te bestrijden. De coronatijd is voorbij, maar het blijft lastig met stijgende energieprijzen, het terugbetalen van de overheidssteun en tegenvallende omzet door personeelstekorten. Een van de stamgasten biedt Laura aan tijdelijk te steunen met wat cash geld zodat zij rond kan komen. De gast komt al vanaf het begin naar het café en is altijd aardig, dus Laura vindt het lastig om nee te zeggen. Al snel blijkt echter dat het niet zonder gevolgen is, want deze foute 'investeerder' krijgt steeds meer grip op Laura en de bedrijfsvoering van haar café, door haar te bedreigen en af te persen. Wat als een gezonde onderneming met veel enthousiasme werd opgezet eindigt als dekmantel voor criminele praktijken, met veel zorgen voor de bonafide eigenaar.

Criminelen misbruiken voor hun activiteiten (deels) de reguliere bedrijfsprocessen van bonafide ondernemers. Ook kunnen zij zich als bonafide ondernemer voordoen zodat zij een dekmantel hebben voor hun criminele activiteiten. Zij hebben immers een plek nodig om hun criminele activiteiten te ontplooien en onder de radar te blijven, moeten zij hun product kunnen verplaatsen en moeten zij de opbrengsten van hun criminele activiteiten kunnen witwassen. Er zijn drie manieren onderkend waarop een bonafide ondernemer met criminele inmenging te maken kan krijgen[10].

1. Een bonafide ondernemer kan criminaliteit onbewust faciliteren door hun product of dienst aan de crimineel te verkopen, zonder er weet van te hebben dat de ondernemer te maken heeft met een crimineel;
2. Criminele organisaties kunnen soms heimelijk en onrechtmatig gebruik maken van de bedrijfsprocessen zonder dat het bedrijf dat bemerkt of daar zelf van profiteert;
3. Criminele organisaties kunnen met voorbedachten

9 Dit zijn fictieve namen.

10 Essen en Maan (2022), Criminele inmenging in het mkb: casusonderzoek naar de faciliterende rol van bonafide ondernemingen in het criminele bedrijfsproces.

Foto:

rade een lid van de organisatie bij een bedrijf plaatsen of een werknemer die al in dienst is rekruteren (mogelijk onder dwang). Ook kan een criminele organisatie de ondernemer zelf rekruteren, bijvoorbeeld als een ondernemer kwetsbaar is doordat het bedrijf zich in zwaar weer bevindt.

Wat willen we bereiken met publiek-private samenwerking tegen de georganiseerde ondermijnende criminaliteit?

Wanneer criminele organisaties de bedrijfsprocessen van bonafide bedrijven misbruiken kan dat schade en gevaarlijke situaties opleveren voor de ondernemer en/of werknemers. Zo kan het zijn dat criminelen een huurauto misbruiken als vluchtauto, waarna het huurbedrijf de auto niet meer terugziet. Als criminelen een bedrijf oprichten als dekmantel, om bijvoorbeeld criminele opbrengsten wit te wassen, dan kan dat leiden tot oneerlijke concurrentie. Dit omdat zij ten slotte niet op een eerlijke manier winst hoeven te maken en daardoor bijvoorbeeld lagere prijzen kunnen rekenen. Daarnaast is het van belang dat bedrijfsprocessen en de aanpak van georganiseerde ondermijnende criminaliteit elkaar niet frustreren. Door publiek-private samenwerking bij de aanpak van ondermijnende criminaliteit ontstaat meer inzicht in en begrip van de bedrijfsprocessen. Hierdoor kan criminaliteit worden voorkomen en bestreden door maatregelen en samenwerkingen die de bonafide bedrijfsprocessen niet in de weg zitten. Kortom, het is cruciaal dat we één brede maatschappelijke coalitie tegen ondermijnende praktijken vormen. We willen ervoor zorgen dat:

- Ondernemers en hun werknemers signalen van georganiseerde ondermijnende criminaliteit herkennen, weten wat zij kunnen doen als ze signalen tegenkomen en welke vervolgstappen mogelijk zijn;
- Bedrijfsprocessen zo weerbaar mogelijk zijn tegen crimineel misbruik door criminele organisaties;
- Private en publieke partners de juiste partijen weten te vinden in het geval dat zij hulpvraag hebben of een kans zien om samen te werken.

Hoe gaan we dat bereiken?

De afgelopen jaren zijn al veel stappen gezet om bovenstaande doelen te realiseren. Het is daarom van belang om, overeenkomstig met de strategische invalshoeken binnen dit actieprogramma, succesvolle initiatieven te borgen en eventueel op te schalen, breder uit te rollen en nieuwe initiatieven op te zetten. We identificeren goede praktijkvoorbeelden en gaan deze met een aantal branches breder uitrollen. Hieronder worden een paar succesvolle initiatieven benoemd die als eerste een vervolg krijgen en in welke branche. Medebepalend daarbij is dat er in die branches energie zit om criminaliteit aan te pakken en zij een rol voor zichzelf zien om de branche verder weerbaar te maken tegen criminaliteit. De acties die worden ingezet vanuit dit actieprogramma staan niet op zichzelf maar zijn een aanvulling op lopende aanpakken, zoals het programma weerbare sierteelt en de aanpak van georganiseerde ondermijnende criminaliteit via de logistieke knooppunten[11].

Acties – weerbare mensen

Vertrouwenspersonen voor meerdere branches (5)

Sinds 2022 is een vertrouwenspersoon voor ondernemers in het agrarische gebied actief. Deze pilot is een initiatief van de Zuidelijke Land- en Tuinbouw Organisatie (ZLTO) met een subsidie van het Ministerie van Justitie en Veiligheid. Deze vertrouwenspersoon helpt agrariërs en tuinders wanneer zij een vermoeden hebben van criminaliteit of onveiligheid ervaren. Ook vervult de vertrouwenspersoon een brugfunctie tussen de ondernemer en de overheid. Iedereen die actief is in het buitengebied kan meldingen, zorgen of vragen bij deze vertrouwenspersoon kwijt met als doel de ervaren veiligheid te verhogen, vertrouwen te vergroten en meldingsbereidheid te doen toenemen. Uit de eerste bevindingen blijkt dat deze ondernemers eerder openstaan voor hulp en advies, doordat zij contact hebben met iemand uit hun eigen branche/sector. De vertrouwenspersoon heeft een goed netwerk binnen de overheid en kan op deze wijze de brug slaan tussen overheidsinstanties als politie, OM en gemeenten aan de ene kant en de agrarische ondernemers aan de andere kant. Hierdoor wordt gebouwd aan onderling vertrouwen, ontstaat een beter inzicht in de problematiek én mogelijk handelingsperspectief om criminaliteit effectiever te voorkomen en bestrijden. De inzet van dergelijke vertrouwenspersonen voor andere branches kan bijdragen aan herstel van vertrouwen in de overheid binnen die branches en biedt kansen voor de verlangde wederkerigheid. Het inzicht van crimineel misbruik in branches kan op fenomeenniveau gedeeld worden met opsporingsdiensten en Wwft-plichtige instanties, zodat zij een beter begrip kunnen ontwikkelen van de fenomenen in de branches.

We verlengen de instelling van de vertrouwenspersoon bij ZLTO met drie jaar en verkennen in ieder geval de mogelijkheid van een vertrouwenspersoon bij brancheorganisatie Cumela en HISWA-RECRON. Het aanstellen van meerdere vertrouwenspersonen biedt ook de kans voor het uitwisselen van ervaringen en de doorontwikkeling van de vertrouwenspersoon. De vertrouwenspersonen worden met middelen behorende bij het Actieprogramma gefinancierd. De branches faciliteren de vertrouwenspersoon door deze onder te brengen binnen hun organisaties.

Meest betrokken partijen: Brancheorganisaties en JenV.

11 Zie "Toelichting kabinetsbrede aanpak ondermijnende criminaliteit" als bijlage opgenomen bij de Najaarsbrief georganiseerde, ondermijnende criminaliteit, Kamerstuk 29911 nr. 379.

