Actieprogramma

Veilig Ondernemen 2017-2018

Nationaal Platform Criminaliteitsbeheersing (NPC)

1 Uitgangspunten en doel

Criminaliteit tegen en gefaciliteerd door bedrijven wordt gericht aangepakt. Het Nationaal Platform Criminaliteitsbestrijding (NPC), waarin overheid en bedrijfsleven samenwerken aan het terugdringen van criminaliteit tegen bedrijfsleven, wil de aanpak versterken door het stimuleren en verstevigen van publiek-private samenwerking op nationaal, regionaal en lokaal niveau. Daarbij richt het NPC zich zowel op de aanpak van criminaliteit *tegen* het bedrijfsleven, als ook op de aanpak van criminaliteit *gefaciliteerd* door het bedrijfsleven. De verruiming naar laatstgenoemd fenomeen is belangrijk gezien de gelegenheidsstructuren die het bedrijfsleven soms ongewild en onwetend biedt bij het faciliteren van ondermijnende criminaliteit.

Het NPC werkt vanuit de volgende uitgangspunten:

1. Het NPC stimuleert publiek-private samenwerking om criminaliteit tegen te gaan en formuleert prioriteiten bij de aanpak. Het NPC heeft de centrale regie en oog voor samenhang van de verschillende activiteiten en prioriteiten;
2. Overheid en ondernemersorganisaties hebben een gezamenlijk doel en werken daar samen aan, elk vanuit hun eigen verantwoordelijkheid;
3. Preventieve maatregelen en repressie versterken elkaar.

Actieplan veilig ondernemen 2017 - 2018

Het actieplan veilig ondernemen 2017-2018 draagt bij aan het doel 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 tussen publieke en private partners te stimuleren en gebruik te maken van innovatieve maatregelen;
4. Zorgen voor schone bedrijfssectoren die criminaliteit niet onbewust faciliteren;
5. en daarmee een bijdrage te leveren aan een veiliger ondernemersklimaat en een veiliger samenleving.

Dit actieprogramma presenteert acties op thema's waar het NPC de komende twee jaar de focus legt en waarmee ze bovenbeschreven doelen wil bereiken. Hiermee wordt het inzicht vergroot in de criminaliteitsontwikkeling in het bedrijfsleven, worden goede voorbeelden makkelijk beschikbaar gesteld en kan concrete hulp worden geboden bij een lokale maatwerkaanpak.
Een veilige onderneming, bedrijventerrein of winkelstraat ontstaat alleen als er samen aan gewerkt wordt.

Overheid en bedrijfsleven samen aan het werk

Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een in 1992 opgericht samenwerkingsverband tussen overheid en bedrijfsleven gericht op het aanpakken van criminaliteit gericht tegen het bedrijfsleven. Het NPC is samengesteld uit vertegenwoordigers van overheid en bedrijfsleven. De Minister van Veiligheid en Justitie is voorzitter van het platform. Naast het ministerie van Veiligheid en Justitie is het ministerie van Economische Zaken in het platform vertegenwoordigd, samen met de politie, het Openbaar Ministerie en de gemeenten. Namens het bedrijfsleven maken brancheorganisaties, die een dwarsdoorsnede van het bedrijfsleven vertegenwoordigen, deel uit van het platform.

Ambassadeurs

In het NPC zijn ambassadeurs benoemd voor de verschillende thema's. De ambassadeur voelt zich verantwoordelijk voor het stimuleren van de integrale aanpak met partners en de te bereiken doelstellingen. De ambassadeur is op de hoogte van de voortgang en vormt voor het NPC het aanspreekpunt voor het betreffende thema.

Cybersecurity	*Michaël van Straalen (VNO-NCW / MKB)*
Afpersing	*Lodewijk van der Grinten (KHN)*
Mobiele bendes	*Henk van Essen (NP)*
Heling	*Gerard van Breen (DHN)*
Transportcriminaliteit	*Arthur van Dijk (TLN)*
Faillissementsfraude	*Chris Buijink (NVB)*
Ondermijning	*Roger Bos (OM)/Michaël van Straalen (VNO-NCW/MKB)*

2 Probleem**beschrijving**

Criminaliteit tegen ondernemers en het ongewild faciliteren van criminaliteit door het bedrijfsleven is een actueel probleem. Via de fysieke én de digitale weg verliezen bedrijven inmiddels jaarlijks miljarden euro's en worden criminele gelegenheidsstructuren in stand gehouden. Dit vormt een risico voor de groei, werkgelegenheid en soms zelfs de continuïteit van bedrijven en de maatschappij als geheel. De laatste jaren is binnen het bedrijfsleven de bewustwording toegenomen ze geconfronteerd wordt met georganiseerde criminaliteit.
De georganiseerde of ondermijnende criminaliteit roert zich steeds intensiever in het private en publieke domein en is een steeds groter wordend maatschappelijk probleem. Ondermijnende criminaliteit is vooral een economisch gedreven maatschappelijk fenomeen waarbij de verwevenheid van de onderwereld met de boven-wereld een belangrijk kenmerk is.

Dit heeft gevolgen voor het bedrijfsleven. De economische activiteiten van bonafide ondernemers worden aangetast door de criminele praktijken van malafide ondernemers. Deze zullen zich bij de keuze voor de locatie van vestiging en activiteiten laten leiden door de mogelijkheden die de plaatselijke omgeving hen bieden. Net als bij legale sectoren van onze economie geldt hier dat het succes vooral afhankelijk is van een gunstig vestigings- en investeringsklimaat. [1] Daarnaast faciliteren bedrijven en ondernemers soms onbewust criminele processen en vormen ze een essentiële gelegenheidsstructuur voor criminele markten. Criminele ondernemers maken graag gebruik van legale voorzieningen en structuren.
Dat ontwricht de economische activiteiten van bonafide bedrijven.

