Blijft cybercrime een eldorado voor criminelen?

Voorlopig nog Code oranje!

In juli 2021 was ik op wandelvakantie in Polen toen ik een appje kreeg van mijn dochter dat ze financiële moeilijkheden had. Ik liep er met open ogen in. Het appje was uiteraard niet van mijn dochter, maar van oplichters. Het resultaat: een schadepost van ruim 1900 € en een deuk in het zelfbeeld. En ook nog wat anders, het maakte mij als ouder duidelijk hoe kwetsbaar je bent als het gaat om de zorg voor je kinderen.

Een slachtoffer staat nooit alleen

Internet oplichting? Dat zal mij nooit overkomen, zullen veel lezers nu denken.

Dit zal mij nooit overkomen zullen veel lezers nu denken. Dat valt nog maar te bezien. Cybercrime, want daar valt deze vorm van criminaliteit onder, is big business. In mijn geval ging het om cybercrime in brede zin, eigenlijk traditionele misdaad, maar dan met behulp van de digitale middelen waar wij allen dagelijks zo ruimschoots gebruik van maken. Deze vorm van cybercrime wordt ook wel aangeduid als gedigitaliseerde criminaliteit. Er is een vorm van cybercrime die wel nieuw is, waarbij de computer doel en middel van de modus operandi (MO) zijn. Bijvoorbeeld het installeren van gijzelingssoftware ('ransomware').

De cybercrime waar ik slachtoffer van werd, is een van de favoriete verdienmodellen bij gedigitaliseerde criminaliteit . De politie noemt het 'vriend-in-nood' fraude. Marianne Junger, onderzoeker van de universiteit Twente schat de totale schade van gedigitaliseerde criminaliteit op 2,75 miljard euro per jaar. In het interview dat de hoogste baas van het OM, van der Burg, jongstleden gaf, hield hij het op een iets bescheidener bedrag, 2,5 miljard euro. Maar wel met groeipotentie en misschien nog wel winstgevender dan drugscriminaliteit, zei hij. Hij zag de toekomst niet zonder zorgen in. Een brede aanpak is gewenst om dat te voorkomen.

Er zijn ook andere onthullende cijfers. Volgens de 'Veiligheidsmonitor 2021' van het CBS zijn 2,5 miljoen mensen boven de 15 slachtoffer geworden van online criminaliteit. Hier werd het breder geformuleerd. Ook bedreiging, intimidatie en sexting vielen hier onder. Het grootste aandeel betrof overigens wel oplichting en fraude. Maar één op de vijf slachtoffers deed aangifte. Daarnaast zijn er nog veel meer mensen in aanraking geweest met online criminaliteit. Uit cijfers blijkt dat – als je alleen al naar phishing kijkt – 68% van alle Nederlanders boven de 15 hiermee in aanraking is gekomen.

Als het gaat om gedigitaliseerde criminaliteit met financiële gevolgen dan stelt hetzelfde prevalentie onderzoek van de universiteit Twente dat naar alle waarschijnlijkheid 41,7 % van de Nederlanders boven 15 jaar in 2020 benaderd is met een poging tot fraude, 15,7 % (grofweg 2,3 miljoen mensen) is daar ook daadwerkelijk op ingegaan. Met naast financiële, ook mogelijk emotionele schade tot gevolg. Bijvoorbeeld bij dating fraude waarbij het slachtoffer meent met een mogelijke partner te communiceren, die hem of haar op een gegeven moment ook financiële steun vraagt. Het overgrote deel van fraude had een digitale component.

Lucratieve verdienmodellen

De bedragen die gemoeid zijn met deze digitale fraude variëren. Volgens cijfer van de Fraudehelpdesk was de gemiddelde schade in 2022 bij dating fraude € 21.478 Bij aan en verkoop fraude lag dat verhoudingsgewijs veel lager: € 244 . Beleggingsfraude scoorde gemiddeld het hoogst: € 21.687.

Bij gedigitaliseerde criminaliteit geldt de macht van het getal. Je zorgt dat je aan een dataset van contactgegevens komt (die zijn nl. te koop) en dan ga je aan de slag. Of zoals, Bobby Markus, de landelijke woordvoerder van de politie het formuleert:

'Cybercriminelen maken vanuit één handeling op afstand veel slachtoffers en dat levert hun veel op. De financiële en emotionele gevolgen voor burgers en bedrijven zijn groot. Dit kan dus iedereen raken.'

Het is dus betrekkelijk eenvoudig. En ook al reageert maar 10 procent, dan is dat nog voldoende om een behoorlijke som binnen te halen. Bij de fraude waarvan ik slachtoffer werd, is in 2022 per slachtoffer gemiddeld € 3.496 'opgehaald'. Voor de 'vriend-in-nood 'fraude is wel de piek in meldingen tijdens de corona periode opvallend : 12.133 in 2021 tegen 3490 in 2022.