Foto: Rutger Rog

Meer bekendheid vertrouwenslijn afpersing (6)

Afpersing is een verborgen delict met grote impact op slachtoffers. De meldings- en aangiftebereidheid is in het geval van afpersing laag. Angst voor represailles, reputatieschade en gevoelens van schaamte zijn belangrijke redenen om geen hulp te zoeken bij de politie. Slachtoffers die afgeperst worden door criminele groeperingen blijken het meest terughoudend te zijn in het doen van aangifte. Voor een goede aanpak is het uitermate belangrijk dat slachtoffers wel durven te melden en hulp zoeken. De vertrouwenslijn afpersing is een onafhankelijke hulplijn die de ondernemer kan benutten. De belangrijkste functie van de vertrouwenslijn afpersing is het slachtoffer goede ondersteuning bieden in een lastige situatie door middel van gespecialiseerde en speciaal opgeleide personen. De ondernemer kan desgewenst in contact worden gebracht met politie en justitie, zodat zij zicht krijgen op het delict. We brengen de deze vertrouwenslijn meer en beter onder de aandacht van ondernemers. Daarbij wordt gekeken naar het niveau waarop de acties plaatsvinden, landelijk of lokaal.

Meest betrokken partijen: JenV, VNO-NCW en MKB-Nederland.

Weerbaarheidstraining voor meerdere branches (7)

Criminele groeperingen hebben baat bij het gebruiken van werknemers van ondernemers voor criminele doeleinden. Zo kunnen zij gevraagd worden om illegale goederen te smokkelen of kan het zijn dat een crimineel bepaalde diensten en/of goederen wil afnemen. Het is daarom belangrijk dat werknemers de signalen van criminaliteit herkennen, weten hoe zij zichzelf weerbaarder kunnen maken en weten waar zij terecht kunnen met signalen en vermoedens. In de haven van Rotterdam en op Schiphol zijn succesvolle weerbaarheidstrainingen ontwikkeld. We verkennen hoe deze trainingen aangepast en toegepast kunnen worden voor en door branches en vinden daarmee aansluiting met verschillende strategische invalshoeken binnen dit actieprogramma, zoals de borging van initiatieven en de branchegerichte aanpak. Daarnaast faciliteren de Platforms Veilig Ondernemen ook verschillende weerbaarheidstrainingen op het gebied van bewustzijn en herkennen van signalen van ondermijning. Die trainingen worden voortgezet gedurende de looptijd van het actieprogramma.

Meest betrokken partijen: JenV en brancheorganisaties.

Meer bewustwording in risicobranches via beroepsopleidingen (8)

Om ervoor te zorgen dat zoveel mogelijk medewerkers in risicobranches weerbaar zijn tegen criminele inmenging is het belangrijk dat we zo vroeg mogelijk inzetten op voorlichting en het vergroten van het bewustzijn. Door (meer) aandacht te schenken aan potentiële criminele inmenging in de opleiding voor beroepen in risicobranches wordt het bewustzijn worden verhoogd. In sommige branches vindt deze voorlichting al plaats. We willen faciliteren dat in meer branches hierop wordt ingezet. In 2023 inventariseren we in welke opleidingen (meer) aandacht nodig is voor dit thema zodat in 2024 gestart kan worden met concrete activiteiten om dit doel te behalen.

Meest betrokken partijen: VNO-NCW en MKB-Nederland, JenV.

Afscherming adressen Handelsregister (9)

Om het risico op bedreigingen en intimidatie van ondernemers te beperken is gewerkt aan een regeling afscherming op verzoek. Dit geldt na dreiging én voor beroepsgroepen waarbij vanuit de branche of individuele verzoeken signalen komen. Gestreefd wordt naar een zo spoedig mogelijke verdere aanpassing van het openbaarheidsregime, binnen de juridische mogelijkheden, met name voor eenmanszaken. Evenals de registratie van bestuursverboden. Dit vindt plaats in het kader van de datavisie. Tegelijkertijd blijft ook de functie van het Handelsregister ten behoeve van

criminaliteitsbestrijding en weerbaarheid tegen fraude van belang.

Meest betrokken partijen: EZK, BZK, JenV.

Aanpak ondermijnende criminaliteit rondom vastgoed en vakantieparken (10)
In het vergroten van de bewustwording in de vastgoedbranche zijn de afgelopen jaren goede stappen gezet. Dat criminelen reguliere bedrijfsprocessen en vastgoed nodig hebben voor hun criminele activiteiten is duidelijk. Zo zijn huurconstructies een dekmantel voor criminelen, met name vanwege de relatief grotere anonimiteit van en verminderde wettelijke controles op een huurder ten opzichte van een koper. Via tussenpersonen en valse of dubbele registraties is de huurder op papier niet altijd de feitelijke gebruiker van het pand. Dit betekent dat bonafide verhuurders met de verhuur van panden onbewust het plegen van strafbare feiten kunnen faciliteren. Te denken valt aan de opslag van wapens of de productie van en handel in drugs[12]. Naast het gebruik van panden voor criminele doeleinden kan vastgoed worden aangekocht voor het witwassen van crimineel vermogen. Het is belangrijk dat poortwachters in de vastgoedbranche hun verantwoordelijkheid nemen en alert zijn op signalen. Meer bewustzijn en handelingsperspectief bieden aan verhuurders is cruciaal om de weerbaarheid in de vastgoedsector te vergroten. Daar blijven we op inzetten onder andere met screeningslijsten, een actueel webdossier vastgoedcriminaliteit bij het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en

voortzetting van de campagne die is opgezet door Meld Misdaad Anoniem. Verder wordt ingezet op het beter delen van de modus operandi, zodat in de vastgoedbranche signalen tijdig worden herkend. We benutten het netwerk ook om in te spelen op nieuwe behoeften of ontwikkelingen in de vastgoedbranche.

Wat betreft vakantieparken wordt gewerkt aan een plan om ondermijnende criminaliteit op vakantieparken beter aan te pakken. De focus ligt op het toepassen en waar nodig versterken van het al ontwikkelde handelingskader voor gemeenten. Het plan wordt in nauwe samenwerking met relevante partners, waaronder de Regionale Informatie- en Expertise Centra (RIEC's), het Landelijk Bureau Bibob en experts werkzaam in het project Ariadne opgesteld.

Publieke en private partijen die betrokken zijn bij de bredere problematiek van ondermijnende criminaliteit in de vastgoedketen zijn duurzaam met elkaar verbonden in de landelijke fenomeentafel (LFT), gecoördineerd en ondersteund door het Landelijk Informatie- en Expertise Centrum (LIEC).

Meest betrokken partijen: BZK, JenV, LIEC, het CCV, gemeenten.

Beleidsagenda aanpak witwassen (11)
Op 23 september 2022 hebben de minister van Financiën en van Justitie en Veiligheid de beleidsagenda aanpak witwassen gedeeld met de Tweede en Eerste Kamer. Daarin geeft het kabinet aan, mede naar aanleiding van recente onderzoeken, dat op een aantal terreinen mogelijkheden voor verdere verbeteringen zijn. In de beleidsagenda wordt ingegaan op de prioriteiten voor de komende periode om verbeteringen te realiseren. Aan alle prioriteiten, waaronder de toegang tot het betalingsverkeer, zijn verschillende vervolgacties gekoppeld. De vervolgacties zullen de komende periode worden uitgewerkt met publieke en private partners. Poortwachters vervullen een cruciale taak in het voorkomen van het gebruik van het financiële stelsel voor witwassen, onderliggende delicten en terrorismefinanciering. De veiligheid van poortwachters bij het melden van ongebruikelijke transacties is belangrijk. Het is ook daarom dat er verschillende maatregelen zijn getroffen om de veiligheid in het meldproces te waarborgen. Op dit moment wordt bezien of er mogelijkheden zijn voor verdere verbetering van de veiligheid van en het gevoel van veiligheid bij melders.

