Leren van publiek-private samenwerking in een afpersingszaak

Nicolien Kop, lector criminaliteitsbeheersing & recherchekunde aan de Politieacademie.

Publiek-private samenwerking (PPS) biedt kansen voor een toekomstbestendige opsporing. Dat blijkt ook uit een actuele afpersingszaak die nieuwe inzichten heeft opgeleverd over het gebruik van ICT als middel in afpersingszaken en forensische computertechnieken bij de opsporing. De opgedane kennis is op verzoek van de politie door onderzoekers van de Politieacademie vastgelegd in de vorm van leerpunten, waarvan de belangrijkste in dit artikel aan bod komen.

In 2016 werd een bedrijf gedurende een zestal weken afgeperst. Om te voorkomen dat de dreiger de daad bij het woord zou voegen, moest het bedrijf een groot geldbedrag in bitcoins betalen. Het bedrijf meldde de zaak direct bij de politie en deed aangifte. Dit was de start van een intensieve samenwerking.

Samenwerking

Zowel de politie als het bedrijf nam de dreiging uiterst serieus. Het bedrijf trof de nodige voorzorgsmaatregelen en startte met een analyse op wat het aan gegevens van de dreiger had. De politie begon met een regulier rechercheteam, maar koos al snel voor opschaling naar een Team Grootschalige Opsporing (TGO). Toen echter bleek dat daadwerkelijk 'spullen' waren verstuurd (in verband met de anonimiteit en herleidbaarheid laat ik buiten beschouwing wat voor spullen dit waren), werd de urgentie van de zaak nog groter en vond verdere opschaling plaats naar een Staf Grootschalig en Bijzonder Optreden (SGBO). De potentiële omvang van de zaak, de mogelijke impact van de dreiging op de maatschappij en de imagoschade voor het bedrijf maakten dat de prioriteit lag bij de veiligheid van publiek en medewerkers, dus bij het wegnemen van de dreiging. Het daadwerkelijk opsporen van de dader was hieraan ondergeschikt.

Het bedrijf kreeg in deze zaak als private partij een plek in de SGBO, wat vrijwel nooit voorkomt. In gezamenlijk overleg werden ook andere partijen bij de zaak betrokken. De politie werkte onder meer samen met deskundigen uit de cybercrimeteams en het Team High Tech Crime (THTC), en het bedrijf huurde op verzoek van het beleidsteam extra digitale expertise in bij een consultancybedrijf. Zo ontstond een intensieve samenwerking tussen teams van specialisten uit het afgeperste bedrijf, het consultancybedrijf, het Openbaar Ministerie, de Fiscale inlichtingen- en opsporingsdienst (FIOD) en de politie.

> » *Een plek in de SGBO voor het bedrijf komt vrijwel nooit voor*

Resultaat

Dankzij de genoemde samenwerking werden de 'spullen' vroegtijdig onderschept en nam de acute dreiging voor de samenleving af. Door de inzet van de digitale experts werd ook een spoor naar de dreiger gevonden. Deze persoon is vervolgens aangehouden op zijn zolderkamer, van waaruit hij zijn poging tot afpersing deed.

Unieke zaak

Deze afpersingszaak wordt door de twintig betrokkenen die hierover zijn geïnterviewd als uniek gedefinieerd. Allereerst is dat vanwege de combinatie van de potentiële omvang van de dreiging en de wijze waarop de afpersing werd uitgevoerd. De afperser werkte alleen via 'versluierende diensten', zoals een virtueel privénetwerk (VPN[1]), een Tor-netwerk[2] en *Darknetmarket*[3] – waar hij de 'spullen' kocht –, en eiste betaling in bitcoins.

Hieraan gerelateerd is het tweede unieke punt. Binnen een TGO gaat het veelal om moord en doodslag; met digitale afpersingszaken is tot op heden weinig ervaring opgedaan binnen de politie-eenheden. In deze TGO-zaak was de rol van digitale rechercheurs leidend, zeker in de eerste fase van het onderzoek. Vroegtijdig werden digitale experts van binnen en buiten de politie bij de zaak betrokken, waardoor 'digitaal' in kwantiteit maar ook qua inbreng groter was dan 'tactiek'. Dat maakt deze zaak bijzonder, want eigenlijk is 'tactiek' altijd leidend in een TGO.

