Actieprogramma

Veilig Ondernemen 2019-2022

Nationaal Platform Criminaliteitsbeheersing (NPC)

1 Inleiding

In het Nationaal Platform Criminaliteitsbeheersing (NPC) werken overheid en bedrijfsleven nauw samen om criminaliteit te voorkomen en terug te dringen. Dit doet het NPC door publiek-private samenwerking op nationaal, regionaal en lokaal niveau te stimuleren en - waar mogelijk - verder te verstevigen. Daarbij richt het platform zich zowel op de aanpak van criminaliteit *tegen* het bedrijfsleven, als ook op de aanpak van criminaliteit die het bedrijfsleven (onbewust) zelf *faciliteert*. Op een aantal geprioriteerde thema's - ondermijning, cyber(security) en mobiel banditisme – wil het NPC deze aanpak versterken: daartoe lanceert het in dit *Actieprogramma Veilig Ondernemen 2019-2022* concrete voorstellen.
De focus van de integrale aanpak ligt op de *gezamenlijke* opgave. Daarnaast blijft publiek-private samenwerking ook van belang om andere vormen van criminaliteit effectief terug te dringen.

Het NPC werkt vanuit de volgende uitgangspunten:

1. Het stimuleren van publiek-private samenwerking om criminaliteit tegen te gaan en het formuleren van prioriteiten bij de aanpak. Het NPC voert de centrale regie en heeft oog voor de samenhang van de verschillende activiteiten en prioriteiten;
2. Overheid en ondernemersorganisaties hebben een *gezamenlijk* doel voor ogen en werken daar gezamenlijk aan - elk uiteraard vanuit zijn eigen verantwoordelijkheid;
3. Preventieve maatregelen en repressie versterken elkaar.

Overheid en bedrijfsleven samen aan het werk

Het Nationaal Platform Criminaliteitsbeheersing (NPC) werd in 1992 opgericht. Het is een samenwerkingsverband tussen overheid en bedrijfsleven, dat zich richt op de aanpak van criminaliteit tegen het bedrijfsleven. Het NPC is samengesteld uit vertegenwoordigers van overheid en bedrijfsleven. De Minister van Justitie en Veiligheid is voorzitter van het platform. Naast het ministerie van Justitie en Veiligheid is ook het ministerie van Economische Zaken en Klimaat in het platform vertegenwoordigd. Ook politie, Openbaar Ministerie en gemeenten maken deel uit van het platform. Het bedrijfsleven wordt vertegenwoordigd door brancheorganisaties die gezamenlijk een goede afspiegeling van het bedrijfsleven vormen.

Het *Actieprogramma Veilig Ondernemen 2019-2022* draagt bij aan de doelstelling van het NPC om:

1. Het bedrijfsleven weerbaarder te maken tegen de risico's van (ondermijnende) criminaliteit;
2. Samenwerking tussen publieke en private partners te stimuleren en faciliteren om preventie te verbeteren;
3. Binnen bestaande kaders informatie-uitwisseling te stimuleren tussen publieke en private partners en gebruik te maken van innovatieve maatregelen;
4. Te zorgen voor schone bedrijfssectoren die criminaliteit niet faciliteren;
5. en daarmee een bijdrage te leveren aan een veiliger ondernemersklimaat en een veiligere samenleving.

2 Agenda voor de Toekomst

In 2016 is het *Actieprogramma Veilig Ondernemen 2017 - 2018* vastgesteld. Met dit Actieprogramma presenteerde het NPC voor het eerst sinds lange tijd weer een systematische aanpak van de criminaliteit gericht tegen het bedrijfsleven. Sindsdien is er veel in gang gezet. Tal van publieke en private organisaties op lokaal, regionaal en landelijk niveau zijn actief aan de slag gegaan met veilig ondernemen. Met voortvarendheid zijn diverse nieuwe projecten gestart om het bedrijfsleven veiliger te maken; reeds lopende veiligheidsprojecten werden geïntensiveerd.

Om de veiligheidsthema's voor het Actieprogramma 2019-2022 te bepalen is in 2018 het traject '*Agenda voor de toekomst*' gestart. Doel van dit traject was om ontwikkelingen in de criminaliteit *tegen* het bedrijfsleven, maar ook gefaciliteerd *door* bedrijfsleven, in kaart te brengen en op basis daarvan het vaststellen welke thema's integraal, publiek-privaat, de komende jaren moeten worden aangepakt. Bij dit traject zijn tal van publieke en private partijen betrokken, om draagvlak voor deze nieuwe veiligheidsthema's te verwerven onder de deelnemende partijen.

Uit het traject komt naar voren dat aandachtspunten anno 2019 niet meer worden gevormd door klassieke vormen van criminaliteit, maar door criminaliteit met een digitale component en criminaliteit die zich kenmerkt door een verwevenheid tussen onder- en bovenwereld (ondermijning). Deze ontwikkeling stelt het bedrijfsleven en de overheid voor nieuwe uitdagingen. De private sector en deskundigen hebben de volgende thema's als meest relevant benoemd:

a. Ondermijning
b. Mobiel banditisme
c. Cyber(security)

Deze onderwerpen zijn door het NPC in de vergadering van 18 december 2018 vastgesteld, om verder in dit Actieprogramma Veilig Ondernemen 2019-2022 uit te werken.