In het kader van de algehele monitoring van de beleidsagenda hebben het ministerie van Financiën en het ministerie van Justitie een stakeholderoverleg opgericht met een aantal betrokken publieke en private partijen.

Acties - weerbare bedrijfsprocessen

Barrièremodellen voor extra branches (12)
Het is belangrijk dat bedrijfsprocessen en de aanpak van georganiseerde ondermijnende criminaliteit elkaar niet frustreren, maar elkaar juist versterken. Het begrip van het bedrijfsproces kan de aanpak van criminaliteit helpen en begrip van het criminele proces kan helpen voorkomen dat een ondernemer slachtoffer wordt. Barrièremodellen zijn een bewezen methodiek om hieraan bij te dragen. Een barrièremodel brengt het criminele bedrijfsproces in kaart. Zo wordt in een oogopslag inzichtelijk welke stappen criminelen moeten zetten om een delict te kunnen plegen en welke partijen en gelegenheden het delict mogelijk maken. Hierdoor wordt ook duidelijk welke barrières publieke en private partners kunnen opwerpen om het proces van criminele organisaties te frustreren. Een barrièremodel voor ondermijning op vakantieparken is in ontwikkeling. We starten met de ontwikkeling van een barrièremodel in de transportsector en de autoverhuur. De strategische invalshoek branchegerichte aanpak komt hier, alsook in de volgende actie, nadrukkelijk naar voren.

Meest betrokken partijen: JenV, CCV en brancheorganisaties.

12 Zie o.a. onderzoek Panden met een luchtje (Bureau Beke, 2020) en Criminele gebouwen (Ateno, 2021).

Onderzoek naar indicatoren van criminele inmenging in bedrijfsprocessen (13)

De afgelopen jaren is er onderzoek gedaan naar branche-specifieke signalen van criminele inmenging in bedrijfsprocessen. Op basis van die kennis kunnen tools worden ontwikkeld die helpen bij het vergroten van de weerbaarheid. In 2023 verkennen we in welke branches al dergelijke onderzoeken zijn gedaan en of aanvullend onderzoek nodig is. Indien dat zo is kan onderzoek voor relevante branches in 2024 en 2025 worden uitgevoerd. De uitkomsten van deze onderzoeken kunnen publieke partners en sectoren en poortwachters, die gebruik van het financiële stelsel moeten voorkomen, meer inzicht in risicobranches bieden en wat vervolgens ondernomen kan worden.

Meest betrokken partijen: Brancheorganisaties en JenV.

Extra hulp bij screening voor ondernemers en gebruiksvriendelijker maken van bestaande tools (14)

Ondernemers willen vaak voordat zij een relatie sluiten met een klant die partij screenen. Voor poortwachters van het financiële stelsel is dit een wettelijk verplichting. Er zijn verschillende tools die ondernemers kunnen gebruiken, maar voor kleine MKB-ondernemers zijn die niet altijd even makkelijk om in te zetten. Bijvoorbeeld omdat een instrument te tijdrovend of kostbaar is. We maken een inventarisatie van screeningstools waarvoor dit van toepassing is en zetten in op het vergroten van het gebruikersgemak voor ondernemers.

Meest betrokken partijen: VNO-NCW en MKB-Nederland, JenV

Acties - weerbaar netwerk

Weerbare brancheorganisaties (15)

Brancheorganisaties hebben belangrijke specifieke vakkennis over hoe een bonafide ondernemer kan voorkomen dat een criminele organisatie misbruik maakt van de ondernemer. Dat is relevante informatie voor criminelen, die een onderneming als dekmantel willen gebruiken. Daarom onderzoeken we hoe brancheorganisaties het beste kunnen voorkomen dat malafide ondernemers lid worden en indien zij al lid zijn, hoe zij uit de brancheorganisatie verwijderd kunnen worden. De uitkomsten van het onderzoek verwerken we tot een handreiking, die brancheorganisaties informeert welke concrete stappen zij kunnen nemen.

Meest betrokken partijen: JenV, VNO-NCW en MKB-Nederland.

Informatie- en gegevensdeling en juridisch steunpunt (16)

Informatie- en gegevensdeling loopt als rode draad door de aanpak van georganiseerde ondermijnende criminaliteit en heeft als strategische invalshoek een belangrijke plek binnen dit Actieprogramma. Privacy en de aanpak van ondermijning staan niet lijn recht tegenover elkaar; de relevante wetgeving laat ruimte voor de uitwisseling van gegevens, binnen een aantal kaders. Ook is het zo dat informatie over bijvoorbeeld modus operandi, trends en fenomenen, die dus géén persoonsgegevens bevatten, veel kunnen bijdragen aan de aanpak. Die informatiedeling is momenteel echter nog te vrijblijvend. Gedurende het actieprogramma onderzoeken we hoe we meer gestructureerde informatiedeling kunnen aanmoedigen, waar de ruimte in de wetgeving zit voor gegevensdeling met private partners en zoeken we goede praktijkvoorbeelden op het gebied van informatie- en gegevensdeling om breder onder de aandacht te brengen. Daarbij is ook aandacht voor de vraag hoe informatie uit de opsporing, bijvoorbeeld trends en modus operandi, de ondernemers kunnen helpen, zoals bij de Gemeenschappelijke Informatie Organisatie (GIO) van Stichting GIO, politie, OM en de detailhandel.

Ook ambiëren we gedurende de eerste twee jaar van het actieprogramma een pilot met een juridisch steunpunt voor private partners. Het steunpunt kan brancheorganisaties helpen met vragen op het gebied

Foto: Nienke Elenbaas

van gegevensdeling in relatie tot criminaliteitsbeheersing, bijvoorbeeld bij het opstellen van een convenant. Met betrekking tot cross-sectorale gegevensdeling wordt opvolging gegeven aan het WODC-onderzoek 'foute huurders'.

Meest betrokken partijen: JenV, VNO-NCW en MKB-Nederland.

Aanscherping wet- en regelgeving (17)

Voor een integrale aanpak van georganiseerde ondermijnende criminaliteit moeten we alle instrumenten gebruiken in ons arsenaal, waaronder ook passende wet- en regelgeving. We kijken naar verschillende mogelijkheden op het gebied van wet- en regelgeving om de aanpak van georganiseerde ondermijnende criminaliteit te versterken, zoals de regulering van verschillende risicobranches. Hierbij nemen we onder andere de lopende trajecten voor relevante branches in overweging, kaders voor landelijke regulering, uitvoerbaarheid, mogelijke ongewenste gevolgen en regeldruk voor ondernemers en subsidiariteit. Dat vergt een proces van enige tijd, dat verder uitgedacht dient te worden in samenspraak met de RIEC's en andere betrokken partijen.

Zo wordt ingezet op aanvullende wet- en regelgeving om de georganiseerde ondermijnende criminaliteit in de vastgoedbranche een halt toe te roepen. Er is behoefte aan meer grip en tijdig acteren op signalen die wijzen op mogelijke malafide verhuur. Het wetsvoorstel Goed verhuurderschap is een mooie kans om een perspectief met betrekking tot ondermijnende criminaliteit te formuleren en onder het bereik van deze wet te brengen. Hierbij wordt gedacht aan een grondslag te bieden om een vergunningsplicht in te stellen. Doelstelling is bonafide verhuurders te beschermen en het misbruik van vastgoed door criminelen te bemoeilijken.

In de autobranche spelen vergelijkbare dilemma's en problemen. Uit signalen van (onder meer) de politie blijkt dat huurauto's voor criminele activiteiten worden gebruikt vanwege de anonimiteit van het gebruik. Dit beeld wordt gesteund door de uitkomsten van het onderzoeksrapport '*Criminelen achter het stuur*' van Bureau Beke dat in 2019 is gepubliceerd. Om de gebruikers van huurauto's uit de anonimiteit te halen wordt er met publieke en private partners gesproken over een registratieplicht voor alle huurders en bestuurders van huurauto's. In samenwerking met het ministerie van Infrastructuur en Waterstaat en andere relevante partners wordt de nadere verkenning uitgewerkt.

