



Samen criminaliteit bestrijden

Eerste input richting de nieuwe agenda van het Nationaal Platform Criminaliteitsbeheersing

Bureau **Beke**

Inleiding

Binnen het Nationaal Platform Criminaliteitsbeheersing (NPC) – een samenwerkingsverband van overheid en bedrijfsleven – wordt vanuit een meerjarig actieprogramma samengewerkt in de aanpak van verschillende vormen van criminaliteit tegen en (onbewust) gefaciliteerd door het bedrijfsleven. De samenwerking heeft als doel het terugdringen en voorkomen van deze criminaliteit en het versterken van de aanpak door het stimuleren en verstevigen van publiek-private samenwerking op nationaal, regionaal en lokaal niveau. Het huidige actieprogramma loopt eind 2022 af en het is nu tijd om te gaan werken aan de inhoud van een nieuw actieprogramma (2023-2026). Aan Bureau Beke is gevraagd om middels onderzoek input hiervoor te leveren.

Voor het onderzoek zijn diverse activiteiten verricht om een beeld te schetsen van de actuele problematiek waarmee het bedrijfsleven te maken heeft. Dit maakt het mogelijk dat het NPC zich kan richten op de juiste opgaves en de nieuwe prioriteiten (focus aanbrengen) en dat men kan rekenen op een breder draagvlak vanuit het bedrijfsleven. Naast het in beeld brengen van actuele problematiek hebben de thema's ondermijnende criminaliteit en cybercrime extra aandacht gekregen. Dit om een verdieping aan te kunnen brengen in deze vormen van criminaliteit die naar verwachting de komende jaren prioriteit blijven houden. De onderzoeksactiviteiten zijn hiernaast schematisch weergegeven.

Figuur 1: Onderzoeksdesign



Een terugblik op eerder onderzoek in 2018

In 2018/2019 werd door Bureau Beke het onderzoek 'Agenda voor de toekomst' uitgevoerd dat input heeft gegeven voor het huidige actieprogramma 2019-2022. In dat onderzoek werden de volgende hoofdlijnen – veiligheidsthema's en aanpak van criminaliteit tegen en door het bedrijfsleven – opgetekend: zichtbaar en tastbaar maken van ondermijnende criminaliteit, afstand tot de overheid verkleinen, vergroten meldingsbereidheid en meer aandacht voor cybercrime. We lichten deze hoofdlijnen kort toe:

1. Zichtbaar en tastbaar maken van ondermijnende criminaliteit: ondermijnende criminaliteit is veelal onzichtbaar en kent veel verschijningsvormen. Voor zowel de overheid als ondernemers is het belangrijk om ondermijnende criminaliteit zichtbaar en tastbaar te maken. Daarom moeten initiatieven dichtbij ondernemers worden georganiseerd. Deze kunnen bijvoorbeeld op sectorniveau worden ontplooid of locatiegebonden (bedrijventerrein, gemeente, regio) zijn. Vanuit casuïstiek kan het onderwerp zicht- en tastbaar worden. Inzichten vanuit de uitvoering kunnen worden gebruikt om tot een concrete aanpak te komen op basis van bijvoorbeeld barrièremodellen, om de weerbaarheid van ondernemers en het zelfreinigend vermogen van sectoren te vergroten en om systeemfouten te identificeren. Mandaat en bestuurlijke draagkracht – zoals bij de Taskforce Mobiel Banditisme het geval is – zijn daarbij van belang;
2. Afstand tot overheid verkleinen: de overheid is geen betrouwbare partner (meer) voor het bedrijfsleven door een te grote afstand met de lokale ondernemer en het ontbreken van opvolging van door burgers en ondernemers gedane meldingen en aangiften. Ook het uitwisselen van informatie wordt door wetten en regels te zeer beperkt. Investeren in de onderlinge relatie is belangrijk om in de nabije toekomst gestalte te kunnen geven aan het aanpakken van de uitdagingen waarvoor het bedrijfsleven zich gesteld

ziet. Een manier om dit te bewerkstelligen, is het organiseren van activiteiten dicht bij de ondernemer (zoals ondernemersavonden);

3. Vergroten meldingsbereidheid: de meldingsbereidheid van het bedrijfsleven op het vlak van ondermijnende criminaliteit is klein. Dit heeft niet alleen te maken met bewustzijn (zie punt 1), maar ook met een te grote afstand tussen overheid en ondernemer. Om deze afstand te overbruggen, moeten initiatieven op regionaal en lokaal niveau worden ontplooid en het aangifteproces worden versimpeld (met name in relatie tot veelvoorkomende criminaliteit zoals winkeldiefstal);
4. Meer aandacht voor cybercrime: criminaliteit met een digitale component wordt binnen een groot deel van het Nederlandse bedrijfsleven veronachtzaamd. Niet alleen het vergroten van het bewustzijn maar ook het bieden van mogelijkheden om de veiligheid van de eigen digitale infrastructuur te testen, zijn belangrijk om kwetsbaarheid voor cybercrime te beperken.

Leeswijzer

De notitie valt in eerste instantie uiteen in drie delen: bevindingen uit de desk-research, de online survey en de raadpleging van ondernemersverenigingen/panelgesprekken met stakeholders. In een laatste, afsluitend deel worden alle bevindingen met elkaar in verband beschouwd. Dit deel is ook te lezen als een samenvatting.



Inzichten vanuit de deskresearch (literatuur en media)

In de deskresearch is bestaande kennis over criminaliteit tegen en gefaciliteerd door het bedrijfsleven verzameld en geanalyseerd. De focus lag daarbij op zowel wetenschappelijke literatuur als andere kennisdocumenten ('grijze literatuur') vanaf het moment waarop de deskresearch uit het onderzoek uit 2018 stopte tot en met voorjaar 2022. Omdat in dat onderzoek naar voren kwam dat er relatief weinig relevante literatuur beschikbaar was, is aanvullend ook een media-analyse uitgevoerd.

Bevindingen uit de deskresearch

4

In de periode 2018-2022 zijn [47 wetenschappelijke publicaties](#) gevonden die betrekking hebben op criminaliteit in het bedrijfsleven. Het grootste deel hiervan heeft betrekking op ondermijnende criminaliteit (21 publicaties) en cybercrime (twaalf publicaties). Daarnaast beschrijven zeven publicaties het thema vermogensdelicten (winkel- en ladingdiefstal, overval en inbraak), drie faillissementsfraude, drie arbeidscriminaliteit en illegale tewerkstelling. De resterende twee onderzoeken hebben betrekking op vandalisme en financiële fraude.