3 Uitwerking thema's Veilig Ondernemen

A Ondermijning

Aanleiding

Dat bij de aanpak van ondermijning de overheid het niet alleen kan is evident. Zonder betrokkenheid en medewerking van maatschappelijke partners is een overheidsaanpak - ook als deze eenduidiger en effectiever wordt georganiseerd - gedoemd te mislukken. Publiek-private samenwerking is in de aanpak van ondermijning dan ook noodzakelijk. De samenwerking moet ook worden bekeken vanuit het belang van een goed en integer handelsklimaat. Ondermijnende criminaliteit kan bedrijfstakken aantasten en hiermee leiden tot economische schade. Verder moet er het besef zijn dat ondermijnende criminelen deels gebruik maken van legale handelsactiviteiten en hierbij ook proberen bedrijven en branches aan te tasten op hun bijdrage om maatschappelijk verantwoord te ondernemen. Daarom is het belangrijk om de publieke private samenwerking deels ook te richten op facilitatoren: bedrijven/bedrijfstakken die, bewust of onbewust, de criminele industrie in hun activiteiten bijstaan. Verder zal het bedrijfsleven met zelfreinigende maatregelen komen. Zo kunnen ondernemers op een bedrijventerrein, die last hebben van criminele activiteiten en die hun vastgoed daardoor in waarde zien dalen, besluiten om samen met de overheid op te trekken, om zo hun weerbaarheid te vergroten. Samenwerking zoekt de overheid ook met (groepen) burgers of branches die zich te weer willen stellen tegen ondermijnende criminaliteit. Omdat als hun branche getroffen wordt, zijzelf daardoor getroffen worden, dan wel hun medewerkers in criminele zaken verzeild dreigen te raken. Publiek-private samenwerking (PPS) is dus een veelomvattend begrip.

Doel

De inzet van het Actieprogramma Veilig Ondernemen beoogt bij te dragen aan een effectieve en toekomstbestendige aanpak van de georganiseerde, ondermijnende criminaliteit en is aanvullend op de versterkingsplannen die door de RIEC's (Regionaal Informatie en Expertise Centra/Centrum) worden uitgevoerd. Doel is het terugdringen en beheersbaar maken en houden van de georganiseerde, ondermijnende criminaliteit in Nederland. Belangrijke stappen hierbij zijn: verbreding van het maatschappelijk draagvlak, de slagkracht van de overheid vergroten en het opwerpen van barrières voor criminele markten.

Acties

Het voorstel is om, met als achtergrond de werkwijze/businessmodellen van de criminele industrie, één PPS-agenda te ontwikkelen opgesteld door publiek en private partijen. De drie hierna genoemde teams en daaronder hangende projecten geven een eerste invulling aan het PPS-programma. Het idee is om per halfjaar een update van de PPS-agenda te maken.

1 Team "Wielen"

- De logistieke kant van de drugsindustrie: samen met TLN wordt in kaart gebracht hoe we bij de misbruik van (container)vervoer de samenwerking tussen overheid en bedrijfsleven kunnen verbeteren. Onderzoek moet uitwijzen wat effectieve maatregelen zijn om ondermijning bij logistiek dienstverleners tegen te gaan, zonder de logistieke processen te frustreren. Dit moet leiden tot brancheafspraken en aan overheidskant tot afspraken over geregisseerde handhaving.
- In samenwerking met BOVAG komen er maatregelen om ondermijning in de mobiliteitssector tegen te gaan, onder meer ten aanzien van autoverhuur.
- Eveneens voor de logistieke kant van de drugsindustrie: het lopende project met de postpakkettenbranche wordt doorontwikkeld, met onder meer als doel barrières op te werpen voor het verzenden van drugs via de postpakketten. Mede door de inrichting van een gezamenlijke informatiecel dient deze aanpak als voorbeeld van een publiek-private samenwerking.

2 Team "Locaties"

- Voor productielocaties in de drugsindustrie ontwikkelen we, samen met MKB-Nederland, een model voor publiek-private samenwerking op bedrijventerreinen. Het gaat om de uitbouw van het Keurmerk Veilig Ondernemen en een koppeling tussen parkmanagement en veiligheidsmaatregelen op een

bedrijventerrein. Behalve productielocaties zijn ook verblijfplaatsen voor ondermijnende criminelen van belang om criminele activiteiten te kunnen organiseren.