Het derde unieke punt betreft de invulling van de publiek-private samenwerking, die in deze zaak plaatsvond op zowel strategisch als operationeel niveau. Op strategisch niveau sloot de private partij aan als deelnemer bij het SGBO en op operationeel niveau kreeg de zaak een *boost* door de samenwerking van digitale experts van diverse pluimage. De experts werkten in één ruimte samen en beschikten over dezelfde informatie. Zo wisten ze de zaak tot een goed einde te brengen. Het afgeperste bedrijf zette alles op alles en benoemde expliciet een volwaardige partner te willen zijn voor de politie. De partijen hadden respect voor elkaars belangen en hierover werd op transparante wijze gecommuniceerd.

Het vierde unieke punt is de brede aanpak van de zaak, waarin alle expertise zonder restrictie kon worden benut en waarbij echt buiten de gebaande paden is gedacht. Hoewel het voor alle partijen in het begin wel even wennen was om op deze manier samen te werken, bleek die werkwijze al snel haar vruchten af te werpen.

Ten slotte het vijfde punt: de positieve bewustwording bij met name de politie, die heeft laten zien dit soort complexe digitale zaken aan te kunnen. In de interviews werd dan ook met trots gesproken over het oplossen van deze zaak.

Dilemma's

De besproken zaak bracht tijdens de uitvoering vanzelfsprekend verschillende vraagstukken met zich mee die een dilemma vormden voor één, enkele of alle betrokken partijen. Ter illustratie wordt op een viertal dilemma's ingegaan: informatie delen, prioriteiten stellen, de snelheid en de inzet van deskundigen.