Wat betreft ondermijnende criminaliteit focussen de onderzoeken zich op diverse verschijningsvormen. Veel ondermijningsonderzoeken belichten fenomenen als drugscriminaliteit, opslag en vervoer van andere goederen, personen of geld en het witwassen van criminele gelden. De branches die hierin worden genoemd zijn logistieke knooppunten in Nederland (Schiphol, bloemensector, zeehavens, et cetera) maar ook de vastgoedsector zoals woningen en bedrijfspanden. Ook worden opslaglocaties zoals opslagboxen en dergelijke genoemd. Een aandachtspunt in de onderzoeken is dat het slechts zelden duidelijk wordt of de

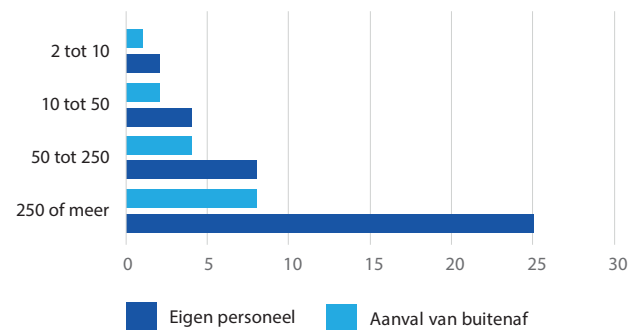
ondernemers de criminele activiteiten bewust of onbewust gefaciliteerd hebben. Dit geldt ook voor makelaars, taxateurs en notarissen die vanuit hun functie erop moeten toezien dat de vastgoedsector wordt misbruikt. Het is ook de vraag in hoeverre ondernemers zich bewust zijn van ondermijnende activiteiten. Wanneer de criminelen zogenoemde facilitators gebruiken, is het bijvoorbeeld al erg lastig om aan de voorkant te vermoeden dat hier criminelen achter schuilen.

Wat betreft cybercrime komt uit de deskresearch naar voren dat mkb'ers relatief vaak slachtoffer van deze criminaliteitsvorm worden. Het CBS heeft hier in 2021 ook enige aandacht aan besteed, door in de zogenaamde Cybersecuritymonitor een vergelijking te maken een vergelijking tussen incidenten uit 2019 en 2016, vooral aan zogenaamde data-onthullingen.¹

Het blijkt dat relatief gezien vooral grotere bedrijven met 250 of meer werknemers in 2019, vergeleken met 2016, vaker slachtoffer waren van een data-onthulling door eigen personeel: 25 om 17 procent. Omdat hier ook sprake kan zijn van onbedoelde onthullingen, zijn de aanvallen van buitenaf voor onderhavig onderzoek relevanter. Het blijkt dat 2 procent van de bedrijven in 2019 te maken kreeg met dataonthulingsincidenten als gevolg van een aanval (hack of inbraak) van buitenaf. Figuur 2 toont de verschillen naar bedrijfsgrootte tussen interne incidenten en aanvallen van buitenaf.

1. Bron: www.cbs.nl/nl-nl/nieuws/2021/r8/toename-dataonthulling-bij-grote-bedrijven. Bij data-onthullingen gaat het om elektronische gegevens, zoals persoonsgegevens van klanten of digitale informatie over bedrijfsprocessen, die onbedoeld geopenbaard worden. De oorzaak kan zowel onopzettelijk zijn, door bijvoorbeeld het laten liggen van een USB-stick met gevoelige bedrijfsinformatie, als het gevolg zijn van een aanval van buitenaf, zoals een hack van de ICT-systemen door cybercriminelen. Er is in 2022 ook een Cybersecuritymonitor opgeleverd, maar deze heeft niet geleid tot meer actuele cijfers.

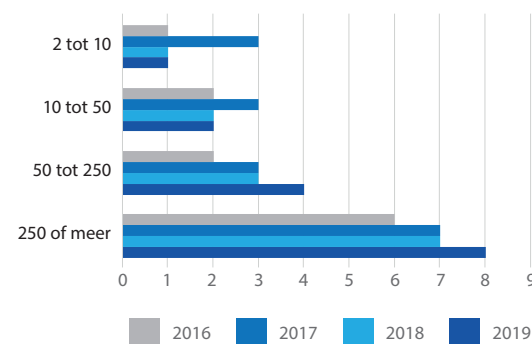
Figuur 2: Slachtofferschap data-onthulling naar bedrijfsgrootte en aard (in %)



Bron: CBS, 2021.

Als wordt ingezoomd op de dataonthullingen van buitenaf tussen 2016 en 2019 (figuur 3) dan blijkt dat deze criminaliteitsvorm in die periode vooral de grotere bedrijven in toenemende mate treft.

Figuur 3: Slachtofferschap data-onthulling van buitenaf, naar bedrijfsgrootte (in %)



Bron: CBS, 2021.

Uit de bestudeerde literatuur over cybercrime komt naar voren dat het fenomeen vele verschijningsvormen kent: hacken, malware, Distributed-Denial-of-Service (DDoS)-aanvallen, phishing, CEO-fraude, ransomware, social engineering, Business E-mail Compromise (BEC)-fraude en valse factuurfraude worden genoemd. Vaak is het motief van criminelen om de ondernemers af te persen en hen te dwingen om losgeld te betalen. Ook blijkt dat de coronacrisis het risico op cybercrime heeft vergroot. Het aantal computers waar hackers gebruik van konden maken om bij bedrijfsnetwerken binnen te komen, was door thuiswerk namelijk veel groter dan voor de coronapandemie. Daarbij kwam dat twee derde van de Nederlanders meende uitstekend op de hoogte te zijn van alle digitale gevaren. Zij achtten de kans om thuis of in een werksituatie slachtoffer te worden van cybercrime dan ook klein. In werksituaties waande maar liefst drie kwart van de Nederlanders zich bijzonder veilig. Mogelijke schade zagen mensen vooral door hacking (13%), een DDoS-aanval (12%) en ransomware (12%) gebeuren. In thuissituaties stond malware op de eerste plaats (14%), gevolgd door cryptojacking (het hacken van iemands computer om cryptomunten als bitcoins te delven) en phishing met respectievelijk 12 en 11 procent.²

Bevindingen uit de media-analyse

Om een beeld te krijgen van berichtgeving over criminaliteit tegen en gefaciliteerd door het bedrijfsleven is in LexisNexis³ gezocht naar mediaberichten in de periode 1 januari 2019 tot en met 31 december 2021. Dit leverde in totaal 1.709 mediaberichten op, waarvan 73 mediaberichten uiteindelijk daadwerkelijk betrekking hadden op het onderzoeksthema. Eerst wordt ingegaan op de omvang en aard van verschillende criminaliteitsvormen, daarna op de impact op slachtoffers en ten slotte op de aanpak van diverse criminaliteitsvormen. Een belangrijke disclaimer hierbij is dat journalisten vanwege tijdsgebrek selectief moeten zijn in de onderwerpen waarover zij schrijven, dus de resultaten zullen mogelijk geen volledig beeld geven van de criminaliteit tegen en gefaciliteerd door het bedrijfsleven.

Mediaberichten over de verschillende criminaliteitsvormen

Van de 73 mediaberichten gaan twee mediaberichten niet in op een specifieke criminaliteitsvorm, maar wordt in het algemeen over criminaliteit gesproken. In beide mediaberichten gaat het over criminaliteit op bedrijventerreinen. In de andere 71 mediaberichten wordt wel gesproken over specifieke criminaliteitsvormen. In tabel 1 staat een overzicht van de artikelen per criminaliteitsvorm.

-
2. Bron: Ministerie van Economische Zaken en Klimaat (2020). Veilig Online 2020.
 3. LexisNexis geeft toegang tot meer dan 36.000 internationaal gerenommeerde nieuwsbronnen en zakelijke bronnen. De database bevat ruim 75 Nederlandse uitgevers, waaronder alle grote landelijke en regionale kranten en opiniebladen.