- We ontwikkelen een aanpak om barrières tegen malafide verhuurders op te werpen.
- Onderzoek moet inzicht geven langs welke weg particuliere vastgoedeigenaren en woningcorporaties gewaarschuwd kunnen worden voor criminele intenties van potentiële gebruikers. De resultaten, die naar verwachting eind 2019 gereed zijn, bieden handvatten voor aanvullende maatregelen.
- Nauwe samenwerking met de Koninklijke Notariële Beroepsorganisatie (KNB) en Nederlandse Vereniging van Makelaars (NVM) moet voorkomen dat mensen of organisaties vastgoed kunnen verwerven met crimineel geld.
- Met betrekking tot productielocaties is er een aanpak opgezet, gericht op publiek-private barrières in het landelijk gebied. Het gaat hier om het doorontwikkelen van het keurmerk Veilig Agrarisch Ondernemen, met daarbij handhaving op maat en het zoeken c.q. mogelijk maken van positieve herbestemming van agrarisch vastgoed.
- Voor de aanpak in wijken en buurten gaat het zowel om repressie (productielocaties) als om preventie (resocialisatie en wijkaanpak). Een coalitie met woningcorporaties dient zich aan in het verlengde van succesvolle initiatieven zoals die in sommige steden al lopen. Samen met de vereniging van woningcorporaties AEDES worden maatregelen genomen die lokaal kunnen worden uitgerold.

3 Team “Schone Branches”

- Branches en brancheverenigingen zijn zeer deskundig op hun terrein en weten alles over een bepaald segment. Dit kan heel handig zijn voor criminelen, dan wel (potentieel) kwaadwillende leden, maar het levert ook informatie op voor gemeenten en handhavende diensten. Branchespecifieke wet- en regelgeving en branchespecifieke informatie gaan we gebruiken om zicht te krijgen op malafide ondernemers. De branche wil geen foute lieden ongemerkt lid laten worden en wil ook niet dat er misbruik wordt gemaakt van het lidmaatschap. Een schone en betrouwbare brancheorganisatie is zowel voor de branche als voor de overheid van belang.
- De resultaten van de pilot met de kappersbranche in RIEC Midden-Nederland zullen worden gebruikt voor landelijke afspraken. Ook gaan we de samenwerking zoeken met andere branches, zoals BOVAG, vastgoed en horeca.
- Er komen allerlei instrumenten, zoals integriteittoetsen en mogelijke keurmerken, die kunnen worden gebruikt om te voorkomen dat “rotte appels” lid kunnen worden van een brancheverenigingen. “Rotte appels” die al lid zijn, moeten uit de brancheverenigingen kunnen worden gezet. Zo doet de branche aan zelfreiniging en blijft ze gezond en betrouwbaar voor haar eigen leden en voor de overheid.
- Ook gemeenten kunnen hun steentje bijdragen. Door bestuurlijke maatregelen te nemen en de APV aan te passen kunnen zij de aanwas van kwetsbare branches binnen hun gemeentegrenzen verstoren. Met het oog hierop zullen voor het einde van 2019 vijf proeftuinen starten om de weerbaarheid van branches en gemeenten te vergroten.

B Mobiel Banditisme

Aanleiding

Nederland is, ook in vergelijking met andere Europese landen, voor mobiele bendes uit het buitenland een heel aantrekkelijk land. De mobiele dadergroepen ervaren de pakkans als laag en er zijn legio mogelijkheden om hun stelselmatige vermogensdelicten te plegen. In binnen- en buitenland zijn er aanwijzingen dat een groot deel van de georganiseerde vermogenscriminaliteit vaak wordt gepleegd door deze internationaal opererende dadergroepen. Bestrijding van mobiel banditisme vereist, naast de snelle operationele aanpak van gepleegde delicten, dus ook vooral een meer fenomeengerichte en internationaal georiënteerde aanpak.

Mobiel banditisme is een paraplubegrip voor het stelselmatig en in georganiseerd verband plegen van vermogensdelicten, zoals auto-, lading-, en winkeldiefstal, auto- en woninginbraak, zakkenrollerij en straatroof, door rondtrekkende dadergroepen die zowel in Nederland als in andere landen actief zijn. De samenstelling van deze dadergroepen wisselt en hun verblijfplaats is vaak onbekend. Door de aard en omvang van de delicten heeft mobiel banditisme een grote impact op de samenleving. De delicten die mobiele bendes plegen hebben een groot en direct effect op burgers: het gaat vaak om zogenoemde *high impact* crimes. Ook het midden- en kleinbedrijf is regelmatig slachtoffer van de vermogensdelicten. Het OM schat de economische schade van deze vorm van criminaliteit op 2,19 miljard euro per jaar. De schade van winkeldiefstallen alleen al loopt in de honderden miljoenen euro's, volgens Detailhandel Nederland.

Het NPC heeft reeds in het Actieprogramma Veilig Ondernemen 2017-2018 mobiel banditisme als actiethema benoemd. De uitwerking hiervan heeft onder meer geleid tot het instellen van een Taskforce Mobiel Banditisme. Deze Taskforce is een publiek-privaat samenwerkingsverband, waarin het lokaal bestuur, politie, OM, branches en het departement vertegenwoordigd zijn. In het Actieprogramma 2019-2022 is dit thema opnieuw opgenomen, vanwege het grote belang dat het NPC hecht aan een goede, integrale aanpak van deze vorm van criminaliteit.