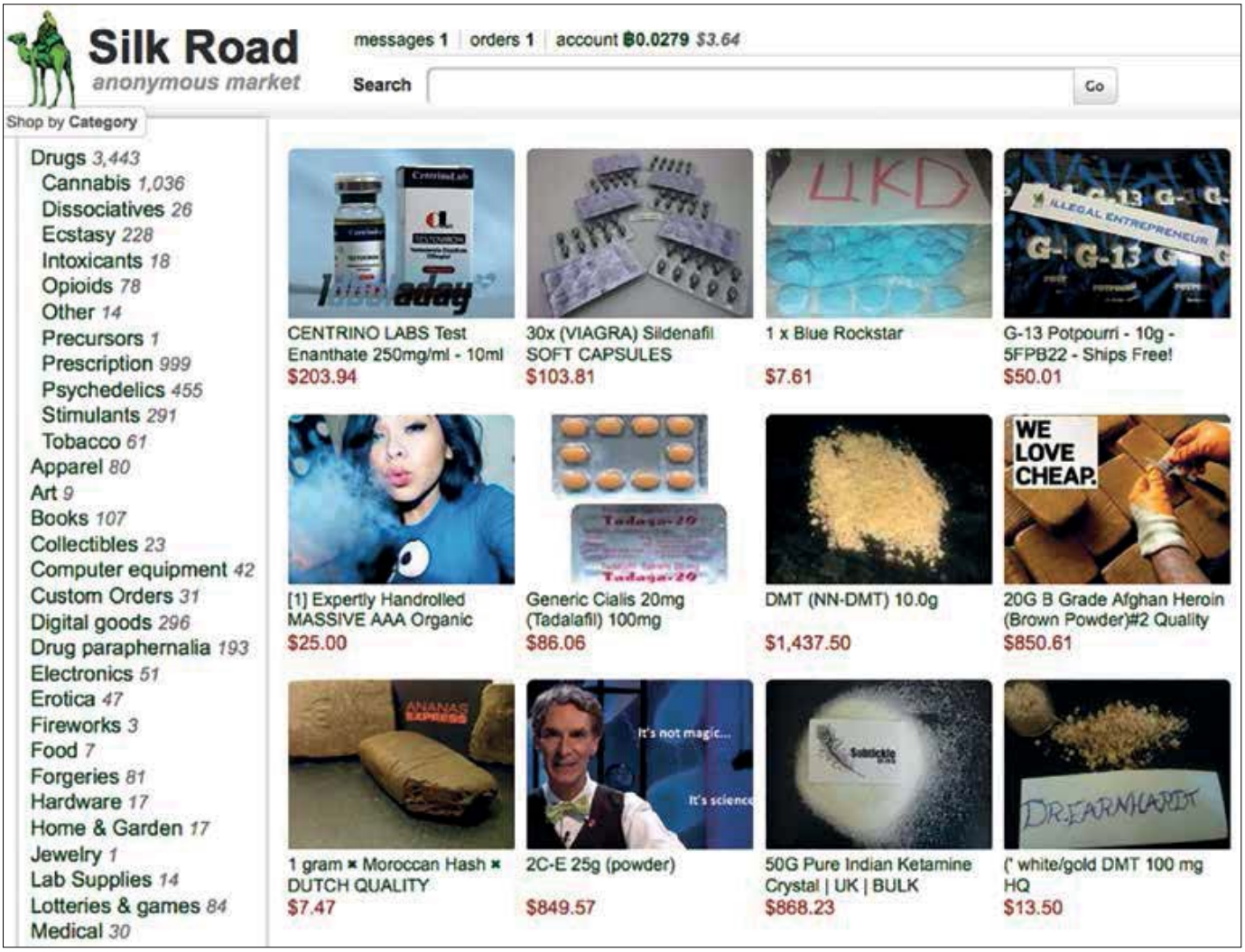
Informatie delen

Een dilemma in PPS is de vraag welke informatie kan of mag worden gedeeld. Bij aanvang van de samenwerking was dat niet meteen duidelijk, maar toen later toestemming werd gegeven alle voor de zaak relevante informatie te delen, vonden de betrokkenen dat in de beginfase nogal ongemakkelijk. Hiermee samen hangt het alert blijven op het delen van informatie die niet aan de zaak gerelateerd is. Hoe transparant kan er gewerkt en gesproken worden als de politie meerdere dagen in één ruimte werkt met een private partij?

Het dilemma rondom informatie delen speelt niet alleen tussen publieke en private partijen, maar ook intern bij de politie en het Openbaar Ministerie. Soms is de SGBO of een teamchef niet in staat alle technische informatie van de zaak, acties of consequenties te begrijpen, terwijl dit wel nodig is om tot een besluit te komen en/of de medewerkers en het onderzoek goed aan te sturen. Binnen de mogelijkheden moet steeds worden gezocht naar een goede balans.

Prioriteiten stellen

De prioriteitsvraag is een tweede dilemma. Wat heeft voor wie prioriteit? Bij het uitwerken van de scenario's werden onderliggende belangen en problemen inzichtelijk gemaakt. Het wegnemen van de dreiging en het opsporen van een



verdachte gaan niet vanzelfsprekend samen. In deze zaak is ervoor gekozen steeds open met elkaar te spreken over de verschillende belangen en elkaars insteek. Daarbij werd eens te meer duidelijk hoe politie en bedrijfsleven van elkaar verschillen.

De transparantie leverde uiteindelijk echter begrip op voor elkaars positie en belangen, wat de samenwerking tussen de politie, het Openbaar Ministerie en het bedrijf positief heeft beïnvloed. Het uitgangspunt in deze zaak was het gezamenlijke belang, namelijk de veiligheid en de volksgezondheid in Nederland en daarmee het wegnemen van de dreiging. De politie was daarnaast gefocust op het aanhouden van de afperser, wat voor het bedrijf niet noodzakelijk was.

Snelheid

Een derde dilemma betreft de snelheid van de digitale wereld versus de traagheid van de organisatie. Het tempo waarmee een commerciële partij als het betrokken bedrijf middelen aanschaft, extra capaciteit inhuurt en beslissingen neemt (met één telefoontje is het geregeld), ligt in het algemeen hoger dan bij de politieorganisatie. Het geduld van het betrokken bedrijf werd daarom soms op de proef gesteld. Toch koos men steeds voor de samenwerking met de politie, omdat er (enig) begrip bestond over de wijze waarop processen binnen de politieorganisatie verlopen. Het bedrijf benadrukt dan ook dat het voor samenwerking uitermate belangrijk is zich te verdiepen in elkaars 'werelden' en (on)mogelijkheden.

Inzet van deskundigen

Een vierde dilemma voor de politie is ten slotte een maximale inzet met beperkte capaciteit. Tot op heden zijn binnen de politieorganisatie (nog) niet alle functies op digitaal gebied ingevuld, wat betekent dat de experts bij dergelijke zaken flink worden belast. Een commerciële partij kan extra capaciteit (middelen) inhuren, maar voor de politie is dat lastiger. De vraag is dan ook: hoe lang houden de medewerkers de maximale inzet vol?

Leerpunten

In deze zaak zijn door de betrokken publieke en private partijen verschillende leerervaringen opgedaan over de wijze van samenwerking en het gebruik van ICT-*tooling* in afpersingszaken. De zaak heeft kennis en nieuwe inzichten opgeleverd over de aanpak en over mogelijke ontwikkelingen op het gebied van de digitale criminaliteit, die naar verwachting alleen maar verder zal toenemen. Twintig direct betrokkenen hebben op basis van de zaak leerpunten geformuleerd voor de politie en voor de publiek-private samenwerking. De eenheid waarin deze zaak speelde, vindt die leerpunten in het kader van een toekomstbestendige opsporing belangrijk en wil ze dan ook graag met politie en partners delen.