Tabel 1: Overzicht van de artikelen per criminaliteitsvorm

Criminaliteitsvorm	Aantal artikelen waarin de vorm genoemd wordt	Belangrijkste bevindingen uit de media-analyse
Cybercrime	34	
Cybercrime algemeen	14	
Ransomware	11	
Hacken	4	
Phishing	3	
CEO-fraude	1	
DDos-aanval	1	
Ondermijning	18	
Ondermijning algemeen	6	
Bedreiging en intimidatie	1	
Criminele financiering	3	
Drugscriminaliteit	8	
Afpersing/bedreiging	6	
Diefstal/overval/inbraak	13	

- in coronatijd, tussen 2019 en 2021, is sprake van een toename van 200 procent cybercrime-incidenten.
- een op de vijf ondernemers krijgt jaarlijks te maken met een cyberaanval, zoals ransomware, hacken of phishing
- volgens de Kamer van Koophandel vinden er wekelijks bijna driehonderd cyberaanvallen op het Nederlandse bedrijfsleven plaats
- exploitatie van horecagelegenheden, coffee-shops, seksinrichtingen, kapsalons en nagel-salons zijn extra gevoelig voor ondermijnende activiteiten
- veel mediaberichten over ondermijnende drugscriminaliteit leggen een verband met het platteland als locatie
- de omvang van afpersing is niet eenduidig
- bedreiging heeft betrekking op tegenstanders van het bouwen van grote windmolenparken
- berichten over diefstallen/overvallen focussen zich vooral op supermarkten, benzinestations en koeriers. Agrarische bedrijven hebben met diefstal te maken
- inbraken komen voor in winkels, op bedrijven-terreinen en in de vorm van ladingdiefstal



Initiatieven en suggesties voor aanpakken tegen criminaliteit tegen bedrijven

In onderzoeken en mediaberichten is informatie verschenen over diverse initiatieven en suggesties om verschillende criminaliteitsvormen aan te pakken, zowel op landelijk, regionaal als lokaal niveau. Deze initiatieven zijn in tabel 2 naar criminaliteitsvorm gerangschikt.

Tabel 2: Initiatieven naar criminaliteitsvorm gerangschikt

Vorm	Initiatieven en suggesties voor aanpak
Cybercrime	• verdubbeling capaciteit cybercrimeteams bij de politie en een opleidingsspecialist bij iedere politie-eenheid • samenwerking politie met Europol en Interpol • suggestie: meldplicht bij cybercrime instellen • grote bedrijven die zich ontfemen over de cybersecurity van kleinere bedrijven • campagne Alert Online (ministerie van Economische Zaken) • monitoring van kwetsbaarheden binnen de digitale wereld door het Dutch Institute for Vulnerability Disclosure • activiteiten van het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC). Via het voorstel van de Wet bevordering digitale weerbaarheid bedrijven zal dreigingsinformatie vanuit het NCSC breder gedeeld worden, ook met het bedrijfsleven • (buiten)strafrechtelijk traject voor jeugdige hackers: Hack_Right • vijf basisregels van het DTC voor het vergroten van de weerbaarheid van ondernemers opgesteld • Onderzoeksraad voor de Veiligheid: waarschuw zo snel mogelijk na een cyberaanval, tuig een centrale cyberveiligheidsdienst op en maak een minister verantwoordelijk voor cyberveiligheid. En laat softwareproducten, bedrijven, overheden en instellingen verplicht verantwoording afleggen over hun aanpak • vanaf 2023: kans op boete van Agentschap Telecom in het geval van stilzwijgende betaling losgeld aan cybercriminelen • op regionaal niveau: diverse initiatieven rondom het vergroten van ondernemersbewustzijn over cybercrime (onder andere gratis phishingtest, Week van de Veiligheid en andere evenementen)

Cybercrime (vervolg)	• op lokaal niveau: diverse voorlichtingsbijeenkomsten/workshops bij ondernemersverenigingen en via het Platform Veilig Ondernemen
Ondermijning	• Keurmerk Veilig Ondernemen Bedrijventerreinen (KVO-B): in 2019 hebben meer dan 900 bedrijventerreinen in Nederland dit keurmerk behaald • suggestie en enkele lokale initiatieven: burgers meer aansporen om ondermijnende criminaliteit te herkennen en vermoedens van criminaliteit tegen bedrijven te melden bij de politie of via Meld Misdaad Anoniem • samenwerking tussen bedrijven via het project Veilig Ondernemen Door Informatie Op Maat • suggestie voorzitter MKB-Nederland: gegevens over criminelen delen moet mogelijk worden, zonder dat de Autoriteit Persoonsgegevens vooraf toestemming moet geven • aanpak ondermijnende criminaliteit op specifieke gebieden: bijvoorbeeld het Combiteam Havens (Rotterdam en Vlissingen), samenwerking provincie Limburg en Limburgse Land- en Tuinbouwbond bij inzet drones tegen hennepeteelt
Afpersing bedreiging	• advies MKB-Nederland en VNO-NCW: niet ingaan op eisen afpersers, maar aangifte doen, melden via Meld Misdaad Anoniem of de Vertrouwenslijn Afpersing. In 2019 blijkt deze laatste lijn slechts 25 keer te zijn geraadpleegd, vooral omdat de lijn te onbekend is of ondernemers te bang zijn om hulp in te schakelen
Diefstal/overval/inbraak	• ontwikkeling programma 'Straatwaarden': repressieve inzet op 'negatieve rolmodellen'/sleutelfiguren in drugshandel en geweldsincidenten • steeds meer koeriersbedrijven gaan over op alleen digitaal betalen. In een enkel geval worden bodycams/groepsapps voor de veiligheid gebruikt • diefstal bij agrariërs: vermoeden van mobiele bendes leidt tot aanpak landelijk politieteam

Resultaten uit de survey

In dit hoofdstuk beschrijven we de bevindingen die uit de survey onder ondernemers naar voren komen, opgedeeld naar achtergrond van de ondernemers, eigen slachtofferschap en de aanpak van criminaliteit.

Achtergrond respondenten

In totaal hebben 298 ondernemers in voorjaar 2022 de vragenlijst (gedeeltelijk) ingevuld. Respondenten hebben gemiddeld 24 jaar ervaring als ondernemer. De sectoren waarin de ondernemers actief zijn, zijn voornamelijk de groot- en detailhandel (32%) en de sector landbouw, bosbouw en visserij (18%). In het onderzoek uit 2018 waren de meeste respondenten actief in de zakelijke dienstverlening (22%), groot- en detailhandel (11%), horeca (10%), gezondheidszorg (9%) of de informatie- en communicatiesector (9%). Omdat voor de twee onderzoeken voor een verschillende indeling is gekozen, is de responsherkomst niet vergelijkbaar.