Doel

Doel van de Taskforce Mobiel Banditisme is, door een stevige aanpak, Nederland onaantrekkelijk te maken als delictgebied voor mobiele dadergroepen. Willen we deze samenhangende en integrale aanpak doen slagen, dan is het van belang een gemeenschappelijk gevoel van maatschappelijke urgentie te creëren. Dit krijgt onder meer gestalte door dit thema op te nemen in zowel de Veiligheidsagenda 2019-2022 als het Actieprogramma Veilig Ondernemen. Ook hebben we, met alle betrokken organisaties, een integraal en richtinggevend Actieprogramma Integrale aanpak Mobiel Banditisme 2018-2020 opgesteld dat ten grondslag ligt aan de gezamenlijke aanpak. Het actieprogramma wordt de komende jaren uitgevoerd onder regie van de Taskforce.

Acties

De Taskforce werkt met een Actieprogramma Integrale aanpak Mobiel Banditisme 2018-2020 geënt op het barrièremodel mobiele bendes dat is opgesteld in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Dat betekent dat er per fase binnen de modus operandi van bendes (bijvoorbeeld de inreis in Nederland, accommodatie of de opslag van gestolen goederen) wordt bekeken welke barrières opgeworpen kunnen worden om het de bendes zo moeilijk mogelijk te maken. Zo ontstaat er een compleet pakket aan maatregelen dat mobiele bendes in alle facetten van hun werkwijze raakt – zowel preventief als repressief. Behalve aan de uitvoering van de maatregelen uit het barrièremodel werkt de Taskforce aan de volgende acties:

1. **Landelijke informatievoorziening en (internationale) gegevensuitwisseling**
   Informatiecoördinatie is van cruciaal belang om regie te geven aan de aanpak van mobiel banditisme. Een solide aanpak van mobiel banditisme kan dan ook alleen slagen als de partners zich een betere informatiepositie verwerven. Door de mogelijkheden van (internationale) informatie-uitwisseling beter te benutten, kunnen de mobiele daders en dadergroepen uit de anonimiteit worden gehaald. Dat maakt het mogelijk hen in EU-verband effectiever op te sporen en te vervolgen. Ook private (branche) organisaties hebben relevante informatie voorhanden die nuttig is bij het maken van keuzes in de aanpak van mobiel banditisme. Daarom wordt ook de informatie-uitwisseling tussen private organisaties en de overheid versterkt. Bijvoorbeeld om winkeliers te kunnen waarschuwen voor rondtrekkende groepen en om daders van criminaliteit te kunnen tegenhouden.

2. **Bestuurlijke aanpak**
   Gemeenten zijn soms ongewild facilitator van mobiele bendes: onder andere overbewoning, spookbewoning, zwarte markten, opslagboxen en vakantieparken bieden mobiele bendes de gelegenheid om hun criminele activiteiten voort te zetten. Samenwerking met én tussen gemeenten is dus cruciaal voor een succesvolle aanpak. De Taskforce wil inzetten op meer bestuurlijke awareness en urgentie rondom mobiel banditisme en het lokaal bestuur betrekken als partner bij de aanpak waar nodig.

C Cybersecurity

Aanleiding

In de Agenda voor de Toekomst is eind 2018 door de meeste ondernemers (94%) cybersecurity benoemd als zeer belangrijke vorm van (aan te pakken) criminaliteit. Ondernemers vinden een gemeenschappelijke aanpak van cybercrime van belang. In 2018 hebben internetcriminelen bij ruim de helft (52%) van het MKB geprobeerd om geld of data buit te maken. Onderzoek in de regio Limburg toont aan dat 39% van de MKB-ers het nog steeds onwaarschijnlijk acht dat ze slachtoffer worden van cybercriminaliteit, dat 32% geen drijfveer heeft om zich met cybercriminaliteit bezig te houden en dat 60% aangeeft geen idee te hebben hoe leveranciers omgaan met hun gegevens.

Een gecoördineerde aanpak blijft noodzakelijk om de effectiviteit en doelmatigheid van de initiatieven te optimaliseren, kennis en ervaring te bundelen en fragmentatie te voorkomen. Op departementaal niveau werkt het ministerie van JenV in de aanpak van cybersecurity in het bedrijfsleven nauw samen met het ministerie van EZK.

Doel

Ondernemers uiten een duidelijke hulpbehoefte, maar het blijkt in de praktijk moeilijk om ondernemers ook daadwerkelijk aan te zetten tot actie. Bedrijven, en met name MKB-ers, hebben vaak niet de capaciteit, de kennis en hulpbronnen om zich te weren tegen cyberaanvallen en worden daarom relatief vaak slachtoffer. Veiligheid in het digitale domein kan alleen in samenwerking met, en voor een belangrijk deel ook door, het bedrijfsleven vorm krijgen. Publiek-private samenwerking staat daarom aan de basis van de Nederlandse cybersecurity aanpak.