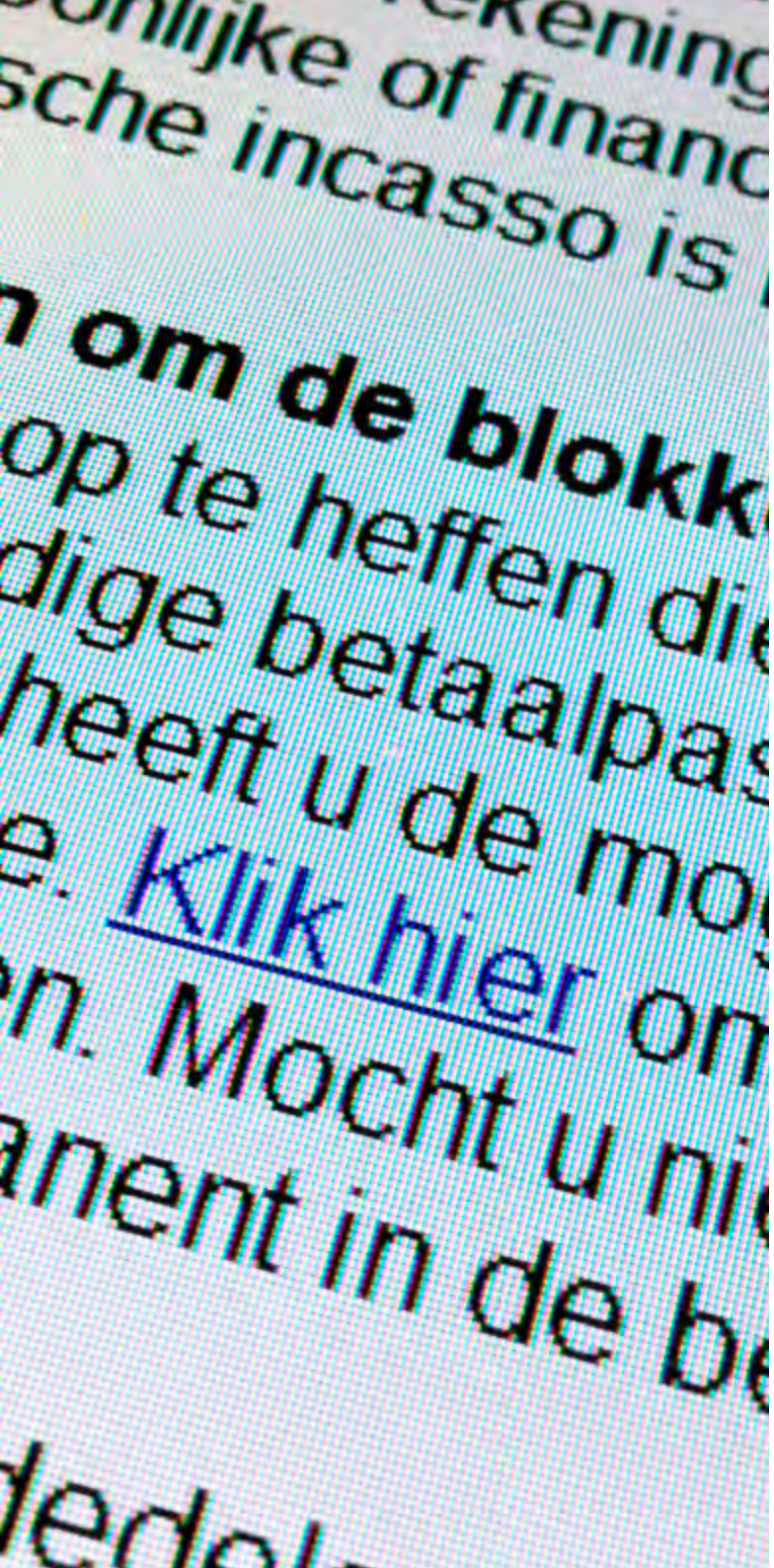
1 *Integraal tenzij...*Leidraad om samen het criminele ondernemingsklimaat te verslechteren

Ontwikkelingen in de aanpak van criminaliteit in het bedrijfsleven

In dit actieprogramma staat een drietal ontwikkelingen dan wel kansen centraal die van invloed zijn op de aanpak van criminaliteit in het bedrijfsleven. Het gaat om kansen en ontwikkelingen op het terrein van de digitalisering, informatie-uitwisseling en de samenwerking in de aanpak van criminaliteit. In de uitvoering van het actieprogramma wordt gekeken hoe overheid en bedrijfsleven hierop kunnen anticiperen, welke rol zij spelen en welke kansen er kunnen worden benut.

1. Digitalisering vernieuwt crimineel gedrag

Informatie en communicatietechnologie (ICT) zijn voor de samenleving en het bedrijfsleven onmisbaar geworden. Steeds meer mensen en organisaties maken gebruik van ICT en daarnaast wordt ICT voor steeds meer doeleinden gebruikt. Het voortschrijden van de technologische vooruitgang en het breder beschikbaar komen van technische middelen brengt met zich mee dat er sprake is van een toename van cybercrime en criminaliteit met een digitale component. Net zoals bedrijven en overheidsinstanties innoveren ook criminelen.



Criminelen en criminele organisaties zijn beter dan voorheen in staat hun criminele handelingen te plegen. Digitalisering zorgt er enerzijds voor dat oude, bekende vormen van criminaliteit zich op een nieuwe manier manifesteren, maar maakt ook nieuwe vormen van crimineel gedrag mogelijk. Daar komt bij dat daders vanuit de hele wereld hun activiteiten kunnen uitvoeren.

Het bedrijfsleven wordt in toenemende mate geconfronteerd met cybercrime. Het gebruik van digitale systemen door ondernemers is economisch gezien niet meer weg te denken. Tegelijkertijd is door de afhankelijkheid ervan een nieuwe kwetsbaarheid ontstaan. Ondernemers zijn zich ervan bewust dat er cyberdreigingen zijn, maar nog onvoldoende bewust van de aard en ernst van die gevaren, de impact die dit kan hebben op hun onderneming en de maatregelen die zij kunnen nemen om zichzelf beter te beschermen.