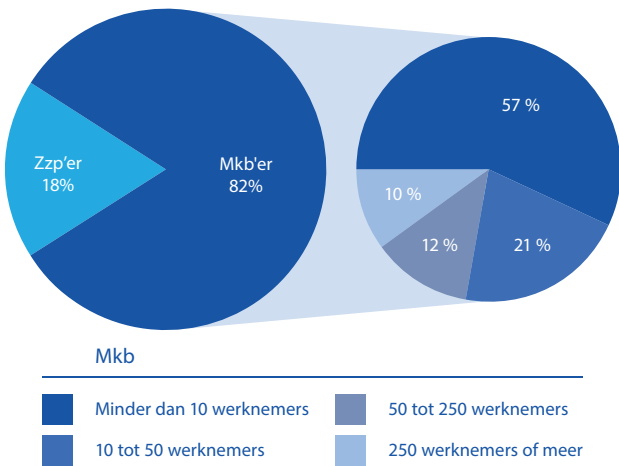
Tabel 3: Sector ondernemer (n=298, in %)

Sector	2018 %	2022 %
Groot- en detailhandel	11%	32%
Landbouw, bosbouw en visserij	-	18%
Overige dienstverlening	3%	10%
Zakelijke dienstverlening	22%	10%
Horeca	10%	9%
Bouwnijverheid	4%	4%

Vervoer en opslag	2%	4%
Financiële dienstverlening	7%	3%
Verhuur en handel van onroerend goed	3%	3%
Industrie	3%	2%
Informatie en communicatie	9%	-
Gezondheidszorg	9%	-
Veiligheidssector	4%	-
Publieke sector	3%	-
Overige	11%	5%
Totaal	100%	100%

Bijna een vijfde van de respondenten (18%) is zzp'er, de rest van de respondenten (82%) heeft een of meerdere werknemers in dienst. Ruim de helft van de ondernemers met werknemers in dienst geeft aan dat dit er niet meer dan tien zijn. Een tiende van de ondernemers heeft meer dan 250 personen in dienst.

Figuur 4: Ondernemingsvorm en aantal werknemers (n=298)



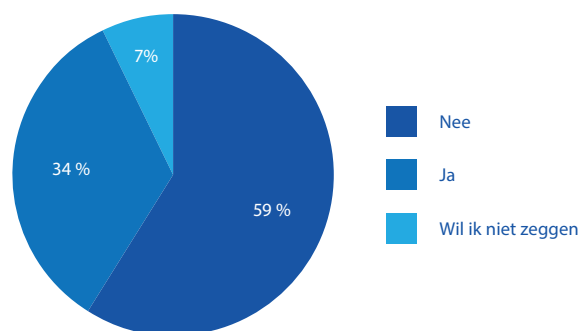
Zzp versus mkb

In het verdere verloop van de surveybeschrijving zullen we, als dit aan de orde is, vermeldenswaardige verschillen in de mening tussen zzp'ers versus mkb'ers beschrijven. Deze verschillen staan in soortgelijke blauwe kaders.

Slachtofferschap bedrijven

Ongeveer een derde van de respondenten (34%) geeft aan dat hun onderneming het afgelopen jaar (2021) slachtoffer is geworden van een bepaalde vorm van criminaliteit (zie figuur 5).

Figuur 5: Slachtofferschap criminaliteit 2021 (n=221)



Zzp versus mkb

Mkb'ers worden beduidend vaker slachtoffer van een vorm van criminaliteit dan zzp'ers: 39 om 12 procent van de respondenten geeft aan het afgelopen jaar slachtoffer te zijn geworden.

Van de 75 respondenten die slachtoffer zijn geworden van een vorm van criminaliteit, geeft ongeveer de helft (51%) aan dat dit van diefstal van buitenaf was. Ondernemers worden het minst slachtoffer van heling, mensenhandel of prostitutie, plof- en ramkraken, afpersing en ondermijnende criminaliteit (zie tabel 4). De respondenten die aangeven slachtoffer te zijn geworden van een andere vorm van criminaliteit, lichten dat toe als geluidsoverlast, oplichting of intimidatie.

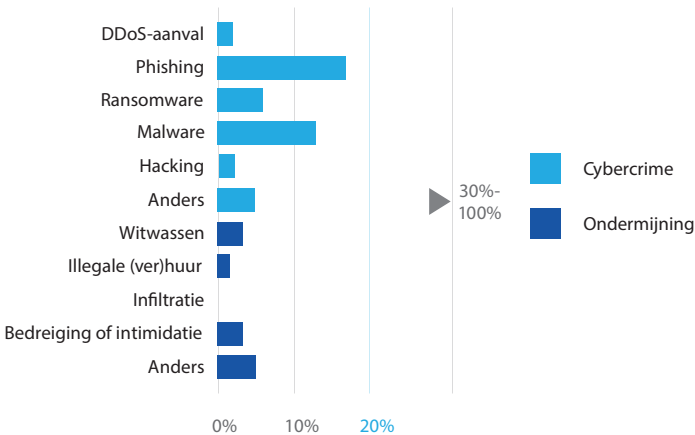
Tabel 4: Criminaliteitsvormen slachtofferschap ondernemingen 2021 (n=75)

Criminaliteitsvormen	n	%
Diefstal van buitenaf	38	51%
Bedreiging	23	31%
Fraude	22	29%
Diefstal door personeel	21	28%
Geweld tegen personeel	20	27%
Vandalisme	19	25%
Inbraak	18	24%
Cybercrime	16	21%
Overval	13	17%
Ondermijning	3	4%
Afpersing	2	3%
Plof- en ramkraken	2	3%
Mensenhandel of prostitutie	1	1%
Heling	0	0%
Anders	7	9%

Inzoomen op cybercrime en ondermijnende criminaliteit

Behalve de vraag van welke vormen van criminaliteit ondernemers slachtoffer zijn geworden, is ook gevraagd of ze te maken hebben gehad met specifieke vormen van cybercrime en ondermijnende criminaliteit. Bijna een derde van de ondernemers (31%) geeft aan dat zijn of haar bedrijf in 2021 te maken heeft gehad met een vorm van cybercrime. Phishing en malware zijn de meest voorkomende vormen van cybercrime waar bedrijven mee te maken kregen (zie figuur 6). Ongeveer een op de acht respondenten (12%) geeft aan dat zij het afgelopen jaar te maken kregen met een vorm van ondermijnende criminaliteit. Witwassen en bedreiging of intimidatie worden – na een ‘andere’ vorm van ondermijnende criminaliteit – het meest genoemd als vorm van ondermijnende criminaliteit (zie figuur 6). Voorbeelden van andere vormen van ondermijnende criminaliteit die respondenten noemen zijn verduistering van voertuigen en oplichting.

Figuur 6: Met welke vormen van cybercrime en ondermijnende criminaliteit hebben ondernemers het afgelopen jaar te maken gehad (n=211)



Een speciale vorm: criminaliteit vanwege maatschappelijke onrust

De afgelopen jaren was er onder – delen van – de bevolking veel maatschappelijke onrust, wat zich onder andere heeft geuit in agressie maar soms ook in vernielingen en plunderingen. Ruim een kwart van de respondenten (27%) heeft hier last van gehad. Volgens deze ondernemers uitte zich dit voornamelijk in agressie (60%) en vernielingen (47%), terwijl een enkeling geeft aan dat zijn of haar onderneming is geplunderd (11%).

Aanpak criminaliteit

In het Actieprogramma Veilig Ondernemen werken de overheid en het bedrijfsleven samen aan de aanpak van criminaliteit. Aan respondenten is gevraagd om verschillende criminaliteitsvormen te rangschikken en zo aan te geven wat zij belangrijk vinden om aan te pakken binnen dit programma. Diefstal van buitenaf blijkt voor de ondernemers de belangrijkste criminaliteitsvorm om aan te pakken, gevolgd door cybercrime en inbraak. Tabel 5 presenteert de rangorde voor alle bevroagde criminaliteitsvormen.

