

Vergaderjaar 2014–2015

29 911

Bestrijding georganiseerde criminaliteit

Nr. 95

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 oktober 2014

Hierbij bied ik u het onderzoeksrapport «Ondergaan of Ondernemen» aan van Bureau Beke aangaande het actuele beeld van afpersing van het bedrijfsleven in Nederland¹.

Aanleiding

Afpersing van bedrijven kan gepaard gaan met veel schade en financieel en persoonlijk leed voor de slachtoffers. Naast de grote impact van dit delict op slachtoffers brengt dit delict een risico op uitermate onwenselijke vermenging van onder- en bovenwereld met zich mee. Dit maakt dat de bestrijding van afpersing de voortdurende aandacht van het Ministerie van Veiligheid en Justitie heeft.

Eerder onderzoek in 2007 wees uit dat bedrijven ondanks deze forse impact weinig aangifte doen². Dit maakt dat afpersing zich voor een deel buiten het zicht van politie en justitie afspeelt. Om te zorgen dat de bestrijding van afpersing blijft aansluiten bij de actuele verschijningsvormen is in opdracht van mijn ministerie opnieuw onderzoek uitgevoerd met als doel de actuele stand van zaken met betrekking tot afpersing van het bedrijfsleven in kaart te brengen. Daarnaast evalueert het onderzoek of de aanpak die sinds 2010 is ingezet volgens plan verloopt en of de maatregelen nog effectief zijn om het probleem van de afpersing te kunnen bestrijden.

Samenvatting

Het aantal gevallen van afpersing is, naar de ervaring van deskundigen uit verschillende Europese landen, de laatste jaren toegenomen. Vooral protectie- en cyberafpersing zijn in opkomst. Bij de ontwikkeling van protectieafpersing, de meest klassieke vorm van het delict, gaat het met

¹ Raadpleegbaar via www.tweedekamer.nl

² Leiden, I. van, E. de Vries Robbé & H. Ferwerda (2007). Je bedrijf of je leven: aard en aanpak van afpersing van het bedrijfsleven.

name om afpersing van horecaondernemers door Outlaw Motorcycle Gangs (OMG's). Bij cyberafpersing gaat het om het onrechtmatig verkrijgen van gegevens door hacken en het dreigen deze openbaar te maken, het (tijdelijk) ontoegankelijk maken van gegevens door middel van *ransomware*, of het dreigen om websites onbereikbaar te maken door ddos-aanvallen.

De onderzoekers geven op basis van politieregistraties, rechterlijke uitspraken en zelfrapportage een voorzichtige indicatie van de omvang van afpersing van bedrijven in Nederland. Jaarlijks komen er gemiddeld 55 afpersingszaken ter kennis van de politie en komen gemiddeld 11 afpersingszaken voor de rechter. De verdachten van afpersing zijn relatief vaak bekenden van het slachtofferbedrijf zoals voormalige zakenrelaties, ex-klanten en ex-werknemers. De zelfrapportage wijst op een grotere omvang van de problematiek: één op de tien ondernemers geeft aan in de afgelopen vijf jaar een of meerdere malen slachtoffer te zijn geworden van afpersing. Opvallend is dat in de zelfrapportage vooral criminele dadergroepen worden genoemd, terwijl deze dadergroepen in de politieregistraties rondom afpersing nauwelijks voorkomen. Hoewel de onderzoekers wijzen op aanzienlijke beperkingen van de drie bronnen ten aanzien van de inhoud, kwaliteit en representativiteit, concluderen zij dat afpersing, zeker door criminele dadergroepen, een groter probleem voor het bedrijfsleven vormt dan uit het aantal aangiften en rechterlijke uitspraken blijkt.

Aan deze discrepantie liggen volgens de onderzoekers twee oorzaken ten grondslag. In de eerste plaats is er sprake van een lage bereidheid om aangifte te doen van afpersing. Terwijl een meerderheid van de ondernemers (87%) aangeeft de politie te zullen inschakelen in het geval zij worden afgeperst, blijkt een veel lager percentage van de ondernemers die slachtoffer zijn van afpersing (44%) daadwerkelijk over te gaan tot het doen van aangifte. Slachtoffers hebben angst voor represailles van de afpersers, vrezen imagooverlies of hebben onvoldoende vertrouwen dat de politie de zaak zou kunnen oplossen. In de tweede plaats is er sprake van barrières aan politiezijde. Zo stelt het rapport dat het kennisniveau van baliepersoneel van de politie soms tekort schiet en dat afpersingszaken daardoor soms verkeerd geïdentificeerd worden of onvoldoende urgentie krijgen.

Uit het onderzoek komt tevens naar voren dat speciaal ingerichte voorzieningen zoals de vertrouwenslijn afpersing nauwelijks bekend zijn bij de doelgroep. De onderzoekers doen de suggestie om naast de politie ook andere partijen bij de signalering te betrekken. Zij noemen Kamers van Koophandel, het notariaat, brancheorganisaties, gemeenten en het Nationaal Cyber Security Centrum.