2. Aanpak (ondermijnende) criminaliteit vraagt om integrale samenwerking

Criminaliteit heeft zichtbare gevolgen voor het Nederlandse bedrijfsleven. Individuele bedrijven en hele branches ondervinden niet alleen financiële schade als slachtoffer van criminaliteit, maar ook reputatieschade door negatieve publiciteit over betrokkenheid. Dit als mogelijk gevolg van (on)bewust betrokken raken bij criminele activiteiten door producten of diensten te leveren, of door onder bedreiging mee te werken of te zwijgen.

De aanpak van criminaliteit vraagt om een integrale aanpak, waarbij het bereiken van maatschappelijk effect voorop staat. Een effectief antwoord van overheid en bedrijfsleven op criminaliteit in het algemeen en ondermijning in het bijzonder is gericht op het opsporen en vervolgen van daders, het voeren van een effectief preventiebeleid en het opwerpen van barrières om criminaliteit te voorkomen, maar ook op het verstoren van gelegenheidsstructuren en het afbreken van economische machtsposities van criminelen en hun *facilitators*. Daarbij is de inzet van het bedrijfsleven onontbeerlijk.

Overheid en het bedrijfslevens kunnen het niet alleen. Daadwerkelijk integraal samenwerken, zowel tussen publieke als privaat-publieke partijen, is cruciaal om criminaliteit de komende jaren terug te dringen en verplaatsing te voorkomen. Private en publieke partijen zijn zich ervan bewust dat samenwerken, het vormen van één front, het middel is om concrete resultaten te behalen. Zodoende wordt het oplossend vermogen van de partners benut.

3. Informatie-uitwisseling is essentieel

De publiek-private, integrale aanpak van criminaliteit vereist efficiënt en doeltreffend samenwerken van alle betrokken partijen. Daarbij is het uitwisselen van informatie essentieel en biedt het in de uitwerking van dit actieprogramma kansen om te komen tot zo effectief mogelijke en op elkaar afgestemde interventies.
De eerder genoemde ontwikkelingen op het terrein van ICT bieden partijen binnen samenwerkingsverbanden steeds meer mogelijkheden om tot een veilige, accurate en noodzakelijke uitwisseling van informatie te komen en op grond van deze informatie analyses te maken die tot een integraal en effectief optreden leiden[2]. Hierbij kunnen publieke en private partijen ook meer gebruik maken van big data en data-analyse. Eén informatiebron is niet meer genoeg om criminaliteit zoals bijvoorbeeld fraude te vinden. Het combineren van gegevens uit verschillende bestanden draagt bij aan de ontdekking van mogelijke criminele handelingen. Door meer en betere data bij elkaar te brengen, kunnen patronen worden gesignaleerd en wordt afwijkend gedrag in beeld gebracht. Criminelen en fraudeurs blijven daardoor niet meer structureel onder de radar.

Samenwerken geeft ook zicht op de grenzen waar organisaties op stuiten als het gaat om het uitwisselen van informatie, in verband met bijvoorbeeld de bescherming van persoonsgegevens. Bij de integrale aanpak van thema's uit het actieprogramma van het NPC wordt hiermee rekening gehouden en zal per thema worden bekeken welke barrières kunnen worden weggenomen. Daarnaast werkt het kabinet op dit moment aan een kaderwet die op termijn bijdraagt aan het vergemakkelijken van de gegevensuitwisseling.

2 Brief minister van Veiligheid en Justitie van 19 december 2014 over de kaderwet gegevensuitwisseling (TK II 2014/15, 32 761, nr. 79

3 Strategie

Het NPC versterkt de onderlinge integrale samenwerking om op die manier een grotere en effectievere bijdrage te leveren aan de bestrijding van criminaliteit tegen het bedrijfsleven. De focus van de integrale aanpak ligt op het gezamenlijk belang, waarbij het gewenste effect centraal staat. Per fenomeen zal de optimale maatschappelijke coalitie worden gevormd van publieke organisaties en bedrijfsleven om de problematiek in gezamenlijkheid aan te pakken. Daarbij worden zoveel mogelijk aangesloten bij reeds in gang gezette publiek-private projecten en overkoepelende programma's[3]. Door samen te werken kan het effect van de afzonderlijke inspanningen worden vergroot.
De realisatie van het actieprogramma is afhankelijk van de actieve betrokkenheid en verantwoordelijkheidsgevoel van alle lagen binnen betrokken organisaties en bovenal de concrete inzet van alle betrokkenen.

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, van repressieve en preventieve maatregelen bij elkaar te brengen rond een specifiek thema en deze optimaal te benutten. Elke organisatie voegt dus iets toe binnen een integrale aanpak en heeft bovendien vaak belangrijke informatie die, wanneer op adequate wijze met elkaar gedeeld, de effectiviteit van de aanpak kan vergroten.

Integraal werken hecht tevens veel waarde aan maatregelen die preventief van aard zijn en waarbij juist andere openbare instanties en de particuliere sector zijn betrokken. Deze hebben vaak de potentie om succesvol bij te dragen tot de vermindering van het probleem.

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. Daar wordt de problematiek immers ervaren door de gevestigde ondernemers en publieke partners. Het is dan ook daar dat de ontwikkeling en invoering van maatwerk oplossingen plaats dient te vinden. Om dat proces te ondersteunen en optimaliseren is het noodzakelijk dat op regionaal en lokaal niveau een effectieve structuur functioneert van publiek-private samenwerking, via de Regionaal Platform Veilig Ondernemen (PVO's, voorheen RPC's) en de Regionale Informatie en Expertise Centra (RIEC's). In de PVO's slaan politie, Openbaar Ministerie, gemeenten en ondernemers 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 aan te pakken problematiek. Vanuit de PVO's wordt er voor gezorgd dat de veiligheidsvraagstukken worden vertaald naar een concrete aanpak gericht op de oplossing van het probleem.