Tabel 5: Ranking aanpak criminaliteitsvormen (n=298)

1.	Diefstal van buitenaf	8	Fraude
2.	Cybercrime	9	Andere vorm van criminaliteit
3.	Inbraak	10	Diefstal van personeel
4.	Overvallen	11	Afpersing
5.	Geweld tegen personeel	12	Mensenhandel
6.	Bedreiging	13	Heling
7.	Ondermijning	14	Vandalisme

In de huidige survey komt diefstal van buitenaf als belangrijkste criminaliteitsvorm naar voren om aan te pakken. Dit terwijl deze vorm in 2018 in de rangschikking niet verder kwam dan de middenmoot. Dit verschil is te verklaren doordat er in de huidige survey – in vergelijking met de survey uit 2018 – relatief veel respondenten zitten die actief zijn in de groot- en detailhandel en de landbouw, bosbouw en visserij. Juist deze sectoren beschouwen dit fenomeen als belangrijkste criminaliteitsvorm voor de aanpak.

Zzp versus mkb

Mkb-respondenten vinden drie criminaliteitsvormen belangrijker om aan te pakken dan zzp'ers. Dat zijn diefstal van personeel, geweld tegen personeel en heling.

Sowieso loopt de mening over het belang van het aanpakken van bepaalde criminaliteitsvormen uiteen, al naar gelang de bevraagde sector. In tegenstelling tot de sectoren die diefstal van buitenaf het belangrijkste vinden, is cybercrime voor de zakelijke en financiële dienstverlening, de bouwnijverheid en de industrie het belangrijkste. In de tabel hieronder een overzicht van de belangrijkste criminaliteitsvorm(en)⁴ om aan te pakken naar sector.

Tabel 6: Belangrijkste criminaliteitsvorm(en)om aan te pakken naar sector.

Sector	Belangrijkste criminaliteitsvorm
Bouwnijverheid (n=11)	Cybercrime & Inbraak
Financiële dienstverlening (n=8)	Cybercrime
Handel (n=95)	Diefstal van buitenaf
Horeca (n=28)	Geweld tegen personeel
Landbouw, bosbouw en visserij (n=54)	Diefstal van buitenaf
Overige dienstverlening (n=31)	Ondermijning en diefstal van buitenaf

Verhuur/handel onroerend goed (n=8)	Fraude
Vervoer en opslag (n=11)	Diefstal van buitenaf
Zakelijke dienstverlening (n=31)	Cybercrime
Industrie (n=7)	Cybercrime
Overig (n=14)	Cybercrime

Zzp versus mkb

De rangorde verschilt enigszins als gekeken wordt naar zzp'ers enerzijds en mkb'ers anderzijds:

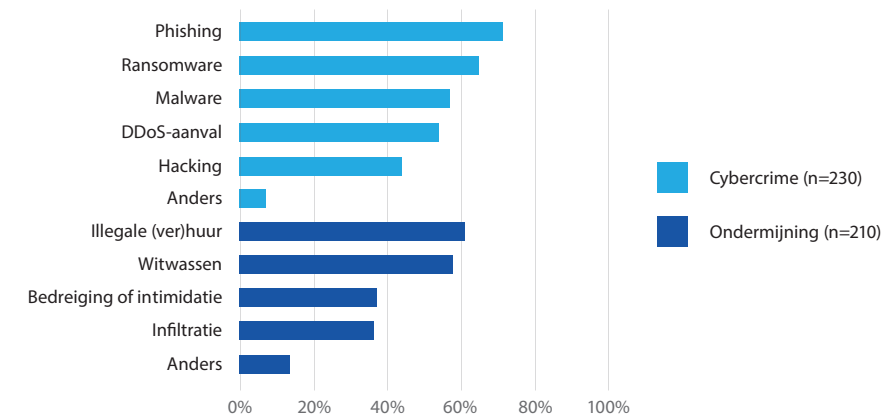
Zzp (n=54)	Mkb (n=244)
1. Cybercrime	1. Diefstal van buitenaf
2. Diefstal van buitenaf	2. Cybercrime
3. Inbraak	3. Inbraak
4. Bedreiging	4. Overvallen
5. Ondermijning	5. Geweld tegen personeel

Het huidige actieprogramma Veilig Ondernemen richt zich voornamelijk op de criminaliteitsvormen cybercrime en ondermijnende criminaliteit. Respondenten is gevraagd of zij een gezamenlijke aanpak van deze twee criminaliteitsvormen belangrijk vinden, en zo ja, om welke vormen van cybercrime en ondermijnende criminaliteit het dan gaat. Ruim drie kwart van de respondenten (77%) geeft aan dat het belangrijk is om cybercrime gezamenlijk aan te pakken. Zeventig procent

4. Voor sommige sectoren geldt dat er niet één, maar twee criminaliteitsvormen als belangrijkste worden gezien.

van de respondenten vindt een gezamenlijke aanpak voor ondermijnende criminaliteit belangrijk. De vormen van cybercrime en ondermijnende criminaliteit die volgens de ondernemers belangrijk zijn voor de aanpak staan gepresenteerd in figuur 7.

Figuur 7: Vormen van cybercrime en ondermijning die ondernemers belangrijk vinden om aan te pakken



Inhoud aanpak

Aan de ondernemers is ook gevraagd naar suggesties voor de toekomstige aanpak. Het belangrijkste vinden respondenten dat ondernemingen weerbaarder/minder kwetsbaar worden tegen criminaliteit. Deels zit deze wens ook verweven in andere suggesties, bijvoorbeeld door het vergroten van kennis, ondernemers die samenwerken, hulp bij problemen/vragen en het opstarten van campagnes.

Tabel 7: Rangorde inhoud aanpak naar belangrijkheid (n=221)

1.	Onderneming weerbaarder maken tegen bepaalde criminaliteitsvormen
2	Publiek-private samenwerking om minder kwetsbaar te zijn voor bepaalde criminaliteitsvormen
3.	Vereenvoudigen van het doen van aangifte bij de politie
4.	Vergroten (inhoudelijke) kennis over bepaalde criminaliteitsvormen
5.	Onderling waarschuwingssysteem als criminelen in mijn omgeving actief zijn
6.	Samenwerken met andere ondernemers om minder kwetsbaar te zijn voor bepaalde criminaliteitsvormen
7.	Hulp bij probleemoplossing
8.	Betere regelgeving
9.	Ik heb behoefte aan een andere inhoudelijke aanpak
10.	Een meldpunt voor vragen
11.	Campagnes (landelijk, lokaal of per sector)



Mening van stakeholders en ondernemers

Om inzicht te krijgen in de verschillende vormen van (on)bewust gefaciliteerde criminaliteit in het bedrijfsleven zijn er vijf panelgesprekken gevoerd en twee individuele interviews. Uiteindelijk is met 30 stakeholders gesproken. Het betreft stakeholders die werkzaam zijn in de wetenschap, de veiligheidsbranche, binnen de overheid en in het bedrijfsleven. Vanuit hun functie beschikken zij over expertise op het thema 'criminaliteit tegen en gefaciliteerd door het bedrijfsleven'. De stakeholders zijn op vijf thema's bevraagd: vormen van criminaliteit die actueel zijn, vormen van ondermijnende criminaliteit, vormen van cybercrime, aandachtspunten in de huidige aanpak en suggesties voor toekomstige aanpak. Ook zijn ondernemersverenigingen via mail benaderd met de vraag met welke criminaliteit zij te maken hebben en welke aanpak daartegen ingezet moet worden. De respons hierop was dermate laag dat dit hoofdstuk voornamelijk een weergave is van de panelgesprekken.