Naar aanleiding van ongeveer vier op de tien aangiften worden opsporingshandelingen verricht. Dat niet alle zaken worden opgepakt past bij de realiteit dat een deel van de afpersingszaken bij een poging blijft en vanzelf stopt. Dat betekent echter wel dat ook pogingen tot afpersing, die eveneens strafbaar zijn, soms geen vervolg krijgen. Uit het onderzoek blijkt dat wanneer er wél opsporingshandelingen worden verricht deze meestal succesvol zijn. Slachtoffers ervaren de begeleiding en aanpak van opsporingsmedewerkers over het algemeen als professioneel.

Gemiddeld vinden er jaarlijks ongeveer elf rechtszaken plaats inzake afpersingen van het bedrijfsleven. In het merendeel van deze zaken volgt een veroordeling van de verdachten variërend van taakstraffen tot jarenlange gevangenisstraffen.

De politie zo snel mogelijk inschakelen blijkt een belangrijke succesfactor voor vervolging. Op die manier heeft de politie de mogelijkheid om bewijs te vergaren tijdens het afpersingsproces.

In 2010 hebben publieke en private partijen de handen ineen geslagen om, onder auspiciën van het Nationaal Platform Criminaliteitsbeheersing, projecten te initiëren om afpersing aan te pakken of te voorkomen. Met vijf deelprojecten is ingezet op vergroting van de kennis en weerbaarheid van ondernemers, verbetering van de vertrouwensrelatie tussen publieke en private partijen en verdere professionalisering bij de politie ten aanzien van de aanpak van afpersing. De onderzoekers concluderen dat resultaten zijn geboekt, maar dat ook een deel van de projecten onvoldoende van de grond heeft kunnen komen. Bij het bereiken van die resultaten zijn communicatie, structurele borging van voorzieningen en goede samenwerking cruciaal gebleken. De onderzoekers noemen in dit kader nog enkele kansen voor de aanpak van afpersing. Hieraan geef ik samen met het bedrijfsleven als volgt nadere invulling.

Aanpak afpersing 2014 tot 2016

In het Nationaal Platform Criminaliteitsbeheersing zijn in december 2013 zes hoofdthema's benoemd waar de publiek-private aanpak zich de komende jaren op zal richten. Naast (horizontale) fraude, transportcriminaliteit, heling, mobiel banditisme en cybercriminaliteit is afpersing een fenomeen waar de partners van het NPC de inzet duidelijk op versterken.

Met ingang van 1 januari 2015 zal de vertrouwenslijn Afpersing worden belegd bij NL Confidential (voorheen Stichting M). Hiermee wordt een structurele voorziening gecreëerd, waar (mogelijke) slachtoffers van afpersing terecht kunnen voor een luisterend oor, melding van hun slachtofferschap en handelingsperspectief voor hun specifieke situatie. Daarnaast zal in voorkomende gevallen persoonlijke begeleiding aan het slachtoffer worden gegeven.

Daarnaast worden in 2015 weer zogenoemde roadshows georganiseerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) waarbij experts het lokale bedrijfsleven, het lokale bestuur en andere betrokken partijen informeren over afpersing en met hen in gesprek gaan over het belang van bewustwording en signalering. Uit het rapport blijkt dat deze vormen van communicatie effectief zijn. Hierbij is het – zoals de onderzoekers ook aangeven – van belang dat ook de omgeving van ondernemers zoals familieleden, zakelijke partners en -contacten zich bewust zijn van mogelijke signalen voor afpersing. De onderzoekers stellen dat van groot belang is dat slachtofferschap van afpersing uit de taboesfeer komt. Om voorgaande te realiseren wordt de komende jaren ingezet op structurele en heldere communicatie over het fenomeen, de vertrouwenslijn en handelingsperspectieven. Hier zie ik ook een belangrijke rol weg gelegd voor het (georganiseerde) bedrijfsleven en zal daarom gezamenlijk met betrokken partijen in het Nationaal Platform Criminaliteitsbeheersing (NPC) – waaronder het georganiseerde bedrijfsleven – concrete acties formuleren met betrekking tot de communicatie en bewustwording van ondernemers. Het georganiseerde bedrijfsleven zal hun diverse communicatiekanalengericht inzetten en waar mogelijk gebruik maken van free publicity. Omdat afpersing meerdere vormen kent, zullen vorm, inhoud en boodschap zorgvuldig worden afgestemd op de verschillende doelgroepen binnen het bedrijfsleven. De algemene boodschap aan (potentiële) afpersers is echter helder: «afpersing pikken we niet».

In het onderzoek worden Outlaw Motorcycle Gangs genoemd als dadergroep die in eerder onderzoek met betrekking tot afpersing van het bedrijfsleven niet naar voren is gekomen. OMG's vormen in het algemeen een bedreiging van de openbare orde en de veiligheid en maken zich schuldig aan georganiseerde criminaliteit en ondermijning of normoverschrijdend gedrag, waaronder ook afpersing. De aanpak van OMG's heeft zodoende een hoge prioriteit bij het OM en de politie. Samen met het lokale bestuur, de Belastingdienst, FIOD en het Landelijk Informatie en Expertisecentrum (LIEC) en de Regionale Informatie en Expertisecentra (RIEC's) zijn deze partijen intensief aan de slag om deze problematiek integraal aan te pakken.