Om tot een succesvollere publiek-private samenwerking te komen via de PVO's zullen een aantal maatregelen worden genomen die de continuïteit en effectiviteit moete garanderen. Ten eerste zal een Raad van Toezicht (RvT) worden ingesteld die bestaat uit openbare bestuurders (burgemeesters, eenheidsleiding politie, plv. hoofdofficier, directie gemeenten e.d.). De RvT benoemt de leden van het dagelijks bestuur en bepaalt met dat bestuur de prioriteiten.

3 Denk hierbij aan concrete projecten, zoals Rotterdam Zuid, Holsteiner en Fabritius, maar ook de RIEC's en het Platform Geïntegreerde Aanpak Ondermijnende Criminaliteit.

Ten tweede wordt door de RvT een dagelijks bestuur benoemd die bestaat uit vertegenwoordigers van alle PPS partijen. Hierdoor hebben private partijen ook indirect invloed op het integraal veiligheidsbeleid van gemeenten. Het bestuur zoekt verbinding met het regionaal college en met andere samenwerkingsverbanden als het RIEC. Dit is belangrijk omdat alle partijen hun bijdrage dienen te leveren aan het reduceren van onveiligheid en beheersing van criminaliteit tegen het bedrijfsleven.

Meer en meer heeft de problematiek echter ook een sterk regio- en landsgrens overstijgend karakter. In de uitvoering moet daarom goed rekening worden gehouden met wat op de verschillende niveaus (landelijke, regionaal, lokaal) nodig is.

Informatiepositie

Een sterke informatiepositie is voor het ontwikkelen en uitvoeren van de acties in dit actieprogramma van essentieel belang en zorgt voor een gedegen inzicht in de betreffende thema's. Een effectief NPC kent de verschijningsvormen van de verschillende vormen van criminaliteit, de betrokken netwerken en heeft een antenne voor de ontwikkeling van de criminaliteit tegen het bedrijfsleven. Het NPC versterkt daarom zijn informatiepositie door het laten uitvoeren van onderzoek en het delen van relevante informatie tussen de partners binnen de grenzen van de privacy kaders.

4 Actiethema's

Prioriteiten

In dit actieprogramma zijn zeven thema's benoemd, waarvan drie actiethema's. Actiethema's zijn onderwerpen die vanwege het belang, de ontwikkelingen en de urgentie die eraan wordt gegeven een investering vergen in de analyse en de ontwikkeling van de voorgestane (effectieve) aanpak. De actiethema's van het NPC zijn cybersecurity MKB, afpersing en mobiele bendes. Daarnaast is er een drietal thema's die verder worden versterkt. Dit zijn onderwerpen die al langer in uitvoering zijn, maar nog steeds aandacht vragen en waarbij de aanpak wordt gecontinueerd of vernieuwd. Deze thema's zijn horizontale fraude, heling en transportcriminaliteit. Ondermijning is een onderwerp met raakvlakken binnen de andere thema's.

4.1 Actiethema Vergroten cybersecurity van het Midden- en Kleinbedrijf (MKB)

Ondernemers in het midden- en kleinbedrijf zijn bekend met het bestaan van cyberdreigingen, maar ze zijn zich vaak onvoldoende bewust van de huidige aard en ernst van de gevaren en de impact ervan op hun onderneming als zij erdoor worden getroffen. Gevolg is dat zij gemiddeld genomen onvoldoende of onjuiste maatregelen treffen om zich te beveiligen. De omvang van de problematiek en in hoeverre dit verschilt per branche of sector is onduidelijk. Beter inzicht in de risico's en mogelijke maatregelen is nodig. Dit stelt ondernemers beter in staat hun eigen verantwoordelijkheid voor cybersecurity te nemen.

De afgelopen jaren zijn cybersecurity-initiatieven ontplooid die gericht waren op het midden- en klein-bedrijf. Eén van de belangrijke lessen is dat een gecoördineerde aanpak noodzakelijk is om de effectiviteit en doelmatigheid van de initiatieven te optimaliseren, kennis en ervaring te bundelen en fragmentatie te voorkomen.

Doel

Bedrijfsleven en overheid hebben in het NPC afgesproken zich met ingang van 2016 gezamenlijk in te zetten voor het verbeteren van de cybersecurity in het midden- en kleinbedrijf door:

A. beter zicht te krijgen op de problematiek en diversiteit hiervan door middel van onderzoek bij branches en het betrekken van de wetenschap en onderwijsinstellingen;

B. het verbinden van initiatieven van publieke organisaties en het bedrijfsleven zodat kennis, inzet en middelen zo efficiënt mogelijk kunnen worden ingezet en resultaten zo breed mogelijk worden gedeeld;

C. gerichte communicatie waarmee gedragsbeïnvloeding wordt beoogd.

Actie 1 Er wordt door brancheorganisaties **onderzoek** gedaan naar de cybersecurity onder hun leden. De branches dienen samen een dwarsdoorsnede te vormen van het MKB-bedrijfsleven. De onderzoeken worden uitgevoerd in samenwerking met de Haagse Hogeschool (HHS).

Actie 2 Er wordt een **communicatie**strategie uitgewerkt waardoor ondernemers zich bewust worden van hun huidige onbewuste onbekwaamheid met betrekking tot cybersecurity en de stap maken hun bedrijf beter te beschermen tegen verlies van kennis, informatie, goederen, geld. Je cybersecurity regelen gaat vanzelfsprekend zijn en leiden tot 'bewust bekwaam' gedrag. Hierbij wordt gebruik gemaakt van inzichten uit de gedragswetenschappen om gedragsveranderingen te stimuleren. Voor de uitrol wordt gebruik gemaakt van bestaande communicatiekanalen van partijen en platforms, zoals Alert Online en veiliginternetten.nl, en waar mogelijk free-publicity.