14

Vormen van criminaliteit waar het bedrijfsleven volgens stakeholders vooral mee te maken heeft

De stakeholders zijn het erover eens dat ondermijnende criminaliteit en cybercrime belangrijke thema's zijn voor het nieuwe actieprogramma (2023-2026) van het NPC. Wat betreft cybercrime wordt onderscheid gemaakt tussen cybercrime (bijvoorbeeld hacken, DDos-aanvallen, malware of phishing) en digitale criminaliteit (bijvoorbeeld het plegen van online identiteitsfraude, online diefstal of aankoopfraude). Beide vormen komen regelmatig terug in de panelgesprekken met stakeholders.

Daarnaast benadrukken zij ook het belang van aandacht voor de volgende vormen van criminaliteit:

- Diefstal binnen verschillende sectoren; bijvoorbeeld (lading)diefstal in het goederentransport en het stelen van diesel uit vrachtwagens. Ook komt diefstal van koperen leidingen of (dure) machines en/of materiaal binnen de agrarische sector voor. En ondernemingen op bedrijventerreinen blijven slachtoffer van diefstal.
- Fysieke overvallen, plofkraak, winkeldiefstal en vooral ook de toenemende agressiviteit en bedreigingen van personen en personeel in winkels. Ook gaat het om overvallen op horecagelegenheden en in de 'fastservice' (bijvoorbeeld maaltijdsbezorgingen). Vooral deze laatste vorm draagt volgens stakeholders bij aan de trend van steeds impulsiever wordende criminaliteit.
- Gewelddelicten; de vroegere kluisroven zijn nu kassagrepen geworden. De retail-branchen zien juist voor deze vorm een daling in de gemiddelde leeftijd van daders.
- (Illegale) pandverhuur voor arbeidsmigranten, uitbuiting (huisjesmelkers) of voor drugshandel en -productie.
- Frauduleuze zaken rond het bankwezen, zowel in de bankomgeving (re-routings door criminelen) als in de klantomgeving (contact met een zogenaamde bankmedewerker of de 'vriend-in-noodfraude'). Ook worden er nog steeds veel witwaspraktijken gezien binnen het bankwezen.
- Zorgfraude, waarbij zorgaanbieders (on)bedoeld regels overtreden bij het bieden van zorg en zorgbehoevende burgers raken hier de dupe van.
- *Human trafficking*; mensen die op bedrijventerreinen binnengebracht worden in vrachtwagens.

Ondermijnende criminaliteit volgens stakeholders

Uit vorig onderzoek en het actieprogramma 2019-2022 van het NPC is gebleken dat ondermijnende criminaliteit een veelal onzichtbaar verschijnsel is en dat het veel verschillende verschijningsvormen kent. Een stakeholder merkt hierover het volgende op: *'Ondermijning is een "ballonbegrip", er valt heel veel onder tegenwoordig*

dig'. In de panelgesprekken worden de volgende concrete voorbeelden van deze criminaliteitsvorm genoemd:

- Katvangers die panden huren voor criminele activiteiten, bijvoorbeeld voor hennepkwekerijen of drugslabs.
- Hennepkwekerijen, illegale sigarettenfabrieken, drugslabs, postbusbedrijven, illegale prostitutie en illegale bewoning door arbeidsmigranten op bedrijventerreinen. Bedrijven kunnen zowel slachtoffer als facilitator van criminaliteit zijn. Specifiek worden buitengebieden (bijvoorbeeld het platteland) als risicolocatie genoemd.
- De aanvoer van drugs via grote logistieke ketens, in het bijzonder luchthaven Schiphol en de haven van Rotterdam. De bijkomende massale stroom aan 'uithalers' in de haven van Rotterdam is problematisch. Daarnaast wordt de export van synthetische drugs geproduceerd in Nederland richting het Verenigd Koninkrijk genoemd.
- Geconditioneerd transportvervoer wordt bijvoorbeeld – bedoeld of onbedoeld - als dekmantel gebruikt om drugs vanuit het buitenland met hoge snelheid door heel Europa te kunnen vervoeren.
- Milieucriminaliteit in het buitengebied, zoals gedumpte (drugs)afval.
- Illegale prostitutie en drugshandel in hotels.

Tevens wordt in de panelgesprekken aangehaald dat het integer handelen binnen bepaalde sectoren onder druk staat. Mede door de coronapandemie, maar ook door de stikstofbeperkingen *'staat het water tot aan de lippen'* bij sommige bedrijven. Dit maakt bedrijven vatbaarder voor criminele inmenging wanneer er ineens een grote som geld wordt aangeboden om bijvoorbeeld een (leegstaand) pand te huren.

Cybercrime volgens stakeholders

In de panelgesprekken werd er onderscheid gemaakt tussen cybercrime (bijvoorbeeld hacken, DDos-aanvallen, malware of phishing) en digitale criminaliteit (bijvoorbeeld het plegen van online identiteitsfraude, het niet betalen van online

bestelde goederen of online diefstal). Desondanks zeggen sommige experts dat *'zaken niet altijd los van elkaar te zien zijn; soms wordt binnen cybercrime ook diefstal gepleegd.'* Cybercrime betreft delicten waarbij ICT het middel en het doel is, terwijl digitale criminaliteit ook de wat traditionelere criminaliteit behelst, via digitale weg uitgevoerd. Bijna alle stakeholders benadrukken het toenemend belang van het weerbaar zijn tegen cybercrime en digitale criminaliteit: *'het is niet de vraag of, maar wanneer er een cyberaanval komt'*. De volgende aandachtspunten worden door stakeholders genoemd:

- Er is sprake van steeds meer digitale criminaliteit, bijvoorbeeld marktplaatsfraude, online (aankoop)fraude of frauduleuze webwinkels die geen spullen leveren. Dit wordt bevestigd door enkele stakeholders, die aangeven dat hun achterban last heeft van personen die bestellen maar niet betalen.
- Er lijkt sprake van verschil in de mate van cybersecurity tussen grote en kleine bedrijven. Vaak hebben de grote organisaties een aparte IT-afdeling, of zelfs een cybersecurity-afdeling en zijn ze goed op de hoogte van de mogelijke online gevaren, terwijl de gemiddelde (kleine) mkb'er nog steeds erg weinig aan cybersecurity doet en amper bewust is van online slachtofferschap.
- Er worden veel ransomware geplaatst en DDos-aanvallen uitgevoerd op ondernemers, waarbij soms accounts ook worden gehackt om er identiteitsfraude mee te plegen. Online reputatieschade, doxing (publicatie van gegevens om bedrijven te intimideren) en het verspreiden van online desinformatie zijn ook een probleem. Er is volgens stakeholders sprake van een toename in incidentie en schade door dit soort praktijken.
- Ook proberen criminelen via (informatie)diefstal bij kleinere onderaannemende bedrijven binnen te komen, om vervolgens door te stoten richting de "grote spelers". Dit roept de vraag op of er een gedeelde verantwoordelijkheid moet komen tussen de grote en kleine bedrijven.