In de transportsector bestaat de wens om te kijken naar de huidige grens voor de vergunningplicht voor het beroepsgoederenvervoer over de weg.

Meest betrokken partijen: JenV, RIEC's, gemeenten, BOVAG en TLN.

Digitaal platform PPS tegen ondermijning (18)

Een semi-gesloten digitaal kennisplatform kan een waardevolle bijdrage leveren aan het versterken van de publiek-private samenwerking op vele fronten. Het digitale PPS-platform ondermijning kan enerzijds een netwerkfunctie vervullen door profielen en contactgegevens van personen die betrokken zijn bij publiek-private samenwerking beschikbaar te maken. Anderzijds dient het platform PPS-ondermijning als een vindplaats voor (niet casus gerelateerde) informatie en kennis over PPS op het gebied van ondermijning. Het digitale platform zal zich in beginsel richten op het netwerk rondom ondermijning en moet een goede verbinding hebben met bestaande platforms. Indien succesvol kan het breder uitgerold worden voor PPS in den brede.

Meest betrokken partijen: JenV, VNO-NCW en MKB-Nederland.

Vergroten netwerk (19)

Samenwerking tussen de overheid en de private partijen is noodzakelijk om het veelkoppige monster van de ondermijning te beteugelen. Er zijn momenteel nog partijen die een rol kunnen spelen in de publiek-private samenwerking, maar nog niet betrokken zijn. We streven het PPS-netwerk te vergroten door aandacht te vragen voor het thema bij partners die nog niet zijn betrokken.

Meest betrokken partijen: JenV, politie, VNO-NCW en MKB-Nederland.

Versterken fenomeengerichte aanpak (20)

Het is van belang dat de inzet van verschillende partijen uit het netwerk goed op elkaar aansluit. Publieke en private partners moeten van elkaar weten wat zij doen en de informatie die wordt gedestilleerd, zoals fenomenen en trends, moet met elkaar worden gedeeld. Een voorbeeld van een middel daartoe is de fenomeengerichte aanpak van de politie. Die aanpak bloeit met voeding met informatie van ondernemers, bijvoorbeeld uit aangiften, maar daarvoor moet wel breder bekend zijn wat de fenomeengerichte aanpak inhoudt. We verkennen daarom hoe we de fenomeengerichte aanpak beter onder de aandacht kunnen brengen van ondernemers en hoe we de beleveniswereld van publieke en private partners dichter bij elkaar kunnen brengen.

Meest betrokken partijen: politie, OM, VNO-NCW en MKB-Nederland.

Gebiedsgerichte aanpak (vermogens) criminaliteit

"Ik ben nu 19 jaar supermarktondernemer. Jullie zijn van harte welkom om de aangiftemap eens door te nemen. Tweemaal een overval, meerdere malen winkeldiefstal met geweld (waarvan alleen ik al twee keer een gebroken vinger heb opgelopen) en ontelbaar vele winkeldiefstallen.

Het zijn vlagen qua hoeveelheid, het is in de afgelopen 19 jaar nooit minder geworden, alleen maar meer."

"Verbaal en fysiek geweld neemt enorm toe en wij als winkeliers maar vriendelijk blijven. Meldingen worden niet serieus genomen, lange tijd komst politie, lange tijd voordat je aangifte kunt doen of beelden kunt overhandigen, meestal verneem je niks. Als je iets verneemt is er vaak meer dan een jaar overheen gegaan."[13]

We hebben als transportondernemers te maken met diefstal van lading, brandstof of zelfs voertuigonderdelen van vrachtauto's die langs de weg of op het (eigen) bedrijventerrein staan geparkeerd. Schuifzeilen van vrachtauto's worden moedwillig vernield en banden lek gestoken. Een voorbeeld is een transportbedrijf waarvan in de laatste vijf jaar bij 123 incidenten in Nederland bijna 37.000 liter diesel uit de voertuigtanks is gestolen. Niet alleen heeft de ondernemer te maken met de directe schade hiervan, maar ook met de vervolgschade, omdat het voertuig gerepareerd moet worden en daarom tijdelijk niet beschikbaar is.

Wat willen we bereiken met gebiedsgerichte publiek-private samenwerking tegen (vermogens) criminaliteit?

Bedrijventerreinen, buitengebied en winkelgebieden moeten veilig zijn en veilig voelen voor ondernemers, medewerkers en bezoekers. Ondernemers geven aan vooral last te hebben van veelvoorkomende vormen van criminaliteit zoals diefstal, en agressie en intimidatie. Dit willen we tegengaan. Het terugdringen van high impact crimes als overvallen blijft belangrijk. Genoemde criminaliteitsfenomenen vragen niet alleen een gebiedsgerichte benadering, die benadering kan echter wel van meerwaarde zijn om deze criminaliteitsvormen te verminderen. Met een dergelijke benadering wordt namelijk eerder door de betrokken partijen op een integrale en samenhangende wijze gewerkt aan een aanpak die effect sorteert. Met een gebiedsgerichte aanpak bundelen we bovendien voordelen van (sectorale) investeringen.

Hoe gaan we dat bereiken?

In de gebiedsgerichte aanpak van criminaliteit zetten we in op een sleutelrol voor de Platforms Veilig Ondernemen. We bevorderen de aanpak met de realisatie van tien goed toegeruste platforms. In samenhang met relevante lokale en landelijke partijen zetten zij zich in om de weerbaarheid van ondernemers tegen criminaliteit te bevorderen. In het volgende hoofdstuk worden de (beoogde) ontwikkelingen daarin nader beschreven. Naast een hotspotbenadering wordt

13 VakcentrumVisie nr.9.

de economische infrastructuur in de veiligheidsanalyse en in de aanpak meegenomen.

Zo verkrijgen de Platforms Veilig Ondernemen een goed beeld van veiligheidsproblematiek die zich op meerdere plekken (lokaal) manifesteert.

De gebiedsgerichte PPS-aanpak staat niet op zichzelf. Het maakt onderdeel uit van de lokale inzet om de veiligheid te vergroten met een belangrijke rol voor gemeenten, ondernemers, RIEC's, politie, wijkteams, hulpverleners etc.

Inhoudelijk gaat het qua gebiedsgerichte aanpak onder meer om facilitering en ondersteuning van beproefde PPS-instrumenten als Veilig Ondernemen voor bedrijventerreinen, winkelgebieden en buitengebied. We werken aan veilige binnensteden. We gaan (winkel) diefstal tegen en dringen mobiel banditisme terug. We zetten in op weerbaarheid tegen agressie en intimidatie van personeel van banken, winkels en horeca. De Taskforce Overvallen gaat verder met de aanpak van overvallen en ram- en plofkraken. In de jaarlijkse Week van de Veiligheid wordt extra aandacht besteed aan criminaliteitspreventie, met een centrale rol voor de Platforms Veilig Ondernemen die regionaal diverse activiteiten ontplooien gericht op ondernemers. PVO-NL zal hierin een trekkersrol vervullen.

Acties

Veilige bedrijventerreinen en winkelgebieden (21)

Veel gemeenten hebben (afgelegen) bedrijventerreinen waar weinig (sociaal) toezicht is, het niet veilig voelt en waar criminaliteit plaatsvindt. Agressieve klanten, vandalisme, hangjongeren, winkeldiefstal of een overval zijn problemen waar veel winkelgebieden mee geconfronteerd worden.

Door een gerichte aanpak op gebiedsniveau, zoals de PPS-aanpak Veilig Winkelgebied en Veilig Bedrijventerrein, worden gezamenlijk (ervaren) problemen aangepakt. Een bedrijventerrein kenmerkt zich door uitdagingen als het gaat om overlast, inbraak, cybercrime en ondermijnende criminaliteit. Daarentegen zijn agressieve klanten, vandalisme, hangjongeren, winkeldiefstal of een overval met name problemen waar veel winkelgebieden mee geconfronteerd worden.