In een voortgangsbrief³ d.d. 20 juni 2014 heb ik u geïnformeerd over de resultaten van de aanpak van OMG's, waaronder strafrechtelijke vervolging, het sluiten van clubhuizen en een pilot van Meld Misdaad Anoniem (M.) in de horeca. Er is voor deze pilot voor de horeca gekozen, omdat daar specifiek sprake is van protectieafpersing door onder andere OMG's en er schroom bestaat om met de politie te spreken over de praktijken of daarvan aangifte te doen uit angst voor represailles. De pilot vond plaats in 2 gemeenten (Arnhem en Alkmaar/Heerhugowaard) met als doel meer strafrechtelijke onderzoeken en integrale handhavingsacties ten aanzien van outlawbikers te starten, door meer meldingen en aangiften te bewerkstelligen van onder andere intimidatie, bedreigingen, geweld, afpersing, opiumwetdelicten, witwassen en wapenhandel. Het delen van informatie en kennis tussen gemeente, politie, OM en lokale – al dan niet getroffen – ondernemers is daarbij cruciaal. De evaluatie van de pilot wordt op dit moment afgerond en ik kijk uit naar de resultaten.

Naast het specifieke slachtofferschap in de horeca, geldt dat vormen van cyberafpersing als ransomware en cryptoware volgens het onderzoek steeds vaker voorkomen. Ook het vierde Cyber Security Beeld Nederland (CSBN4) van 10 juli 2014⁴) benoemt de opkomst van ransomware en cryptoware. Het CSBN4 signaleert ook dat cybercrime vaak internationaal van aard is en veelal in georganiseerd verband wordt gepleegd. In de tweede Nationale Cyber Security Strategie van 28 oktober 2013⁵ is de bestrijding van cybercrime één van de hoofddoelstellingen. De strategie bevat onder meer actiepunten voor versterking van de wetgeving, de capaciteit voor onderzoek en het intake- en registratieproces van aangiften. Dat sluit aan op het signaal uit het onderzoek dat er behoefte is aan meer capaciteit voor de opsporing als het gaat om cyberafpersing.

De politie heeft de afgelopen jaren stevig geïnvesteerd in het Team High Tech Crime, dat dit jaar groeit naar een omvang van 119 vte. De aanpak van ransomware is voor het team een prioriteit. De politie werkt nauw samen met de financiële sector in de Electronic Crime Task Force (ECTF), onder meer om gezamenlijk nieuwe werkwijzen van criminelen te onderkennen en kennis te delen om tot een effectieve aanpak te komen. De capaciteit en kennis op het gebied van cybercrime wordt ook in de regionale eenheden verder ontwikkeld. Door de versterking van de digitale expertise op regionaal niveau wordt een kwaliteitsslag gemaakt en kan het Team High Tech Crime zich meer toeleggen op nieuwe en technologisch geavanceerde werkwijzen van criminelen. Deze lijn wordt onderstreept in de afspraken die ik heb gemaakt met de regioburgemeesters, het college van procureurs-generaal en de politie in de Veiligheidsagenda 2015–2018, waarover ik uw Kamer per brief op

³ Kamerstuk 28 684, nr. 407

⁴ Kamerstuk 26 643, nr. 322

⁵ Kamerstuk 26 643, nr. 291

16 september jl. heb geïnformeerd⁶. Het aantal cybercrime onderzoeken stijgt naar 360 in 2018 en er worden meer complexe zaken aangepakt, tenminste 50 in 2018.

De onderzoekers merken bovendien op dat er behoefte is aan een beter aangifteproces als het gaat om afpersing. In mijn brief d.d. 20 november 2012⁷ heb ik uw Kamer al geïnformeerd over de maatregelen die ik neem ten aanzien van de verbetering van de aangifte in het algemeen. Binnen de politie zal bovendien het landelijk netwerk van deskundigen op het gebied van afpersing worden versterkt. Het herkennen van signalen van afpersing van ondernemers zal ook beter onder de aandacht worden gebracht bij intake medewerkers, wijkagenten en meldkamer medewerkers van de politie. Anderzijds zal de aangiftebereidheid van getroffen ondernemers – bij voorkeur in een vroeg stadium – flink moeten toenemen. Zo snel mogelijk melding maken van mogelijke afpersing is een belangrijke succesfactor voor opsporing en vervolging. Het vergroten van de aangiftebereidheid zal een belangrijk onderdeel zijn van de informatie en communicatie richting ondernemers.

De bovengenoemde wijzen van aanpak worden concreet uitgewerkt in een gezamenlijk publiekprivaat plan van aanpak onder het NPC. Dat betekent dat betrokken partijen als het (georganiseerde) bedrijfsleven, politie en OM en mijn Ministerie actief participeren in het aanpakken en terugdringen van afpersing en de kwalijke gevolgen daarvan.

De Minister van Veiligheid en Justitie,
I.W. Opstelten

⁶ Kamerstuk 28 684, nr. 412

⁷ Kamerstuk 29 628, nr. 340