Actie 3 Er worden **producten** ontwikkeld waarmee brancheorganisaties de bewustwording en actiebereidheid van hun achterban activeren. Deze producten zijn te vinden op een centrale plek (Veiliginternetten.nl). De producten en communicatiestrategie worden in samenwerking met de wetenschap en een vijftal brancheorganisaties uitgetest op werkbaarheid en succes. De bestaande, meer algemene producten wordt aangevuld met meer specifieke producten op grond van de resultaten uit de onderzoeken.

Actie 4 De PVO's ontwikkelen een **plan voor de lokale verbetering** van cybersecurity in bedrijvengebieden. De aanpak via de landelijke brancheorganisaties en de gebiedsgerichte lokale aanpak gaan elkaar in samenhang versterken.

Actie 5 Tijdens Alert Online worden, onder meer in nauwe samenwerking met de RVO's, **evenementen** georganiseerd die zich specifiek richten op het midden- en kleinbedrijf.

Actie 6 De **meldings- en aangiftebereidheid** wordt gestimuleerd.

Actie 7 Er wordt gekeken naar **trends en ontwikkelingen** waartegen kan worden gewaarschuwd.

4.2 Actiethema Afpersing

Uit onderzoek uit 2014 blijkt dat er weinig aangifte wordt gedaan van afpersing in het bedrijfsleven. Jaarlijks komen er gemiddeld 55 afpersingszaken ter kennis van de politie en komen gemiddeld 11 afpersingszaken voor de rechter. Aangenomen wordt dat dit slechts het topje van de ijsberg betreft en dat er sprake is van een groot 'dark number'. Daarnaast constateert het onderzoek dat signalen bij de politie die kunnen duiden op afpersing niet voldoende worden herkend. Inmiddels wordt hieraan gewerkt door middel van het netwerk GOA (Gijzeling, Ontvoeringen, Afpersing) van de Nationale Politie. Tevens is de vertrouwenslijn afpersing in de afgelopen jaren onder de aandacht gebracht van het bedrijfsleven. Eén van de vormen van afpersing die in het rapport is benoemd als zijnde urgent is protectieafpersing van met name horecaondernemers.

Doel

Enerzijds het verbeteren van de publiek private samenwerking en verhogen van de awareness en weerbaarheid van ondernemers en anderzijds het verbeteren van de kennis over en een betere aanpak van afpersing aan de kant van politie en het OM.

De hierna genoemde acties hebben betrekking op het vergroten van bewustwording (actie 1), het verbeteren van signalering en vertrouwensrelaties (actie 2) , het professionaliseren van aangifte en opsporing (acties 3 en 4) en het vergroten van de weerbaarheid van (potentiële) slachtoffers (acties 6 en 7).

Actie 1 Opzetten **communicatiestrategie** door middel van onder andere het plaatsen van artikelen en interviews met slachtoffers in diverse vakbladen. Daarnaast communiceren over succesvol vervolgde zaken die als showcases kunnen worden gebruikt om bewustwording te vergroten;

Actie 2 Om de signalering te verbeteren worden **regionale themabijeenkomsten** met regiomanagers, wijkagenten, OM en politie georganiseerd, bijvoorbeeld onder de vlag van de PVO's of de RIEC's. Hierdoor weten partners elkaar sneller te vinden, kan concrete casuïstiek worden besproken en kunnen eventuele vervolgafspraken worden gemaakt.

Actie 3 Via het GOA netwerk zal worden geïnvesteerd in het vergroten van de kennis over **protectieafpersing**.

Actie 4 De awareness en kennis over afpersing zal bij de politie worden gestimuleerd. In samenwerking met het OM zal door het GOA een checklist voor de aangifte worden ontwikkeld.

Actie 5 Om de weerbaarheid van slachtoffers te vergroten zullen regiomanagers van Koninlijke Horeca Nederland (KHN) en medewerkers van de beveiligingsbranche door middel van actuele kennis en inzichten worden geholpen hoe om te gaan met **Outlaw Motorgangs** (OMG's).

Actie 6 Niet alleen potentiële slachtoffers, maar ook potentiële melders zoals bijvoorbeeld boekhouders, accountants, leveranciers, collega-ondernemers, en familie/vrienden zullen gericht worden benaderd, waarbij duidelijke **handelingsperspectieven** worden meegegeven.

Actie 7 De bekendheid onder ondernemers van de bestaande **Vertrouwenslijn Afpersing** zal in samenwerking met private partners worden vergroot.

4.3 Actiethema Aanpak van mobiel banditisme

Ondernemers uit het midden- en kleinbedrijf worden geconfronteerd met mobiele dadergroepen die zich stelselmatig bezighouden met verschillende vermogensdelicten, zoals zakkenrollen, winkeldiefstal, ladingdiefstal en inbraak, die in georganiseerd verband op grote schaal worden gepleegd. Het bedrijfsleven wordt fors benadeeld door mobiele dadergroepen.

In gezamenlijkheid kunnen het ministerie van Veiligheid en Justitie, politie, OM, het bedrijfsleven en gemeenten preventief optreden om de mobiele dadergroepen te frustreren in hun activiteiten. Voor het voorkomen en bestrijden van mobiel banditisme is vereist dat de verschillende partijen die een rol hebben in de bestrijding van het probleem hun verantwoordelijkheid nemen. Een deel van het bedrijfsleven heeft inmiddels toestemming gekregen

van de Autoriteit Persoonsgegevens om een Gemeenschappelijke Informatie Organisatie (GIO) in te richten dat onder meer regelt dat ondernemers onderling gegevens kunnen uitwisselen. Ook in de Veiligheidsagenda 2015-2018 is het thema mobiele bendes als prioriteit opgenomen, waarbij wordt ingezet op het ontwikkelen van een barrièremodel en afstemming op de lokale, probleemgerichte aanpak onder regie van de lokale driehoek.

Doel

Efficiënte en effectieve beheersing van mobiel banditisme door in te zetten op een integrale aanpak en gerichte interventies en inzet op het lokale en regionale niveau.