Les 1: Zorg dat je digitale basiskennis breed op orde is

Voor een toekomstbestendige opsporing is het noodzakelijk dat de digitale basiskennis, maar ook de bewustwording van het belang ervan binnen de politie en OM op peil zijn. Het niveau van de digitale experts bleek in deze zaak ruim voldoende. Hun aantal is echter klein en er is behoefte aan meer experts en meer mensen die beschikken over digitale basiskennis om het gat tussen de digitale experts en de tactische rechercheurs te verkleinen. Dit kan bijvoorbeeld door een digitaal coördinator aan de vaste kern van leiding-

Foto: Zach Copley

gevenden toe te voegen. Ook is dringend digitale basiskennis nodig bij gedragsdeskundigen, verhoorders en dossiervormers.

Les 2: Investeer op kennisontwikkeling
Zorg dat je binnen de eigen eenheid het netwerk van experts kent en investeer voortdurend in kennisontwikkeling op digitaal terrein. Het benutten van technologie met bijbehorende capaciteit als middelen was in de beschreven zaak essentieel. Investeer in de deskundigheid van medewerkers, maar ook in het gebruik van tooling. De beschikbaarheid van goede tooling is noodzakelijk voor de digitale opsporing.

Les 3: Werk 'echt' samen
Neem in een PPS tijd om kennis te maken met elkaars werelden. Dit bevordert het begrip voor elkaar en de samenwerking. Echt samenwerken betekent je in elkaar verdiepen en soms een interventie of actie niet, later of anders inzetten omdat deze voor de andere partner niet acceptabel is. Een mooi voorbeeld hiervan in deze casus was de inzet van een onderhandelaar: de politie wilde contact leggen met dreiger, terwijl het bedrijf per se geen zaken wilde doen met een afperser.

Les 4: Benut het interne én externe netwerk
Daar waar het gaat om digitalisering wil iedereen zijn kennis en kunde aandragen. Deskundigen van binnen en buiten de politieorganisatie zijn bereid met politie en justitie mee te werken zonder dat ze de casus tot in detail hoeven te kennen. In deze casus heeft de politie veel profijt gehad van het actief betrekken van het externe netwerk.

Les 5: Koester de digitale experts, zodat ze behouden blijven voor de organisatie
Het aantal digitale experts in de organisatie is nog altijd beperkt en het risico op overbelasting van deze deskundigen bij complexe zaken is dan ook groot.

Les 6: Denk buiten de gebaande paden
Creëer ruimte in het werken en handelen in de samenwerking tussen digitale rechercheurs en leidinggevenden. Zoek op zaakniveau naar het best passende antwoord en onderschat de snelheid en complexiteit van digitale zaken niet. Dit kan betekenen dat 'tactiek' ondergeschikt is of wordt aan 'digitaal' of dat 'digitaal' in plaats van een ondersteunende rol ineens een leidende rol krijgt. Voor een toekomstbestendige opsporing is het nodig de organisatie en de medewerkers hierop voor te bereiden.

Ten slotte

De beschreven casus toont eens te meer de kwetsbaarheid van onze samenleving. Eén individu bleek in staat politie en justitie gedurende zes weken meer dan fulltime bezig te houden. Deze zaak staat niet op zichzelf en het aantal cyberzaken zal naar verwachting toenemen. De snelheid en de complexiteit van digitale zaken moeten en mogen niet worden onderschat. De betrokken eenheid is inmiddels doordrongen van het belang van een brede bewustwording op dit vlak en hoopt dat de in deze zaak geleerde lessen en ervaringen direct kunnen bijdragen aan een toekomstbestendige opsporing. «

> » *Investeer voortdurend in digitale kennisontwikkeling*

Noten
1 Met een VPN (*virtual private network*) kan een privénetwerk van computers worden gecreëerd met de infrastructuur van een publiek netwerk. Zo kan via internet een versleutelde beveiligde verbinding gemaakt worden tussen verschillende lokale netwerken en/of computers.
2 Tor (*The Onion Router*) is een open netwerk voor anonieme communicatie. Het is bedoeld om te voorkomen dat anderen door analyse van het berichtenverkeer kunnen achterhalen wat de herkomst en de bestemming van berichten zijn.
3 Darknetmarket is een marktplaats voor illegale goederen op een anoniem en besloten deel van het internet (*darkweb*).