De afgelopen jaren is er veel geïnvesteerd in de bewustwording van ondernemers. De komende jaren willen we daarnaast meer specifiek gaan inzetten op het stimuleren van ondernemers om preventieve maatregelen te nemen, om hun cyberweerbaaheid te vergroten.

Acties

Een gecoördineerde aanpak van cyberveiligheid met het bedrijfsleven is belangrijk om de cybersecurity te vergroten. Een platform met onder meer VNO-NCW / MKB-Nederland, Platform Veilig Ondernemen (PVO), Nationaal Cyber Security Centrum (NCSC), Economische Zaken en Klimaat / Digital Trust Centre (EZK/DTC), Transport en Logistiek Nederland (TLN) en Detailhandel Nederland (DHN) gaat zich de komende periode richten op de uitvoering van de volgende onderzoeken en initiatieven:

1. **Gedragsexperiment “Human Factors in cybersecurity in het MKB”**
   Veiligheidsmaatregelen worden door ondernemers gezien als iets dat op orde moet zijn, dat in potentie negatieve gevolgen kan hebben, maar waarover je je niet echt druk hoeft te maken. Veel MKB-ers zijn vooral bezig met hun onderneming en zijn minder ontvankelijk voor informatie over cybersecurity.
   Het gedragsexperiment wordt uitgevoerd in samenwerking met (onder meer) het lectoraat cybersecurity MKB. Aan de hand van proeftuinen bij verschillende

groepen MKB-ers biedt het gedragsexperiment inzicht in de kansen voor gedragsbeïnvloeding, de ontvankelijkheid en motivatie bij MKB-ers en hun medewerkers, alsmede wetenschappelijk onderbouwde gedragsinterventies. De uitkomsten van het onderzoek zijn toepasbaar in andere branches.

2. Gedragsexperiment "Phishing in het MKB"

In samenwerking met het ministerie van JenV, het Regionaal Platform Criminaliteitsbeheersing Noord Holland, Politie, CCV en PVO's stelt EKZ/DTC, in lijn met de landelijke campagne, een gratis phishingtest beschikbaar voor het MKB. In deze test ervaren bedrijven wat een phishingaanval inhoudt en krijgen tips hoe ze in de toekomst phishing e-mails beter kunnen herkennen.

Doel van het experiment is om (de medewerkers van) de deelnemende bedrijven bewust te maken van de risico's van phishing en weerbaar te maken tegen phishingaanvallen. De uitkomsten van het experiment worden als "best practice" ingezet voor andere branches.

3. Ketendoorlichting

Alle bedrijven zijn onderdeel van een of meerdere ketens, waarin bedrijven (ook) via internet onderling zijn verbonden. Behalve beter inzicht in de risico's en mogelijke maatregelen op individueel en brancheniveau, is ook inzicht op ketenniveau van belang. Tenslotte loopt de cyberveiligheid van een bedrijf of branche ook gevaar, als de ketenpartners niet - of minder - weerbaar zijn.

Om deze problematiek in kaart te brengen, gaan we in nauwe samenwerking met EZK/DTC en een brancheorganisatie de mogelijkheid verkennen van een keten-/ sectordoorlichting. Het idee is om een private keten (met een Nederlands moederbedrijf) van begin tot eind door te lichten, om te achterhalen wat de ketenrisico's zijn, wat we kunnen leren en hoe we een dergelijke keten weerbaar kunnen maken.

De ketendoorlichting wordt eerst verkennend onderzocht om te bepalen of binnen het bedrijfsleven behoefte is aan een doorlichting. Naar aanleiding van het verkennend onderzoek krijgt de ketendoorlichting verder vorm.

4. Ontwikkelen van regionale kenniscentra

EZK/DTC ondersteunt ondernemers via een digitaal platform met actuele informatie en betrouwbare adviezen. Omdat het MKB moeilijk te bereiken is als het gaat om preventieve activiteiten, zijn regionale kenniscentra gewenst om de digitale veiligheid op regionaal niveau aan te vullen en te versterken.

Regionale kenniscentra maken het mogelijk om de benadering van de MKB-ondernemers fijnmaziger te organiseren. Dit is vooral van belang om een vertrouwensrelatie met de ondernemer te kunnen opbouwen.

Bij wijze van pilot voor andere regionale kenniscentra zal het Expertisecentrum Limburg de komende tijd een regionaal kenniscentrum uitbouwen, met onder meer de volgende activiteiten:

- Experimenteren met netwerken in combinatie met korte, gerichte campagnes;
- Ontwikkelen van een cyber-audit voor ondernemers;
- Beschikbaar stellen van leer- en instructiemateriaal voor ondernemers;
- Opbouw van een netwerk van lokale IT-bedrijven.
- Aanbieden van online securitytools;
- Ontwikkelen Cyberkeurmerk (in samenwerking met CCV).