Door middel van het opzetten van een lokaal gebiedsgerichte PPS wordt actief gewerkt aan gezamenlijk (ervaren) problematiek. Dit gebeurt volgens een gestructureerd proces. Het CCV/PVO-NL brengt stap voor stap betrokken partijen samen, veiligheidsproblemen worden in kaart gebracht, oplossingen gezocht en maatregelen genomen. Deze gebiedsgerichte benadering zorgt ervoor dat de veiligheidsproblematiek gericht aangepakt wordt waarbij maatwerk op lokaal niveau mogelijk is. Doordat betrokkenen vanuit verschillende disciplines (gemeente, politie, brandweer, ondernemers) deelnemen aan het PPS-netwerk, kan snel worden gehandeld, ook als zich acute veiligheidsproblemen voordoen.

Met maatregelen zoals betere openbare inrichting inclusief verlichting, georganiseerd toezicht en brandpreventie zorgen lokale partijen gezamenlijk voor een schoon, goed onderhouden en veiliger bedrijventerrein of winkelgebied. De criminaliteit daalt en het veiligheidsgevoel van ondernemers, medewerkers en bezoekers stijgt. PVO-adviseurs helpen lokale partijen bij het hele traject, van het opzetten van de publiek-private samenwerking tot de daadwerkelijke uitvoering van de maatregelen.

Meest betrokken partijen: het CCV/PVO-NL, gemeenten, politie, winkeliers en bedrijven.

Veilig buitengebied (22)

Het buitengebied is aantrekkelijk voor (drugs)criminelen, onder andere vanwege de soms moeilijke financiële positie van boeren, gebrek aan zichtbare handhaving door de overheid en leegstand. Ongeveer 1 op de 5 respondenten heeft weleens iemand aan de deur gehad die het agrarisch vastgoed wilde gebruiken waarbij zijn/haar intenties mogelijk verband hielden met drugscriminaliteit[14].

Met het instrument Veilig Buitengebied wordt middels publiek-private samenwerking een netwerk binnen een gemeente opgezet dat de ondernemers en bewoners in het buitengebied helpt zich te weren tegen criminaliteit en bewust te worden van signalen van (ondermijnende) criminaliteit. Zo wordt er actief met de gemeente gesproken over oplossingen voor problematiek waar ondernemers en bewoners tegenaan lopen met betrekking tot de herbestemming van vastgoed. Daarnaast wordt gekeken hoe de veiligheid in het gebied kan worden vergroot en wordt dit in gezamenlijkheid aangepakt.

In 2023 wordt ingezet op intensivering van het gebruik van het keurmerk bij gemeenten.

Meest betrokken partijen: JenV, LNV, CCV/PVO-NL, gemeenten, agrarisch ondernemers.

Veilige binnensteden (23)

Ontwikkelingen als thuiswerken en de toename van online winkelen vragen om een nieuwe kijk op de binnenstad. Er zijn in de grote binnensteden onder meer uitdagingen op het gebied van verschraling van het aanbod qua voorzieningen, verloedering en ondermijnende criminaliteit. Samen met in ieder geval Eindhoven, Amsterdam, Utrecht, Groningen, Den Haag, Rotterdam, Nijmegen, Breda en de ministeries van

14 Weerbare boeren in kwetsbaar gebied, TwynstraGudde, 2020.

Foto: Rutger Rog

Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken en Klimaat wordt - op basis van een in 2022 opgeleverde verkenning - in samenwerking kennis, denkkracht en capaciteit gebundeld in een City Deal. Doel is om te experimenteren en te leren hoe we gewenste ontwikkelingen in de binnensteden kunnen bevorderen en ongewenste ontwikkelingen kunnen tegengaan. De strategische invalshoek innovatie vindt hier zodoende nadrukkelijk een plek. Te denken valt aan het verbeteren van de informatiepositie op het punt van ondermijnende criminaliteit in de binnensteden en het doen van een pilot om meer grip te krijgen op vastgoed. De verwachting is dat deze City Deal in het voorjaar van 2023 getekend wordt.

Meest betrokken partijen: grote steden, BZK, JenV, EZK, VNO-NCW en MKB-Nederland.

Terugdringen winkeldiefstal (24)

Winkeldiefstal blijft een groot probleem waar de retail de samenwerking met de politie zoekt om deze aan te pakken. Hierbij staan gegevensdeling en informatie-uitwisseling centraal in de preventie en in de aanpak van daders. Om winkeldiefstal terug te dringen, wordt ingezet op de volgende activiteiten:

- Doorontwikkeling en bredere uitrol instrument collectief winkelverbod;
- Ontwikkeling van een toolbox interventies winkeldiefstal.

Momenteel ontwikkelt de politie een nieuwe manier van gegevensuitwisseling tussen enerzijds de politie en anderzijds private partijen, waarbij via een beveiligde koppeling relevante gegevens tussen de eigen software van private partijen automatisch worden uitgewisseld met de software van de politie en andersom. Vanuit deze publiek-private dienstverlening loopt een pilot winkeldiefstal met een aantal grote ketens en private partijen voor civiele afhandeling. Einddoel is dat deze koppeling gebruikt kan worden voor andere gegevens-uitwisseling met private partijen. De strategische invalshoek informatie- en gegevensdeling vindt hier zodoende nadrukkelijk een plek.

- Verkenning van ondernemerspecifieke aangifte- en/of meldwensen en gezamenlijke activiteiten ter ondersteuning van een verbeterproces.

Meest betrokken partijen: retail, politie, het CCV.

Terugdringen mobiel banditisme (25)

Mobiel banditisme is een paraplubegrip voor het stelselmatig en in georganiseerd verband plegen van vermogensdelicten, zoals winkel-, auto- en ladingdiefstal, woninginbraak en zakkenrollerij. Deze misdrijven worden gepleegd door rondtrekkende dadergroepen die zowel in Nederland als in andere landen actief zijn. Door de aard en omvang van de delicten heeft mobiel banditisme een grote impact op de samenleving. De buitenlandse groepen veroorzaken, door het professionele karakter, over het algemeen veel financiële en emotionele schade. Dit doordat de buit groter en duurder is, de restschade bij bijvoorbeeld auto inbraken hoger is en de feiten dichter in de persoonlijke leefomgeving van de aangevers gepleegd worden.

Sinds 2018 heeft de Taskforce Mobiel Banditisme zich ingezet om Nederland onaantrekkelijk te maken als delictgebied voor mobiele dadergroepen. De Taskforce heeft bereikt dat er een structuur is opgericht die heeft gezorgd voor meer scherpte en focus in de aanpak, dat er concrete en zichtbare resultaten zijn behaald en dat er een integrale aanpak is opgezet, waarbij naast het strafrecht een grote rol is weggelegd voor preventie.

De Taskforce heeft haar doelstellingen bereikt en eindigt daarom tegelijktijdig met het aflopen van het vorige Actieprogramma.

De problematiek van criminaliteit gepleegd door mobiele dadergroepen bestaat echter nog steeds. Om

de publiek-private aanpak van Mobiel Banditisme te continueren, blijft de werkgroep bestaan en wordt ingezet op de volgende activiteiten:

- Doorontwikkeling systematische informatie-uitwisseling winkeliers en politie (Gemeenschappelijke Informatie Organisatie);
- Ontwikkeling Digitaal Nachtregister;
- Doorontwikkeling systematische informatie-uitwisseling transportsector en politie met betrekking tot ladingdiefstal en diefstal van diesel uit de brandstoftanks van geparkeerde vrachtwagens op verzorgingsplaatsen. Deze informatie-uitwisseling is gericht op versterking van de preventie, zowel aan publieke als private kant, als op effectievere en efficiëntere repressie.

Meest betrokken partijen: politie, gemeenten, JenV, OM, het CCV, stichting GIO, TLN en detailhandel.