Visie van stakeholders op de huidige aanpak

Op diverse onderzoek- en beleidsterreinen wordt al veel gedaan om (on)bewust gefaciliteerde criminaliteit in het bedrijfsleven tegen te gaan. De stakeholders geven aan dat dit ook tot de nodige aandachtspunten leidt. Achtereenvolgens benoemen zij de volgende aandachtspunten:

- De opvolging van meldingen laat volgens de stakeholders te wensen over. Veel ondernemers wijzen in dit kader naar de nog steeds aanwezige capaciteitsproblemen (bijvoorbeeld bij de politie). Het gevolg is dat het vertrouwen in de overheid om te meldingen tot een goed einde af te handelen daalt. Dit leidt weer tot een verdere afname van de meldingsbereidheid en verminderd zicht op de prevalentie van criminaliteit tegen- en gefaciliteerd door het bedrijfsleven.
- Ondernemers lijken ook bang voor reputatieschade omdat hun persoonsgegevens wellicht op straat komen te liggen na een melding.
- Daarnaast zijn valse KvK-gegevens (bij aankoopfraude) of anonieme daders (bij ransomware/DDos-aanvallen) moeilijk te herleiden naar de daders. Vaak vindt er dan geen dadervervolgning plaats, wat het vertrouwen in de aangifte-afhandeling schaadt. Onder stakeholders leeft nu het gevoel dat *'aangiften soms meer een middel zijn voor meta analyse dan voor daadwerkelijke actie. De aangifte is vooral belangrijk voor de statistieken, maar voor mijn persoonlijke situatie lost het niks op.'*
- Privacywetgeving, zoals de AVG, en aanvullende regulering vanuit de Autoriteit Persoonsgegevens belemmeren de opsporing en vervolging volgens veel stakeholders. Diverse ondernemers die deelnamen aan de panelgesprekken zouden graag informatie over dieven, fraudeurs of louche huurders willen delen om elkaar te waarschuwen voor deze personen, maar dit is vaak niet mogelijk.
- In de panelgesprekken is meerdere keren over het Damoclesbeleid gesproken. Het Damoclesbeleid stelt gemeenten in staat om panden voor langere tijd te sluiten wanneer de Opiumwet wordt overtreden. Dit benadeelt de verhuurder volgens stakeholders, met als gevolg dat zijn/haar meldings-

bereidheid daalt en zij zelf illegale huurders eruit proberen te werken, hetgeen kan eindigen met onveilige situaties.

- De huidige aanpak rond milieucriminaliteit (in het buitengebied) wordt door enkele stakeholders bekritiseerd; vooral toezicht en handhaving door de overheid schiet te kort. Bedrijven hebben regelmatig afvaladministratie niet op orde. Dit beschouwen stakeholders als voedingsbodem voor milieucriminaliteit.

Visie van stakeholders op aanpak voor de toekomst

De stakeholders en vertegenwoordigers van ondernemersverenigingen dragen diverse aanknopingspunten aan voor toekomstige aanpak. Puntsgewijs gaat het om de volgende suggesties:

- Zorg dat lokale problemen, fenomenen en behoeften goed inzichtelijk worden. Allereerst begint dit met het creëren van meer bewustzijn onder ondernemers omtrent de risico's van criminaliteit in de eigen omgeving. Vervolgens zou informatie goed gedeeld moeten worden op lokale platforms, waar ook de wijkagent bij aansluit.
- De wens bestaat om ook op landelijk niveau een platform met instrumenten en informatie te creëren, om bewustzijn bij ondernemers rond de voor hen relevante criminaliteitsvormen te bevorderen.
- Maak jongeren bewuster van de risico's van criminaliteit in het bedrijfsleven, zodat zij kunnen fungeren als potentiële melder. Deze bewustwording zou op scholen al moeten plaatsvinden.
- Doe meer aan *naming and shaming*, om de pakkans te verhogen.
- Laat bedrijven zich verenigen om AVG-drempels te overstijgen. Daardoor zouden persoonsgegevens van criminelen binnen de bedrijvenvereniging wel gedeeld mogen worden.
- Pak de anonimiteit op bedrijventerreinen aan; gemeenten zouden meer controles op locatie moeten uitvoeren. Daarnaast zouden er meer controles aan de voorkant uitgevoerd moeten worden, bijvoorbeeld via de Kamer van Koophandel. Ook moet de verhuurder controles uitvoeren; veel sta-

keholders vinden dat er nog enige mate van bewustzijn mist onder ondernemers/verhuurders over wat *red flags* kunnen zijn bij dubieuze huurders. Ook wordt geopperd om een (wijk)agent of een particuliere partij een vorm van "conciërgefunctie" te geven, waardoor meer (sociale) controle is op bedrijventerreinen. Een (wijk)agent zou dan gekoppeld kunnen worden aan de bijeenkomsten van ondernemersverenigingen.

- Maak gebruik van al bestaande goede praktijkvoorbeelden. Een voorbeeld is het pilotconvenant tegen de gevolgen van het Damoclesbeleid in Gemert-Bakel, Hazeldonk en Helmond.⁵ Op grond van dit convenant wordt het pand van de verhuurder minder snel gesloten voor een langere periode, zelfs als de Opiumwet is overtreden. Een ander voorbeeld is het markeren van agrarische machines en apparatuur plaatjes die niet van de machine of de apparatuur is te halen, zodat de goederen te koppelen zijn aan het bedrijf. En de hotelbranche kan potentiële criminele activiteiten tegen gaan door simpelweg strengere identiteitscontroles van de huurders van kamers uit te voeren.
- Laat ondernemers een digitale analyse uitvoeren, om mogelijke zwakke schakels binnen de cybersecurity te identificeren en op te lossen. Particuliere initiatieven zouden hierbij ook kunnen helpen, bijvoorbeeld via verzekeraars; sommigen stellen al bepaalde voorwaarden aan de cybersecurity van mkb'ers, bijvoorbeeld via lager uitvallende premies wanneer de cybersecurity op orde is.
- Zet in op verstoring als het gaat om cybercrime, door snel te melden dat er cyberaanvallen gepleegd worden. Dit voorkomt volgens stakeholders problemen bij andere ondernemers. In het verlengde hiervan leeft het idee dat ICT-organisaties scherper gecertificeerd moeten worden; een keurmerk waardoor mkb'ers verzekerd zijn van een basisbescherming in hun onli-

5. Meer informatie www.zlto.nl/actueel/gemert-bakel-samen-met-zlto-drugscriminaliteit-te-lijf

ne omgeving. Een idee is om deze certificering te koppelen aan lagere een lagere verzekeringspremie.