Actie 1 Met behulp van het **barrièremodel mobiele bendes** wordt inzichtelijk gemaakt welke maatregelen partijen kunnen nemen om mobiele dadergroepen zoveel mogelijk te frustreren. Hiervoor zullen in eerste instantie in twee regio's Platforms Veilig Ondernemen worden ondersteund om lokaal de overlast van mobiele dadergroepen te bestrijden. Deze ondersteuning dient 'best practices' op te leveren die elders toegepast kunnen worden.

Actie 2 Er wordt een samenwerkingsverband opgezet tussen **politie en de GIO**, teneinde informatie uitwisselingen over mobiele dadergroepen te stroomlijnen en de aanpak op grond van bijeengebrachte en geanalyseerde informatie te versterken.

Actie 3 Er zal een Informatie uitwisselingsplatform (**VeiligheidsApp**) voor verschillende doelgroepen ter beschikking komen. Hiermee kan informatie over (lokale) veiligheid – waaronder mobiel banditisme - worden gedeeld tussen bepaalde groepen onderling zoals winkeliers, horecaondernemers, MKB ondernemers en(horeca/winkel/bedrijventerrein) beveiligers, maar ook met de overheid. Deze groepenkunnen elkaar laagdrempelig en op lokaal niveau informeren. Uiteraard zijn de politie en eventueel gemeentelijke handhavers betrokken bij dit informatie-uitwisselingsplatform. Ook de wenselijke koppeling met de GIO zal worden onderzocht.

Actie 4 Mobiele bandieten houden zich voor een kortere of langere tijd op in Nederland en hebben dus ergens een 'verblijfplaats'. Deze verblijfplaatsen kunnen vakantieparken zijn, campings, pensions of hotels. Een goede controle op deze 'nachtverblijven' is momenteel afwezig. Derhalve zal een **digitaal nachtregister** worden ingevoerd, waardoor de politie doelgericht zicht krijgt op bepaalde personen die vanuit deze ondernemingen criminele activiteiten ontplooien.

Actie 5 Onderzocht wordt of de monitor Veilig Ondernemen in Beeld (VOiB) kan worden benut voor de **aanpak van mobiele dadergroepen**. Door informatie uit VOiB te combineren, ontstaat inzicht in criminaliteit – de aantallen en typen delicten - tegen het bedrijfsleven. De PVO's kunnen op basis hiervan partijen aanzetten om gerichte interventies uit te voeren.

Actie 6 Er zal een pilot worden uitgevoerd in een tweetal grotere gemeenten, waarbij het bezit van (geprepareerde)rooftassen of het voorhanden hebben van andere middelen met als doel het manipuleren van beveiligingsmaatregelen, op basis van de APV ook binnen een onderneming strafbaar gesteld wordt.

Actie 7 In 2017 - 2018 zullen minimaal vier meerdaagse grootschalige acties worden uitgevoerd. Hierbij worden door de Nationale Politie (Landelijke eenheid en Regionale eenheden), Koninklijke Marechaussee, Douane en andere Europese politiediensten intensief en informatiegestuurd controle acties uitgevoerd op de infrastructuur waar mobiele dadergroepen gebruik van maken.

5 Versterking bestaande thema's

5.1 Versterking Thema Transportcriminaliteit

Vanuit het Actieplan Transportcriminaliteit 2015-2016 hebben TLN, EVO, TAPA, Verbond van Verzekeraars, OM, Politie, VenJ, AVc samen met andere partners zoals RWS gewerkt aan het tegenhouden van transportcriminaliteit (preventie), versterken van de repressie en het verbeteren van informatie-uitwisseling tussen partijen. Er zijn concrete resultaten behaald en goede stappen gezet in de verdere uitbouw van de publiek-private samenwerking inzake transportcriminaliteit. Dit neemt niet weg dat criminaliteit in de transport- en logistieke sector (ladingdiefstallen, voertuigdiefstallen, fraude, diefstallen van diesel en voertuigonderdelen, vandalisme en geweld jegens chauffeurs) een groot probleem blijft in Nederland en Europa, waar publieke en private partijen continu aandacht aan moeten geven. Daarom hebben partners besloten om toe te werken naar een nieuw actieplan voor de jaren 2017 en verder. Speerpunten hierin zijn ladingdiefstal, de weerbaarheid van de transportsector en het gebruik maken van technologische ontwikkelingen om criminaliteit te voorkomen en bestrijden.

Doel

Het aanpakken en terugdringen van transportcriminaliteit door in te zetten op een integrale aanpak en gerichte interventies en inzet van maatregelen.

Actie 1 Vergroten van de **bewustwording** en stimuleren van het nemen van de **juiste beveiligings- en organisatorische maatregelen**. Hierbij wordt het barrièremodel ladingdiefstallen toegepast.

Actie 2 Vergroten van de **aangiftebereidheid door de sector** zodat het percentage aangiftes toeneemt en de kwaliteit van de daarbij vastgelegde gegevens verbetert. Ook zal met de politie bekeken hoe het proces m.b.t. internetaangiftes van transportcriminaliteit kan worden geoptimaliseerd.

Actie 3 Stimuleren van **informatie-uitwisseling tussen publieke en private** partners om transport criminaliteit effectiever te bestrijden en strafbare feiten te voorkomen.

Actie 4 Vergroten van de **weerbaarheid van de transportsector** om het groeiende crimineel misbruik van de Nederlandse transportsector te bestrijden.

Actie 5 De **inzet van (nieuwe) technologische oplossingen** in de transport- en logistieke sector, bijvoorbeeld het toepassen van slimme camerasystemen en inzet sensornetwerk, ter voorkoming en bestrijding van transportcriminaliteit.

5.2 Versterking Thema Heling

Heling is ondermijnend voor de reguliere economie en zit op het snijvlak tussen boven- en onderwereld. Goederen worden gestolen om één van twee redenen: eigen gebruik of doorverkoop (heling). Heling is een secundair delict en het stimuleert het ontvreemden van (partij)goederen die eenvoudig verhandelbaar zijn in binnen- of buitenland.