Terugdringen overvallen, straatroof en geweld (26)

Het terugdringen van high impact crimes als geweld, overvallen, ram- en plofkraken en straatroven vindt plaats door de inzet van dadergerichte, slachtoffergerichte en situationele maatregelen, zowel preventief als repressief. Dit betreft niet alleen een gebiedsgerichte aanpak, het manifesteert zich echter wel vooral lokaal en is in veel gemeentelijke veiligheidsplannen en PVO-jaarplannen een thema. De Taskforce Overvallen continueert de integrale aanpak met een nieuw actieprogramma met aandacht voor het voorkomen van slachtofferschap/situationele preventie, het voorkomen van daderschap, opsporing en vervolging en het tegengaan van recidive. Het lokaal bestuur is primair verantwoordelijk voor de lokale veiligheid. Gemeenten worden gestimuleerd en gesteund in het ontwikkelen van nieuwe en het uitvoeren van bestaande maatregelen die aan de lokale veiligheid bijdragen.

Aangezien er al een sterke integrale aanpak is van high impact crimes als geweld, overvallen, ram- en plofkraken en straatroven is geen nieuw actiepunt geformuleerd.

Meest betrokken partijen: retail, banken, gemeenten, politie, OM, horeca, JenV en het CCV.

Terugdringen agressie en intimidatie (27)

De retail heeft te maken criminaliteit en ongewenst gedrag op de winkelvloer. Het tegengaan en/of omgaan met agressie en geweld tegen winkelmedewerkers heeft hierbij prioriteit. Preventief zetten winkels in op buitbeperking, bijvoorbeeld door het stimuleren van pinnen en het onbereikbaar maken van contant geld of goederen. Trainingen van medewerkers gaan in op het voorkomen of omgaan met agressie en geweld.

Mede op basis van de aanpak in de Taskforce Onze Hulpverleners Veilig, de voormalige aanpak Veilige Publieke Taak en samen met de Taskforce Overvallen verkennen we wat we gezamenlijk kunnen ontwikkelen om agressie en intimidatie tegen personeel van o.a. banken, winkels, supermarkten en horeca tegen te gaan. Daarnaast verkennen we gezamenlijk welke samenwerkingsvormen kunnen bijdragen aan verdere verbetering van het beleid tegen agressie, zoals het ontwikkelen van een adequaat dreigingsbeeld aan de hand van open bronnen. Hierbij hebben wij ook aandacht voor opvolging, goed werkgeverschap en slachtofferhulp.

Meest betrokken partijen: banken, retail, horeca, Slachtofferhulp Nederland en JenV.

Terugdringen jeugdcriminaliteit (28)

Uit de Monitor Zelfgerapporteerde Jeugdcriminaliteit (2020) weten we dat ongeveer 37% van de jongeren wel eens een delict heeft gepleegd. De jeugdcriminaliteit daalt, maar - hoewel de aantallen relatief beperkt zijn - steeds meer kwetsbare jongeren raken betrokken bij

zware vormen van criminaliteit. Ook worden meer jongeren veroordeeld voor cybercriminaliteit.

Binnen een breder pakket aan maatregelen is een geselecteerd aantal gemeenten de mogelijkheid geboden om in hun meest kwetsbare wijken een domeinoverstijgende en gebiedsgerichte aanpak neer te zetten. Die bestaat uit het bieden van kansen aan jongeren (en indien in beeld: hun broertjes of zusjes) die kwetsbaar zijn om in de criminaliteit te komen, maatregelen in de sociale, fysieke en online leefomgeving van de jongeren en het versterken van de gemeente en justitiële partners in de wijk, zodat crimineel gedrag gecorrigeerd wordt. Vanaf 2022 starten de 15 gemeenten samen met hun partners de structurele aanpak 'Preventie met gezag' in hun meest kwetsbare wijken. Hierin zoeken zij een goede balans tussen kansen bieden op een betere toekomst aan de ene kant en grenzen stellen aan risico- en crimineel gedrag aan de andere kant[15].

Met het Nationaal programma Leefbaarheid en Veiligheid zet het Rijk stappen voor een langjarige inzet om samen met gemeenten en andere lokale partijen zoals ondernemers de leefbaarheid en veiligheid in 20 focusgebieden in 19 steden weer op orde te krijgen[16].

In het najaar van 2020 is het actieplan Wapens en Jongeren vastgesteld[17]. De deelnemers aan dit actieplan beogen hiermee wapenbezit en -gebruik door jongeren terug te dringen. In het kader van dit actieplan vindt ook publiek private samenwerking plaats. Zo hebben diverse koepels uit de retailbranche aangegeven dat zij vrijwillig afzien van verkoop van messen aan minderjarigen. Hiermee lopen zij vooruit op een wetsvoorstel dat dit zal verbieden en dat nu nog in voorbereiding is. De horeca is een van de speerpunten in het actieplan Wapens en Jongeren, waarbij de lokale samenwerking tussen horeca en politie aandacht krijgt. Bureau Beke heeft in opdracht van het ministerie van Justitie en Veiligheid een checklist geactualiseerd, die ziet op het invoeren van controles op wapenbezit in de horeca. Ook is de Kwaliteitsmeter Veilig Uitgaan (KVU) aangepast met specifieke aandacht voor wapenproblematiek. Het CCV begeleidt gemeenten in de toepassing hiervan.

Voor risicojongeren van 16-27 jaar wordt ingezet op de Integrale Persoonsgerichte Toeleiding naar Arbeid waarbij deze jongeren goede begeleiding krijgen met het oog op toeleiding naar school en werk, ook tijdens hun stage bij bedrijven.

Aangezien voor het terugdringen van jeugdcriminaliteit al een integrale aanpak tot stand is gebracht is geen nieuw actiepunt geformuleerd.

Meest betrokken partijen: gemeenten, bedrijfsleven, CCV, JenV, OCW, BZK, VWS en SZW

15 Kamerstuk 28 741, nr.86.
16 Kamerstuk 30 995, nr. 100.
17 Kamerstuk 28 684, nr. 637.

Foto: Tineke Dijkstra

Doorontwikkeling Platforms Veilig Ondernemen

Bij de inhoudelijke thema's van dit actieprogramma wordt met regelmaat de inzet van de Platforms Veilig Ondernemen beschreven. In dit hoofdstuk wordt de niet themagebonden doorontwikkeling belicht waarbij een inhoudelijke en organisatorische doorkijk wordt gegeven.

De regionale PVO's zijn een laagdrempelige digitale en fysieke ontmoetingsplek, waarin ondernemers en overheid direct samenwerken op het gebied van veilig ondernemen. Juist de combinatie van private ondernemers met hun eigen agenda's, doelstellingen en kennis van eigen organisatie, en de kennis en inzet van publieke partijen op het gebied van criminaliteitsbestrijding, zorgt voor unieke inzichten. Dat begint met elkaar ontmoeten. Elkaar leren kennen en elkaars taal leren spreken. Dit is de basis die het PVO biedt en die het mogelijk maakt maatwerk producten te leveren die impact maken. Want het PVO is gericht op de uitvoering. Op het leveren van diensten en het uitvoeren van innovaties die direct toepasbaar zijn voor de ondernemers. Haar actiegerichtheid maakt de verbinding met ondernemers sterker en zorgt voor meer begrip van en weerbaarheid tegen criminaliteit onder ondernemers. De PVO's zullen ondernemers ook wegwijs maken hoe ondernemers veilig vermoedens kunnen melden, zoals bijvoorbeeld Meld Misdaad Anoniem en voorzien in een hulpmiddel om de verschillende mogelijkheden om te melden duidelijk te maken.

In 2022 is een structurele basis onder de PVO's gelegd. Het vergroten van de slagkracht en effectiviteit van de tien regionale PVO's stonden voorop, met als doel de weerbaarheid van ondernemers tegen criminaliteit te versterken. Ieder regionaal PVO beschikt over een fulltime manager en een aantal adviseurs. Deze adviseurs zijn dagelijks in hun regio actief om ondernemers weerbaar te maken tegen allerlei vormen van criminaliteit. Er is een landelijk expertisecentrum ingericht (PVO-NL) bij het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) dat de regionale platforms ondersteunt en waar landelijke brancheorganisaties aan kunnen

haken. Samenwerkings- en verantwoordingsafspraken die tot stand zijn gebracht en gesprekken met onder meer bestuurders van de stuurgroepen van de PVO's zorgen voor stroomlijning van dit proces en korte lijnen. Het ministerie van JenV heeft structureel middelen (€ 10 miljoen) voor de PVO's gereserveerd in de meerjarenbegroting.