5. Versterken internationale samenwerking

Het digitale domein is per definitie niet gebonden aan landsgrenzen. Om als Nederland te kunnen bijdragen aan internationale vrede en veiligheid in het digitale domein (Nederlandse Cyber Security Agenda), is vanuit het NCSC aandacht voor de sectoren die voor de samenleving van cruciaal belang zijn (de vitale infrastructuur). Nederland is een van de meest gedigitaliseerde landen ter wereld en een van de voorlopers op het gebied van cyberveiligheid in het bedrijfsleven. Vooral de rol van het MKB is internationaal onderbelicht. Nederland kan als voorloper de internationale samenwerking proberen te versterken op het gebied van cybersecurity van het MKB. Het komende jaar zal via bestaande internationale gremia het belang van cybersecurity van ondernemers worden geagendeerd, met als doel de weerbaarheid van ondernemers internationaal te versterken.

6. Eenvoudige tools ontwikkelen en informatie-toegang vereenvoudigen

Het vereenvoudigen van aangifte, de informatietoegang en tools, onder meer door:

- De rol van het DTC verder te versterken als hét platform vanuit de overheid met duidelijke dienstverlening ten behoeve van het bedrijfsleven;
- Het ontwikkelen van een digitaal aangiftemeldpunt;
- Het ontwikkelen van een app met vragen, een weerbaarheidsscore en informatie over de weerbaarheid. De app levert een rapport op voor de ondernemer en een geanonimiseerd overzicht van de data;
- Het ontwikkelen van een *riskcalculator*. De riskcalculator is een dashboard waarop de impact/oorzaak van incidenten wordt weergegeven. Hierdoor kunnen bedrijven in deze branche zien waar zij op moeten inzetten.

4 Strategie

Het NPC versterkt de onderlinge, integrale samenwerking. De focus van de integrale aanpak ligt op de gezamenlijke opgave. Van daaruit bekijken we hoe een netwerk zich het beste kan organiseren; de specifieke opgave bepaalt de samenwerkingstafel. Dit zorgt ervoor dat er rond een opgave een divers netwerk ontstaat van organisaties, ondernemers en maatschappelijke organisaties die zich met de opgave verbonden voelen. Het gaat er niet om wie vanuit zijn formele rol of verantwoordelijkheid betrokken dient te zijn, maar wie een zinvolle bijdrage kan leveren aan het *aanpakken* van de opgave. Door samen te werken kan het effect van de afzonderlijke inspanningen worden vergroot en kunnen we concrete resultaten boeken!

Gerichte interventies

In de uitvoering van het actieprogramma richt het NPC zich op het vinden en toepassen van effectieve interventiestrategieën, gericht op het bestrijden van de (ondermijnende) criminaliteit. Door de (lokale) problematiek in kaart te brengen, kunnen binnen een integrale aanpak passende maatregelen worden genomen om deze aan te pakken. Een belangrijke opdracht voor het NPC is om de verschillende mogelijkheden van publieke en private partners en van de beschikbare repressieve en preventieve maatregelen bij elkaar te brengen rond een specifiek thema - en om deze vervolgens optimaal te benutten. Verder is het belangrijk dat de weerbaarheid van ondernemers en het zelfreinigend vermogen van branches worden vergroot.

Activiteiten worden bij voorkeur dicht bij de ondernemer georganiseerd. De overheid moet een betrouwbare partner zijn voor het bedrijfsleven en *vice versa*.
De afstand tot de lokale ondernemer moet kleiner worden. Investeren in de onderlinge relatie is belangrijk. Zo kunnen we in de nabije toekomst gestalte geven aan een effectieve aanpak van de uitdagingen waarvoor het bedrijfsleven zich gesteld ziet. Via publiek-private proeftuinen op lokaal en regionaal niveau worden de opgaven aangepakt en zichtbaar en tastbaar gemaakt voor de ondernemers en lokale overheid.

Door de afstand tussen overheid en ondernemer te verkleinen zal ook de meldings- en aangiftebereidheid stijgen. Zo ontstaat er meer zicht op de criminaliteit waar het bedrijfsleven mee te maken heeft.
Opgavegericht werken maakt het mogelijk themagericht successen te boeken en systeemfouten te identificeren. Het is vervolgens de taak van het NPC om een vervolg aan deze successen te geven en urgentiebesef te creëren voor het oplossen van systeemfouten.