De Fraudehelpdesk is een private organisatie die zich richt op het adviseren over en helpen van slachtoffers bij fraude. Ook richt het zich op het voorkomen ervan bijvoorbeeld door waarschuwingen uit te brengen. De organisatie heeft, naar zeggen van de woordvoerder Tanya Wijngaarde *'een bescheiden budget'* voor preventieve voorlichtende acties. Inmiddels heeft de organisatie geleerd dat brede algemene publieksvoorlichting niet de beste manier is. Voorlichting en preventie moeten afgestemd zijn op specifieke doelgroepen. *'De boodschap: kijk uit voor je oversteekt'*, is te algemeen, volgens de woordvoerder. Het moet een specifieke boodschap zijn die het beoogde slachtoffer ook kan toepassen om erger te voorkomen. Ook verschillen de doelgroepen,, soms zijn het met name senioren doelwit, dan moet je daar dus je actie op richten. De fraudehelpdesk raadt slachtoffers aan om altijd aangifte te doen.

Bobby Markus, landelijk woordvoerder politie: *'Cybercriminelen maken vanuit één handeling op afstand veel slachtoffers en dat levert hun veel op. De financiële en emotionele gevolgen voor burgers en bedrijven zijn groot. Dit kan dus iedereen raken.'*

Aangifte doen en dan?

Eén van de grote problemen is dat veel slachtoffers dat niet doen. Bij het onderzoek over 2020 van de Universiteit Twente was dat naar schatting maar 1 op vijf, zoals al eerder vermeld. De bereidheid om aangifte bij de politie te doen, is wel groter als er financiële schade is geleden. De wijze van aangifte doen werd als positief ervaren, minder tevreden was men over het vervolg. Slachtoffers doen niet alleen aangifte om mogelijk hun geld terug te krijgen. Zij hopen dat het herhaling bij andere slachtoffers voorkomt en dat er meer bekendheid komt voor deze vorm van criminaliteit.

Als het om opsporing en vervolging gaat dan zijn de politie en het Openbaar Ministerie (OM) aan zet. Gedigitaliseerde criminaliteit c.q. fraude valt onder de categorie horizontale fraude. De politie publiceert cijfers over alle vormen van criminaliteit . Tijdens de corona jaren was er een piek te zien in aangiftes m.b.t. horizontale fraude: 120.502, in 2022 was dat weer gedaald tot 83.709. Het probleem met deze categorisering is dat eigenlijk niet zichtbaar is welk deel van deze aangiftes betrekking heeft op gedigitaliseerde criminaliteit. Zo valt bijvoorbeeld fraude met kilometertellers er ook onder. Bobby Markus, woordvoerder van de politie kan die specifieke cijfers ook niet verstrekken, omdat het niet op dat detailniveau vastgelegd wordt.

CBS heeft recent wel een pilot gestart om met een algoritme aangiftes achteraf te analyseren of het mogelijkerwijs om cybercrime gaat. Van het totaal aantal PV's (processen-verbaal) , 820.000 uit 2016, bleek bijna 9 procent cybercrime te betreffen. Voor de categorie oplichting en bedrog gold, dat bijna alle PV's cybercrime betroffen. Inmiddels zijn we 7 jaar verder. Het lijkt niet waarschijnlijk dat deze verhouding is verminderd, eerder gestegen.

Bij horizontale fraude vindt iets meer dan de helft van de aangiftes via internet plaats. Dat is natuurlijk makkelijk voor de politie en de slachtoffers. Bij (internet)aangiftes m.b.t. internetoplichting (inclusief Whatsapp fraude) wordt maar een gedeelte als opsporing opgepakt, afhankelijk van de specifieke omstandigheden. Bijvoorbeeld in het kader van clustering (groepen aangiftes die naar specifieke verdachte(n) te herleiden zijn). Alle aangiftes zijn wel een belangrijke bron van informatie voor de politie.

Daarnaast heeft de politie het over een ophelderingspercentage. Ook dat is weer even studeren om te weten wat dit betekent. Er is sprake van opheldering als een aangifte – al dan niet via internet - aan een verdachte gekoppeld wordt en na verhoor van die verdachte er wordt besloten dat hij of zij verdachte blijft. Over 2021 was dat

percentage voor horizontale fraude 6 % en in 2022 7%. Daarbij moet wel vermeld worden dat dit ook betrekking kan hebben op aangiftes uit eerdere periodes.

Van de minder dan 10 % zal ook nog een aantal afvallen als het gaat om kans op verdere opsporing met resultaat. Als dat resultaat er wel is, dan kan de zaak aangebracht worden bij het Openbaar Ministerie (OM). De politiewoordvoerder heeft geen cijfers over het aantal zaken aangedragen bij het OM op het gebied van gedigitaliseerde criminaliteit

Daar kan de officier van justitie nog wel besluiten dat de zaak geseponeerd wordt. De pakkans is dus bijzonder klein. Slachtoffers zullen dit ervaren als dat er geen genoegdoening is gedaan, 'de dader komt er mee weg', ook al blijken ze begrip te hebben voor de keuzes van de politie.