Regionale PVO's

Het succes van het PVO-bestel komt van de regionale PVO's. Daar zit kennis van de lokale problematiek en vindt de prioriteitstelling van activiteiten in de regio plaats. De basis is een sterk (lokaal) netwerk van relevante samenwerkende publieke en private partijen dat zorgt voor informatie- en kennisdeling enerzijds en de mogelijkheid van brede distributie van producten en activiteiten anderzijds. Een PVO heeft een krachtige organisatie nodig, verantwoordelijk voor het ondersteunen van het regionale bestuur met alle relevante partners, het onderhouden van het netwerk, het opstellen van het jaarwerkplan en bovenal het uitvoeren van de activiteiten ter preventie van criminaliteit.

Ondersteuning

Omdat de PVO's veelal relatief kleine organisaties zijn met een focus op de uitvoering, is het efficiënt en effectief om aanvullend kennis en expertise te bundelen bij een landelijk expertisecentrum dat desgewenst ook kan ondersteunen in de bedrijfsvoering en in het werkgeverschap van regionale PVO-managers en projectleiders. Het CCV neemt deze taak op zich en heeft daartoe het expertisecentrum PVO-NL opgericht. Op deze manier wordt landelijke expertise op relevante thema's geborgd, hoeft niet ieder PVO het wiel opnieuw uit te vinden en kunnen nieuwe inzichten snel verspreid worden in het land.

PVO-NL bouwt de komende tijd aan een professionalisering van de organisatie waarbij gewerkt wordt aan de volgende taken:

- Kennisverbreding, ontwikkeling en verdieping, productontwikkeling, communicatie, branding en positionering PVO's.
- Faciliteren van de onderlinge samenhang tussen de PVO's en versterking van de samenwerking. Dit geldt zowel voor de inhoud als voor de wijze van uitvoering, het uitrollen van landelijke initiatieven of het bieden van overzicht in waar ondernemers terecht kunnen met meldingen, signalen en hulpvragen. Maar ook op organisatorisch vlak zoals de inrichting van het bestuur, personele vraagstukken en uniforme communicatiestromen (zowel intern als extern).
- Bouwen aan een brugfunctie richting landelijk georganiseerde partijen, waaronder brancheorganisaties en daarbij de PVO-aanpak coördinerend voor branches waarvan de leden landelijk werken en dus in verschillende regio's te maken hebben met (dezelfde vormen van) criminaliteit.

PVO-NL bestaat uit een meewerkend manager en een aantal adviseurs waaronder landelijke themaspecialisten. De themaspecialisten bouwen aan een sterk netwerk waarbij zij de trekker worden van hun thema. Zij zijn expert op het gebied van hun thema en vertalen de praktijk naar visie en strategie (en andersom). Zij zullen op inhoud de brug slaan tussen de problematiek in de regio's, de landelijke ontwikkelingen en de kennis die het CCV in huis heeft. De werkzaamheden van de themaspecialist zijn toegespitst op initiëren, signaleren, adviseren, verbinden en faciliteren en spelen een rol in de samenhang tussen de regio's.

De regionale PVO's maken de komende tijd een verdere professionaliseringsslag. Op basis van de jaarplannen werken zij aan een uitbreiding van de personele capaciteit en een solide backoffice. Daarnaast krijgen de regionale besturen verder vorm en gaan de PVO's verder met de positionering in de regio.

Actie

We stellen een plan op hoe bovenstaande taken vorm krijgen, wat verder moet gebeuren om een professionele organisatie te realiseren ten behoeve van het effectief weerbaarder maken van ondernemers en hoe we daar de komende jaren aan bouwen, zodat daar ook op gestuurd kan worden. (29)

Aanpak fraude

Fraude is een ernstig maatschappelijk probleem dat burgers, private organisaties, bedrijfsleven en overheid financieel benadeelt. Fraude veroorzaakt grote financiele schade voor bedrijven (miljarden op jaarbasis), ondermijnt het vertrouwen in het handelsverkeer, brengt financiële en emotionele schade met zich mee voor slachtoffers en is vaak ook ondersteunend aan andere vormen van criminaliteit. Ook de integriteit van stelsels als financiële markten en de zorgsector lijden hieronder.

Wat willen we bereiken met publiek-private samenwerking tegen fraude?

Het is van belang om met brede preventie en gerichte repressie te werken aan het tegengaan van (online) fraude. Dat kan alleen door met alle bij dit onderwerp betrokken publieke en private partijen samen te werken. Het is een verantwoordelijkheid van bestuurders in het bedrijfsleven om actief te sturen op het nemen van maatregelen in hun organisatie en op samenwerking met partners om fraude effectief te kunnen aanpakken. Niet in de laatste plaats hebben zij een verantwoordelijkheid in het beschermen van hun klanten. De overheid heeft een rol bij het stroomlijnen van de aanpak, het nemen van algemene preventiemaatregelen (denk aan publiekscampagnes), wet- en regelgeving en hulp aan slachtoffers.

Hoe willen we dit bereiken?

Binnen de brede aanpak van fraude zijn preventie, signalering, het kunnen melden van fraude en slachtofferhulp belangrijke onderdelen. Er zijn voor de aanpak van online fraude vijf pijlers geïdentificeerd: preventie, opwerpen technische barrières, slachtofferhulp, opsporing en vervolging en expertiseontwikkeling en informatiedeling. Steeds meer ondernemers hebben of krijgen met online fraude te maken, bijvoorbeeld in de vorm van phishing of CEO-fraude. In aanvulling daarop wordt voor de aanpak van online fraude in samenspraak met publieke en private partijen een integrale aanpak ontwikkeld[18]. De komende jaren wordt daarom fors ingezet op de intensivering van gerichte maatregelen voor de aanpak van online fraude.

Samenhang tussen de integrale aanpak online fraude en het NPC is geborgd doordat verschillende partners in het NPC direct bij de integrale aanpak zijn betrokken. Aangezien er al een sterke integrale aanpak van online fraude is, worden er op het moment van schrijven van het Actieprogramma geen nieuwe acties ingezet vanuit het NPC. Indien partners in de toekomst aanvullende acties nodig achten, kunnen deze in het NPC besproken worden en eventueel worden opgepakt.

18 Kamerstuk 29 911, nr. 372.

Governance, monitoring en middelen

Governance

Publiek-private netwerken zijn flexibel en fluïde. De samenwerkingsvorm is geen vast gegeven; de aard van de opgave en het beoogde effect zijn bepalend voor de partners die bij de samenwerking zijn betrokken. Dit is medebepalend voor de samenstelling van het NPC en de samenstelling of werkvorm van onderliggende werkgroepen.

Het actieprogramma is een gezamenlijk programma, dat ook gezamenlijk tot stand is gekomen. Het succes van het programma valt of staat met de gezamenlijke verantwoordelijkheid voor de uitvoering ervan. In de totstandkoming is daarbij door verschillende betrokken partijen aangegeven dat de organisatie van de uitvoering en de verantwoordelijkheidsverdeling in de komende periode aandacht verdient. Hoe borgen we dat dit gezamenlijke programma ook daadwerkelijk gezamenlijk wordt uitgevoerd waarbij heldere afspraken gemaakt worden over welke partij waarvoor aanspreekbaar en verantwoordelijk is. Het NPC is richtinggevend voor de totstandkoming en uitvoering van dit Actieprogramma Veilig Ondernemen.