Aanpak op verschillende niveaus

De uitingsvormen en ook de inbedding van (ondermijnende) criminaliteit tegen het bedrijfsleven – en daarmee ook de eerste aangrijpingspunten voor een aanpak – liggen vaak op het lokale niveau. Dáár wordt de problematiek immers ervaren - door de gevestigde ondernemers en publieke partners. Het is dan ook daar dat de ontwikkeling en invoering van maatwerkoplossingen moet plaatsvinden. Om dat proces te ondersteunen en te optimaliseren is het noodzakelijk dat op regionaal en lokaal niveau een effectieve structuur functioneert van publiek-private samenwerking, via PVO's en de RIEC's. In de PVO's slaan ondernemers, gemeenten, politie en OM de handen ineen om de criminaliteit tegen en in het bedrijfsleven terug te dringen. Het PVO werkt als stimulator, facilitator en makelaar in het regionale en lokale veiligheidsdomein en heeft daarnaast een signalerings- en uitvoeringstaak met betrekking tot de aan te pakken problematiek.
De PVO's zorgen ervoor dat de veiligheidsvraagstukken worden vertaald naar een concrete aanpak, gericht op de oplossing van het probleem.

5 Informatie-uitwisseling

Een belangrijk aspect in de publiek-private samenwerking is het delen van informatie en kennis. Dit biedt immers meer inzicht in criminele fenomenen. Op basis van het doorgronden c.q. begrijpen van het criminele fenomeen kan vervolgens worden nagegaan hoe we barrières kunnen opwerpen in het publieke en private domein om de criminaliteit tegen te gaan. De informatie levert ook inzicht op hoe de private sector weerbaarder gemaakt kan worden tegen criminele invloeden van buitenaf.

Een instrument dat hierbij in eerdere proeftuinen is gebruikt en waarmee ervaring is opgedaan is Intelligence Driven Security (IDS). Binnen IDS wordt op basis van signalen met betrekking tot een specifieke criminaliteitsvorm – binnen de wettelijke mogelijkheden – informatie verzameld en geanalyseerd om de criminaliteit beter te doorgronden en achterliggende netwerken bloot te leggen. Pas nadat duidelijk is hoe een fenomeen in elkaar zit, heeft interveniëren echt zin. Dan kan gekeken worden naar mogelijkheden voor een aanpak vanuit de verschillende partijen. Een aanpak kan in theorie variëren van beter inzicht *in* en awareness *van* de problematiek en het opwerpen van barrières om criminaliteit tegen te gaan tot opsporing en vervolging.

De kern zit dus in het combineren van kennis en kunde en het doorgronden van het criminele werkproces.
De private partner heeft met toepassing van dit instrument beter zicht op incidenten, trends en kennis van (de invloed van criminaliteit op) het bedrijfsvoeringproces. De overheid krijgt door de samenwerking zicht op de gelegenheidsstructuren en de drijvende krachten binnen het criminele fenomeen. Gezamenlijk komt er zicht op het fenomeen en de mechanismen om barrières te kunnen opwerpen. De private partners worden minder kwetsbaar, terwijl publieke partners hun capaciteit effectiever kunnen inzetten en in de positie komen om bestuurlijke, financiële of strafrechtelijke interventies te plegen. In de uitvoering van de acties uit dit Actieprogramma Veilig Ondernemen zal het concept van IDS, waar mogelijk, vaker worden toegepast door middel van een infocel PPS. Deze cel fungeert als een operationeel samenwerkingsverband en kenmerkt zich door een klein team van analisten, dat in een *pressure cooker*-achtige omgeving intensief en kortstondig een fenomeen kan doorgronden dat valt binnen de agenda van het NPC.

Niet alleen tussen publieke partijen en tussen publieke en private partijen, maar ook tussen private partijen onderling is gegevensuitwisseling wenselijk. Daarbij kan het nodig zijn om over de grenzen van de verschillende branches heen, dus cross-sectoraal, persoonsgegevens over (potentiële) fraudeurs te kunnen delen. Op deze wijze kunnen we voorkomen dat burgers en bedrijven (opnieuw) slachtoffer worden. Binnen het wettelijk kader van AVG en UAVG is cross-sectorale gegevensdeling tussen private partijen mogelijk mèt vergunning van de Autoriteit Persoonsgegevens. Op basis van initiatieven van VNO-NCW / MKB-Nederland gaan we ervaring opdoen met de cross-sectorale gegevensdeling. Deze ervaringen kunnen mogelijk leiden tot nieuwe wetgeving.

6 Governance

De samenwerkingsvorm die wordt gekozen dient een doel en is geen vast gegeven. Publiek-private netwerken zijn flexibel en fluïde. De aard van het probleem en het beoogde effect zijn bepalend voor de partners die bij de samenwerking worden betrokken. Dit kan gevolgen hebben voor de samenstelling van het NPC, maar ook voor de samenstelling of werkvorm van de werkgroepen. Daarnaast moet het NPC gedurende de looptijd van het nieuwe Actieprogramma oog hebben voor ontwikkelingen en daar desgewenst op in (kunnen) spelen. Het NPC is richtinggevend en eindverantwoordelijk voor de totstandkoming en uitvoering van dit Actieprogramma Veilig Ondernemen. Het NPC stelt de projectplannen vast en wordt gedurende de uitvoering van de projecten geïnformeerd over de voortgang en neemt beslissingen over de belangrijkste mijlpalen.