Er zijn vier relevant ontwikkelingen c.q. veranderingen op het gebied van heling te noemen.

1. Heling heeft nog meer een plek in de digitale wereld gekregen, het aantal verkoopsites op internet en social media, het bereik en de populariteit ervan zijn de afgelopen tien jaar toegenomen.
2. De sociale netwerken in bepaalde wijken waar heling normaal is en onderdeel is van een tweede of parallelle economie, lijkt deels een aansluiting te hebben met georganiseerde vormen van heling. Zo komen bepaalde courante goederen (fietsen, scooters, E-bikes) vanuit wijken in het georganiseerde criminele circuit terecht.
3. Naast digitale markten zijn er veel fysieke lokale markten bijgekomen: pop-up markten voor goud en sieraden, self-storage waar garageverkopen plaatsvinden en ketens van tweedehands opkopers.
4. Heling lijkt in vergelijking met tien jaar geleden een meer georganiseerd en internationaal karakter te hebben gekregen. Ook lijkt het erop dat de georganiseerde dadergroepen zich meer zijn gaan richten op specifieke (dure en courante) goederen en onderdelen die heel snel kunnen worden doorgesluisd naar het buitenland.

Doel

Het onaantrekkelijk maken en tegengaan van heling waardoor ook de incentive voor diefstal en inbreken worden weggenomen. Hierbij richten we ons op:

- *het verkleinen van de verhandelbaarheid van gestolen goederen;*
- *het vergroten van de herkenbaarheid van goederen waardoor het ontvreemden ervan minder aantrekkelijk wordt;*
- *het bewust maken van potentiële kopers dat heling een strafbaar feit is en diefstal stimuleert;*
- *standaard betrekken van de component 'Heling' bij opsporing van de ontvreemding van partijgoederen en andere goederen die niet voor eigen gebruik zijn.*

Actie 1 In kaart brengen in hoeverre het **traceren van (niet unieke) goederen** verder kan worden verbeterd en ingevoerd.

Actie 2 In de te ontwikkelen **leermodule** 'Weerbaarheid tegen ondermijning' voor ondernemers zal het herkennen en melden van verkoop- en opslagplaatsen op bedrijvenlocaties worden opgenomen.

Actie 3 Nagaan of verhuurders zoals eigenaren en makelaars van winkel- en bedrijfsvastgoed voldoende in staat zijn te controleren of (vooral tijdelijke) **huurders** eerder gestolen goederen hebben verhandeld, opgeslagen of witgewassen.

Actie 4 Opzetten van een communicatiestrategie en -instrumenten om de **bewustwording van afnemers en kopers** te vergoten.

Actie 5 Nemen van maatregelen om **de infrastructuur** die wordt gebruikt voor heling, zoals opslagplaatsen en transport, weg te nemen. Hierbij wordt ook een relatie gelegd met de aanpak van mobiele bendes.

5.3 Versterking Thema Horizontale fraude

Fraude heeft veel verschijningsvormen en is schadelijk voor ondernemers en burgers, vanwege de financiële[4] en emotionele nadelige gevolgen. Slachtoffers van fraude hebben de fraudeur vertrouwd en daarmee zichzelf – weliswaar onbedoeld - slachtoffer gemaakt. Zelfverwijt kan slachtoffers nog jarenlang achtervolgen en leiden tot verlies van zelfvertrouwen en/of twijfels[5].

4 "Naar een fraudebeeld Nederland; Inzicht in fraude draagt bij aan bewustwording en effectieve prioriteitsstelling in de aanpak" door PwC: €3.7 miljard schade door horizontale fraude

5 "Fraude ontrafeld." Een studie naar de werkwijzen en drijfveren van fraudeurs door Alan Kabki

Fraude wordt verdeeld in verticale fraude (overheid als slachtoffer) en horizontale fraude (burgers en ondernemers als slachtoffer). Fraudeurs maken echter geen onderscheid, sommige vormen treffen zowel publieke als private partijen. Horizontale fraude is een divers en (meestal) complex fenomeen. Het vraagt een aanpak bestaande uit een mix preventieve en repressieve maatregelen. Daarbij staat vast dat de grootste winst bij die aanpak vooral is te behalen door versterking van de preventie van fraude. Het vergroten van de weerbaarheid van potentiële slachtoffers, het opwerpen van barrières, waarschuwen en vroegtijdig verstoren kunnen de kansen van fraudeurs verminderen. Daarvoor is vroegsignalering van fraudeleuze handelingen en patroonherkenning noodzakelijk. De benodigde kennis zit vaak in verschillende databases (zowel publiek als privaat) en is daarmee te versnipperd om momenteel effectief te worden gebruikt om fraude te voorkomen.

Doel

Het tegengaan van slachtofferschap en schade door een effectievere en efficiëntere preventie en bestrijding van horizontale fraude in algemene zin en binnen specifieke deeldomeinen.

Actie 1 De **kennis** over de verschillende fraudefenomenen en daders actualiseren (netwerk-APK's) en aangrijpingspunten identificeren waarmee barrières kunnen worden gerealiseerd.

Actie 2 Focus aanbrengen in **generieke en specifieke fraudevormen**. Hierbij zal worden onderzocht welke generieke problemen branches tegenkomen om hun preventieve rol te kunnen waarmaken en wat zij daarvoor nodig hebben.
Ten aanzien van een aantal nader te bepalen fraudevormen zal meer specifiek met betrokken private en publieke partijen worden bepaald welke maatregelen potentieel succesvol zijn, welke haalbaar zijn, wat de haalbaarheid in de weg staat en bepalen of dat op te lossen is.

Actie 3 In kaart brengen hoe via de bestaande kanalen **de weerbaarheid van ondernemers** tegen diverse vormen van fraude verbeterd kan worden zodat zij minder snel slachtoffer worden.