Actie

Aangezien het huidige instellingsbesluit van het NPC stamt uit 1992 wordt in de eerste helft van 2023 bezien of het een update behoeft. Begin 2023 wordt ook nader verkend hoe de betrokken partijen samenwerken aan de uitvoering van het programma en hoe dit versterkt wordt. (30)

Het NPC moet gedurende de looptijd van het actieprogramma oog hebben voor ontwikkelingen en daar desgewenst op in (kunnen) spelen. Het actieprogramma beoogt bovendien, overeenkomstig met de benoemde strategische invalshoeken, goede praktijkvoorbeelden te identificeren en verder uit te rollen. We beginnen met een aantal branches, waar energie zit en betrekken vervolgens meer en meer branches. Gedurende de looptijd moeten dus ook besluiten worden genomen of een praktijkvoorbeeld verder uitgerold wordt en in welke branches. Het NPC wordt gedurende de uitvoering van projecten geïnformeerd over de voortgang en neemt beslissingen over de belangrijkste mijlpalen, zoals het verder uitrollen van pilots in branches. Hiervoor zal het NPC geadviseerd worden door de adviseurs van de leden die gevoed zullen worden door in ieder geval drie werkgroepen voor de drie kernthema's. Het NPC bespreekt eveneens of er nog nieuwe thema's of kwetsbaarheden zijn die opgepakt dienen te worden. Voor het identificeren van belangrijke strategische thema's is belangrijk om met elkaar in gesprek te blijven, op ieder niveau. Daar zal ruimte voor gecreëerd worden door het organiseren van verschillende evenementen, zoals het Ondernemersdiner.

Monitoring
Om de voortgang te bewaken, zicht te hebben op de resultaten en effecten van de intensiveringen en besluiten te nemen over uitrol en borging van initiatieven is monitoring en evaluatie van belang. Om het jaar voert Bureau Beke een trendanalyse uit om te bepalen wat de belangrijkste ontwikkelingen zijn in criminaliteit tegen en via het bedrijfsleven. Ook wordt gebruik gemaakt van bestaande monitoren, zoals de Veiligheidsmonitor en de cybersecuritymonitor. Zowel dit actieprogramma als de inrichting van het PVO-bestel wordt geëvalueerd via de strategische evaluatieagenda van het ministerie van JenV. Het doel van deze agenda is te komen tot betere en meer bruikbare inzichten in de maatschappelijke toegevoegde waarde op belangrijke beleidsthema's, het meer benutten van dit inzicht en daarmee uiteindelijk hogere maatschappelijke toegevoegde waarde van beleid.

Middelen
Voor de uitvoering van dit actieprogramma is €2,5 miljoen per jaar beschikbaar. Projecten die de doelstellingen en acties van dit actieprogramma invulling geven kunnen in aanmerking komen voor financiering. Daarnaast is in de meerjarenbegroting van het ministerie van JenV €10 miljoen per jaar voor de Platforms Veilig Ondernemen opgenomen en kent het CCV een structurele financiering. Genoemde middelen zijn voor het vormgeven van de publiek-private samenwerking en de genoemde acties in dit programma. De aanpak fraude, witwassen en mainports kennen bijvoorbeeld separate financiering.

Bijlage 1.
Resultaten Actieprogramma Veilig Ondernemen 2019-2022

Pilots
- Regionaal kenniscentrum cybersecurity
- Samen Digitaal Veilig (cybersecurity MKB)
- Vertrouwenspersoon agrarisch ondernemers
- Mob Eyes (beveiligingsproduct)

Projecten
- Lokale projecten City Deal Lokale weerbaarheid cybercrime
- Campagne fout geld (horeca, MKB)
- Opschaling activiteiten Transport Facilitated Organized Crime
- PPS Intelligence (opschaling informatiedeling)
- Keurmerk Veilig Ondernemen (winkelgebied, bedrijventerrein, buitengebied)
- Theseus (veilig bedrijventerrein)
- Barrièremodel vakantieparken
- Verkenning vitale binnensteden
- Stappenplan katvangers
- Informatiedeling binnen de branches en met politie mobiel banditisme
- Cross-sectorale gegevensdeling (DPIA en vergunningaanvraag AP)

Onderzoek
- Samen criminaliteit bestrijden (criminaliteit tegen het bedrijfsleven)
- Gedragsverandering cybersecurity in het MKB
- Ketendoorlichting en gouden regels cyberweerbaarheid MKB
- Effectieve maatregelen om ondermijning bij logistieke dienstverleners tegen te gaan
- Verkenning en uitvoeringstoets verplichte registratie kentekenregister autohuurders
- Vastgoedcriminaliteit (vijf onderzoeken)
- Poortwachters
- Mobiel banditisme: signaleren en aanpakken
- Casuïstiek en interventies mobiel banditisme
- Haalbaarheidsonderzoek inzet sensing ten behoeve van veilige goederencorridors
- Cross-sectorale gegevensdeling

Kennisdeling en ontmoeting
- PPS-congres ‘Eén front tegen criminaliteit’
- Ondernemersdiner
- Webdossier vastgoedcriminaliteit incl. instrument screening
- Regionale talkshows ‘Crimineel verpand’
- Webinar ‘Georganiseerde criminaliteit op de rem’
- Handreiking rotte appels in brancheverenigingen
- Factsheet Toezicht en Handhaving op vakantieparken
- Expertsessies vakantieparken

Platforms Veilig Ondernemen
- Start doorontwikkeling tien regionale PVO’s met ondersteuning van een landelijk expertisecentrum

Bijlage 2.
Overzicht maatregelen Actieprogramma Veilig Ondernemen 2023-2026

Aanpak preventie cybercrime voor het bedrijfsleven

1. Voorlichtingsactiviteiten Digital Trust Center
2. Stimuleren gedragsverandering via samenwerkingsverbanden
3. Cyberweerbaarheidsnetwerken
4. Verkenning aanvullende acties

Aanpak georganiseerde ondermijnende criminaliteit

Weerbare mensen

5. Vertrouwenspersonen voor een aantal branches
6. Meer bekendheid vertrouwenslijn afpersing
7. Weerbaarheidstraining voor meerdere branches
8. Meer bewustwording in risicobranches via beroepsopleidingen
9. Afscherming adressen Handelsregister
10. Aanpak ondermijnende criminaliteit rondom vastgoed en vakantieparken
11. Beleidsagenda aanpak witwassen

Weerbare bedrijfsprocessen

12. Barrièremodellen voor extra branches
13. Onderzoek naar indicatoren van criminele inmenging in bedrijfsprocessen
14. Extra hulp bij screening voor ondernemers en gebruiksvriendelijker maken van bestaande tools

Weerbaar netwerk

15. Weerbare brancheorganisaties
16. Informatie- en gegevensdeling en juridisch steunpunt
17. Aanscherping wet- en regelgeving
18. Digitaal platform PPS tegen ondermijning
19. Vergroten netwerk
20. Versterken fenomeengerichte aanpak

Gebiedsgerichte aanpak vermogenscriminaliteit

21. Veilige bedrijventerreinen en winkelgebieden
22. Veilig buitengebied
23. Veilige binnensteden
24. Terugdringen winkeldiefstal
25. Terugdringen mobiel banditisme
26. Terugdringen overvallen
27. Terugdringen agressie en intimidatie
28. Terugdringen jeugdcriminaliteit

Doorontwikkelen platforms veilig ondernemen

29. Plan voor hoe we komende jaren bouwen aan een professionele organisatie ten behoeve van het effectief weerbaarder maken van ondernemers

Governance, monitoring en middelen

30. Bezien instellingsbesluit NPC en verkennen versterking van de samenwerking in de uitvoering van het programma

Deelnemende partijen Nationaal Platform Criminaliteitsbeheersing

Nederlandse Vereniging van Banken

Ministerie van Justitie en Veiligheid

MKB Nederland

POLITIE
« waakzaam en dienstbaar »

Ministerie van Economische Zaken en Klimaat

VNO NCW

TLN

VNG Vereniging van Nederlandse Gemeenten

Horeca Nederland

BOVAG

OPENBAAR MINISTERIE

Retail Veiligheids Overleg

VERBOND VAN VERZEKERAARS

December 2022
Coverfoto: Bart Maat