Naar aanleiding van ervaringen met de Taskforce Overvallen en de sinds vorig jaar ingestelde Taskforce Mobiel Banditisme kiezen we ervoor om voor elk thema een bestuurlijk platform in te stellen dat verantwoordelijk is voor de voortgang en uitvoering. Deze hebben tot doel in korte tijd voor deze opgaven een aantal acties en ontwikkelingen te forceren. Een taskforce biedt de mogelijkheid om een zetje in de goede richting te geven, door de urgentie van het probleem aan te tonen en tegelijk voor voldoende draagvlak te zorgen. Ook kunnen gewenste doelen goed worden afgestemd op de beschikbare middelen en worden de inspanningen op een gecoördineerde en gestructureerde manier gerealiseerd.

Er is al een Taskforce Mobiel Banditisme. Deze wordt de komende jaren gecontinueerd. Voor de aanpak van ondermijning is er het Strategisch Beraad Ondermijning (SBO), waarbij ook VNO-NCW / MKB-Nederland wordt uitgenodigd, daar waar het gaat om uitvoering van de PPS-agenda. Voor het thema Cybersecurity zal nog worden bekeken welk platform het beste kan worden benut om uitvoering te geven aan de acties uit dit Actieprogramma.

De Stuurgroep / Taskforce krijgt tot taak:

a. het signaleren van knelpunten bij de integrale aanpak van betreffende thema, dan wel fenomeen, en het formuleren van maatregelen om deze knelpunten op te lossen;
b. het periodiek monitoren van de aanpak van het onder a. bedoelde thema en de bijbehorende delicten. waar nodig obstakels in de uitvoering wegnemen en aanvullende maatregelen formuleren;
c. het onderhouden van contacten met relevante partijen in het veld die niet in de Taskforce zijn vertegenwoordigd;
d. het informeren van het NPC over de voortgang van de werkzaamheden van de Taskforce, jaarlijks vóór 1 november;

e. het formuleren van een voorstel voor de borging van de aanpak van onder a bedoelde delicten nadat de Taskforce zijn werkzaamheden heeft voltooid.

Elk thema kent een werkgroep die verantwoordelijk is voor de uitvoering van het Actieprogramma. De werkgroep initieert projecten en bewaakt het niveau en voortgang daarvan. De werkgroep rapporteert vier keer per jaar aan het bestuurlijke platform. Daarnaast zorgt de werkgroep ervoor dat de ervaringen, kennis en voortschrijdend inzichten geborgd en benut kunnen worden binnen publieke en private structuren.
De samenstelling van de leden van de werkgroep wordt door de opgave bepaald.

7 Ontwikkelingen criminaliteit bedrijfsleven

Gedurende de looptijd van dit Actieprogramma Veilig Ondernemen is het van belang om zicht te krijgen en te houden op de criminaliteitsontwikkeling in het bedrijfsleven. Het onderzoek 'Agenda voor de Toekomst' vormt de basis voor dit Actieprogramma. In dit onderzoek zijn door middel van deskresearch, een enquête onder ondernemers en paneldiscussies met onder meer ondernemers, wetenschappers en vertegenwoordigers van de overheid de belangrijkste criminaliteitsontwikkelingen in het bedrijfsleven in beeld gebracht. Doel is om dit onderzoek eens in de twee jaar te herhalen. Enerzijds om de voortgang van de aanpak van huidige speerpunten te volgen, anderzijds om oog te hebben voor nieuwe ontwikkelingen in de criminaliteit tegen het bedrijfsleven, maar ook in die criminaliteit die door het bedrijfsleven wordt gefaciliteerd.

Los van deze periodieke onderzoeken ondersteunt het NPC diverse brancheorganisaties in het laten uitvoeren van onderzoek om kennis van bepaalde criminaliteitsfenomenen op te bouwen. Deze kennis vormt vervolgens de basis om te komen tot specifieke oplossingen.

8 Organisatie

Monitoring

Alle projecten en bijbehorende acties uit dit Actie-programma zullen gedurende de looptijd nauwgezet worden gemonitord. Om de effecten van het totale programma te waarborgen zal het NPC per kwartaal de voortgang van de projecten bespreken.

Communicatie

Partijen stemmen van tevoren met elkaar af welke boodschappen zij vanuit de verschillende projecten uitdragen naar de media.

Vragen?

Neem contact op met Stefan Scheeringa via s.j.scheeringa@minjenv.nl of bel 06 - 130 332 07

of met Els Prins via prins@vnoncw-mkb.nl of bel 06 - 113 517 23

Cover foto:

Bedrijventerrein in Alblasserwaard.

juli 2019 | 122901

Ministerie van Justitie en Veiligheid

Ministerie van Economische Zaken en Klimaat

MKB Nederland

OPENBAAR MINISTERIE

VNG Vereniging van Nederlandse Gemeenten

Detailhandel Nederland

VNO NCW

Horeca Nederland

Nederlandse Vereniging van Banken

VERBOND VAN VERZEKERAARS

POLITIE

« waakzaam en dienstbaar »