- Voer structurele controles op afvalregistratie bij bedrijven uit, om hier vervolgens ook op te handhaven. Enkele stakeholders suggereren dat het creëren van meer binding tussen politie, groene BOA's en de agrarische ondernemers in het buitengebied kan helpen bij de signalerings- en meldingsbereidheid.
- Naast aangiften, al dan niet via Meld Misdaad Anoniem, zou er ook een meldpunt moeten komen voor vermoedens van verdachte activiteiten. Andere stakeholders stellen voor om een speciale Meld Misdaad Anoniem voor ondernemers te creëren, zodat de drempel tot melden verlaagd voor hen wordt.
- Blijf zoeken naar innovatieve (publiek-)private maatregelen om (on)bewust gefaciliteerde criminaliteit tegen te gaan. Goede voorbeelden hiervan zijn de ServiceOrganisatie Directe Aansprakelijkstelling (SODA) waardoor overgegaan wordt op civielrechtelijke aansprakelijkheidsstelling van bijvoorbeeld personen die tanken zonder te betalen. Een ander voorbeeld is de recente inzet van deurwaarders na online handelsfraude.



De bevindingen in samenhang bekeken

In 2018 heeft het onderzoek 'Agenda voor de toekomst' van Bureau Beke input geleverd voor het actieprogramma 2019-2022 van het Nationaal Platform Criminaliteitsbeheersing. Nu het actieprogramma bijna is afgelopen, is het van belang om te werken aan een nieuw actieprogramma, voor de jaren 2023-2026. Ook hiervoor heeft Bureau Beke input geleverd door verschillende onderzoeksactiviteiten uit te voeren. Het gaat dan om een deskresearch, een online survey onder ondernemers (N=298), het raadplegen van ondernemersverenigingen en het voeren van panelgesprekken met stakeholders (MKB, ministerie van JenV, OM, politie, brancheorganisaties, et cetera, N=30).

Aan het eind van deze notitie is het de vraag in hoeverre de input uit de diverse onderzoeksactiviteiten elkaar ondersteunt. Met andere woorden: in hoeverre komen de opgetekende onderzoeksbevindingen vanuit meerdere invalshoeken terug? Hiervoor maken we onderscheid tussen a) vormen van criminaliteit waarmee ondernemers vooral te maken hebben en b) suggesties voor de aanpak van criminaliteit.

a) Criminaliteitsvormen waarmee ondernemers vooral te maken hebben

In tabel 8 is per bron weergegeven welke vormen van criminaliteit tegen het bedrijfsleven sinds 2018 (vanuit de deskresearch) en actueel (vanuit de survey en de panelgesprekken) centraal staan. De benoemde subvormen van cybercrime en ondermijnende criminaliteit staan eveneens in de tabel vermeld.

Tabel 8: Benoemde criminaliteitsvormen die sinds 2018 actueel zijn

Criminaliteitsvorm	Bron		
	Deskresearch	Survey	Panelgesprekken
Cybercrime			
Cybercrime algemeen	x	x	
Ransomware	x	x	x
Hacken	x	x	
Phishing	x	x	
CEO-fraude	x		
DDos-aanval	x	x	x
Malware	x	x	
Social engineering	x		
BEC-fraude	x		
'Vriend-in-nood'-fraude			x
Doxing			x
Verspreiden van desinformatie			x
Digitale criminaliteit			
Marktplaatsfraude			x
Online (aankoop)fraude			x
Frauduleuze webwinkels			x
Ondermijning			
Ondermijning algemeen	x	x	
Bedreiging en intimidatie	x		
Criminele financiering	x		
Drugscriminaliteit	x		x
Witwassen		x	x
Illegale (ver)huur		x	x
Infiltratie		x	
Verduisteren van voertuigen		x	
Human-trafficking			x
Milieucriminaliteit			x
Illegale prostitutie			x

Afpersing/bedreiging	x	x	x
Vermogensdelicten	x		
Diefstal van buitenaf		x	x
Diefstal door personeel		x	
Overval		x	x
Inbraak		x	
Plof- en ramkraken		x	
Zorgfraude			x

Vanuit alle bronnen worden de diverse criminaliteitsvormen grotendeels wel genoemd. Wat opvalt, is dat de stakeholders in de panelgesprekken als enige aandacht vragen voor vormen van 'digitale criminaliteit', zoals online (aankoop)fraude. Wanneer alle bronnen in samenhang bekeken worden, dan vormen cybercrime, diefstal van buitenaf en inbraak de vormen van criminaliteit waarmee ondernemers (zowel zzp'ers als de rest) in hoofdzaak te maken heeft. Dit is wel afhankelijk van de sector waar men werkzaam is; bijvoorbeeld in de sectoren waar goederen voorhanden zijn, is diefstal van buitenaf een probleem, terwijl dienstverlenende bedrijven veel te maken hebben met cybercrime. Een aandachtspunt is dat sommige bedrijven in financiële moeilijkheden zitten, onder andere door de coronapandemie en stikstofbeperkingen, en daardoor gevoeliger lijken voor een stap richting bewuste deelname aan criminaliteit. Ook is van belang te vermelden dat er verschillen tussen grote en kleine bedrijven lijken te ontstaan in de mate waarin bedrijven hun cybersecurity op orde hebben.

b) Suggesties voor aanpak van criminaliteit

In de literatuur/mediaberichten, in de survey en in de panelgesprekken zijn diverse suggesties gegeven voor de aanpak van criminaliteit in het bedrijfsleven. Deze suggesties hebben betrekking op verschillende thema's, zoals preventie, repressie, informatiedeling en monitoring. De suggesties worden in de volgende tabel aan een thema gekoppeld.

Tabel 9: Suggesties voor de aanpak van criminaliteit naar thema

Thema	Suggestie
Bewustwording en preventie	• zet een informatieplatform op, met daarop concrete fenomenen en instrumenten om criminaliteit te bestrijden • maak ondernemers weerbaarder door meer informatieverstrekking en publiek-private samenwerking • creëer een helpdesk als er problemen na criminaliteit zijn • denk naast publiek-private samenwerking ook aan oplossingen door als ondernemers zelf samen te werken • blijf ook lokaal periodiek terugkerende informatieavonden organiseren
Repressie	• vereenvoudig het doen van aangifte/stimuleer het melden via Meld Misdaad Anoniem/stimuleer melden via de Vertrouwenslijn Afpersing • stimuleer het melden van criminaliteit, al was het maar door middel van een meldpunt (ipv aangifte)
Toezicht en handhaving	• voer met name in buitengebieden en op bedrijventerreinen meer toezicht uit • ondersteun benadeelde ondernemers door een sluiting op grond van de Wet Damocles te verkorten
Informatie-huishouding	• maak gebruik van al bestaande convenanten • verbeter het inzicht in hoe om te gaan met de AVG en andere regels • laat bedrijven zich verenigen om onderling melden te faciliteren • bekijk te mogelijkheden binnen de AVG om namen en rugnummers van criminelen te verspreiden
Monitoring en uitvoeren audits	• voer een digitale analyse van bedrijven in, bij voorkeur uitgevoerd door gecertificeerde IT-bedrijven
Communicatie	• meld sneller en breder dat cyberaanvallen plaatsvinden • betrek de burger, bijvoorbeeld jongeren, meer als potentiële melder

Colofon

In opdracht van:
Ministerie van Justitie en Veiligheid

Realisatie:
Bureau Beke, Arnhem

Foto's:
Unsplash.com

© Bureau Beke, 2022



bureaubeke.nl