Actie 4 In kaart brengen welke **data en informatiekanalen** van belang zijn bij het voorkomen en tegengaan van fraude en hoe deze optimaal benut zouden kunnen worden.

Actie 5 Bepalen hoe een **civiele aanpak** en **het strafrecht** elkaar kunnen versterken.

Actie 6 Onderzoeken hoe melden en/of aangifte doen van fraude zodanig kan worden gefaciliteerd zodat de verkregen informatie ook kan worden gebruikt voor **preventie en het opwerpen van barrières.**

6 Ondermijning

Bedrijfsleven en overheid gaan zich gezamenlijk inzetten voor het terugdringen van de invloed van ondermijning op het bedrijfsleven en de faciliterende rol die bedrijven daarin hebben. Naast specifieke maatregelen die zich richten op de bestrijding van ondermijnende en faciliterende fenomenen uit dit actieplan draait het voor een belangrijk deel om bewustwording, zowel in branches als van individuele ondernemers, van het feit dat bedrijven of sectoren worden gebruikt om criminele activiteiten te faciliteren. De maatschappelijke weerbaarheid van het bedrijfsleven moet worden vergroot. Het NPC voelt zich verantwoordelijk om een ieder betrokken te laten voelen bij de aanpak van ondermijnende criminaliteit. Daarbij is het belangrijk om oog te hebben voor de tegenstrijdige belangen binnen een sector, bijvoorbeeld daar waar economische belangen botsen met het belang om ondermijnende criminaliteit tegen te gaan.

Daarnaast richt de aanpak zich op branches waar faciliteerders voorkomen. Het NPC spreekt deze branches aan op het belang van een schone branche. Door bijvoorbeeld gedragsafspraken te maken en convenanten af te sluiten, worden branches gecommitteerd om corrigerend op te treden tegen foute branchegenoten.

Doelen

a) *De weerbaarheid vergroten van (potentiële) slachtoffers en (onbewuste) facilitators. Daarnaast worden bewuste facilitators uit de sector geweerd en actief bestreden.*
b) *Intensiveren publiek-private samenwerking en verbinden van bestaande initiatieven, zodat kennis en middelen met betrekking tot de aanpak van ondermijnende criminaliteit zo efficiënt mogelijk kunnen worden ingezet en resultaten zo breed mogelijk worden gedeeld.*

Actie 1 **Ontwikkelen van een leergang** om de weerbaarheid van ondernemers in bedrijvengebieden en buitengebieden te verhogen. Door zelf weerbaar te zijn tegen directe ondermijnende activiteiten, maar ook door het signaleren van ondermijnende activiteiten. Daarbij is het belangrijk te onderzoeken welke factoren de meldingsbereidheid aan de overheid stimuleren en belemmeren en hoe deze zijn te beïnvloeden.

Actie 2 **Facilitator aanpak** stimuleren, blokkades identificeren en weghalen.

Actie 3 **Onderzoeken** hoe beschikbare publieke informatie op maat valt te ontsluiten voor private partijen die een rol kunnen spelen bij de bestrijding van ondermijnende criminaliteit. Ook de overheid heeft veel gegevens die voor bedrijven(terreinen) en sectoren bruikbaar kunnen zijn.Ook de overheid heeft veel gegevens die voor bedrijven(terreinen) en sectoren bruikbaar kunnen zijn.

Actie 4 Best- en bad practices verzamelen en **toegankelijk maken** voor andere partijen die oplossingen zoeken.

Actie 5 Stimuleren en faciliteren van concrete **publiek-private samenwerkingsprojecten** bij de bestrijding van ondermijnende criminaliteit.

Onder meer door in samenwerking met de beveiligingsbranche, bedrijfsleven en de (lokale) overheid afspraken te maken om de integriteit en weerbaarheid van deze branche te versterken.

7 Organisatie

Organisatiestructuur NPC

NPC

Het NPC is eindverantwoordelijk en besluitvormend. De leden van het NPC stellen de verschillende projectplannen formeel vast en worden gedurende de uitvoering van de projecten geïnformeerd over de voortgang en nemen beslissingen over de belangrijkste mijlpalen.

Kernteam

Het Kernteam treedt op als stuurgroep en is verantwoordelijk voor de realisatie van alle in het actieplan genoemde projecten. Het kernteam volgt via het ON de voortgang van de bestaande projecten, beoordeelt nieuwe projectvoorstellen en stuurt het ON aan.

Operationeel Netwerk

Het ON bewaakt het niveau en voortgang van de projecten en rapporteert daarover richting het kernteam en het NPC. Daarnaast zorgt ze ervoor dat de ervaringen/kennis/voortschrijdend inzichten geborgd en benut kunnen worden binnen publieke en private structuren.

Projectleider - werkgroep

Voor elk van de projecten is één van de betrokken organisaties aangewezen als projectleider. Deze is verantwoordelijk voor de opzet en uitvoering van het desbetreffende project. De project leiders rapporteren per kwartaal aan het Kernteam.

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. Door met deze cyclus te werken kan tijdig worden bijgestuurd en kunnen interventies tussentijds worden aangescherpt.

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@minvenj.nl of bel 06- 13033207

Cover foto:
Bedrijventerrein Spaanse Polder in Rotterdam en Schiedam. Het NPC heeft op 9 mei 2016 een werkbezoek gebracht aan dit gebied en zal de Spaanse Polder gebruiken als proeftuin voor verschillende projecten uit dit actieprogramma.

oktober 2016 | 94796

Ministerie van Veiligheid en Justitie

Ministerie van Economische Zaken

VNG Vereniging van Nederlandse Gemeenten

Detailhandel Nederland

Horeca Nederland

Nederlandse Vereniging van Banken

POLITIE « waakzaam en dienstbaar »

MKB Nederland

TLN

OPENBAAR MINISTERIE

VNO NCW

VERBOND VAN VERZEKERAARS