Het meest interessante zijn natuurlijk de daders. Je hebt de organisatoren en het voetvolk. Zo zijn er de al eerder genoemde 'geldezels'. Mensen die hun bankrekening ter beschikking stellen voor het geld dat het slachtoffer overmaakt. Het kan ook zijn dat iemand geld pint met een door fraude verkregen pinpas, hij krijgt daarvoor een geringe beloning, de rest gaat naar de organisatoren. De landelijk woordvoerder van de politie omschrijft de geldezels als *'vaak sociaal zwakkeren'*. Van de rekening van de geldezel, wordt het daarna zo snel mogelijk doorgesluisd naar een andere rekening en dan pas begint de organisator in beeld te komen. De organisator kan zich natuurlijk heel goed buiten Nederland bevinden. Geldezel zijn is in principe ook strafbaar en ook om andere redenen niet zonder risico.

Het meest interessante zijn natuurlijk de daders. Je hebt de organisatoren en het voetvolk. Zo zijn er de zogenaamde 'geldezels'. De politie omschrijft deze geldezels als 'vaak sociaal zwakkeren'.

Slachtoffer kan soms geld terughalen

Sinds 2021 is het mogelijk om via civiel recht de schade te verhalen op deze geldezels. Dat is alleen nog niet zo simpel. Eerst moet het slachtoffer via zijn bank de NAW gegevens van de geldezel opvragen. Daarna moet hij persoonlijk deze persoon benaderen. En als dat allemaal niet werkt dan is er nog een andere weg nl. via het civiel recht en de gerechtsdeurwaarder. Er zijn twee organisaties in Nederland die dit op een 'no cure, no pay' basis doen, LAVG en Soda. Volgens de woordvoerder van de LAVG zijn er tot nu toe ruim 1000 van dit soort procedures in behandeling genomen. In ongeveer 50 % van de gevallen heeft dat ook succes. Maar vaak dus ook niet. Benadeelden haken ook wel af als zij zien wie de dader is en wat het voor de geldezel en/of zijn familie betekent om de schade terug te betalen. Het kan zijn dat er een betalingsregeling getroffen moet worden. Dan komt de geleden schade in termijnen terug

Brede aanpak noodzakelijk

De laatste jaren is er een aantal informatie trajecten opgestart. Zo is er het onderzoek van de universiteit Twente, waar ook de politie aan heeft meegewerkt. En het ministerie van Justitie en Veiligheid heeft onderzoek gedaan naar wat slachtoffers beweegt. In de brief die de minister op 4 november 2022 naar de tweede kamer stuurde, is sprake van twee sporen: *preventie & slachtofferzorg* naast *opsporen, vervolgen, verstoren*. Er wordt ook extra geld ter beschikking gesteld, 12 miljoen structureel voor het OM in 2024. Naar zeggen van het OM is dit nodig om *'het been bij te trekken ten opzichte van ketenpartners (waaronder politie en rechtspraak)'.*

Het verstoren doe je als het niet meteen lukt om de daders te vervolgen en te straffen. Het verstoren moet er toe leiden dat criminele winsten minder makkelijk gerealiseerd kunnen. Het is een vorm van preventie. Uiteraard kan altijd alsnog tot vervolging overgegaan worden. Ook hier komen de 'geldezels' weer in beeld als hefboom. Officier van justitie Jan Hoekman over het aanpakken van geldezels: *'Het vergroot ook meteen de kans om uit te komen bij de ronselaars van geldezels, vaak de hoofddaders achter deze delicten.'*

Opsporen en vervolgen

Uiteindelijk ligt de taak van opsporen dus bij de politie onder gezag van het OM. De politie erkent de urgentie van het terug dringen van cybercrime. OM en politie werken samen aan een aanpak gedigitaliseerde criminaliteit. Ik spreek Yoanne Spoormans van de eenheid Oost-Nederland die zeer bevlogen kan vertellen over deze aanpak Over

één ding is zij duidelijk. Als je denkt dat de politie het probleem van cybercrime alleen kan oplossen dan zit je mis. Zij citeert Loesje*: 'Dweilen met de kraan open werkt beter, als iemand anders ondertussen de kraan dicht draait.'*

De aanpak van de politie is wel veel gerichter geworden en zij ziet daar ook de effecten van. Meer aandacht voor slachtoffers, verstoren van het criminele proces en op jacht naar de achterliggende netwerken. Dat heeft al een paar mooie resultaten opgeleverd. Deze vorm van criminaliteit vraagt ook om een landelijke aanpak. Terwijl de politie veelal toch in eerste instantie lokaal opereert.

Yoanne Spoormans, politie Oost-Nederland over aanpak cybercrime: *'Dweilen met de kraan open werkt beter, als iemand anders ondertussen de kraan dicht draait.'*

De politie kiest er ook bewust voor niet tot opsporing over te gaan bij de tussenpersonen zoals geldezels. Ook weer volgens Spoormans van regio Oost-Nederland:

'Dit zijn namelijk vaak geen criminelen, maar gewone burgers, die op dezelfde manier worden ingepalmd als de slachtoffers die hun geld kwijt zijn.'

Bovendien signaleert zij een *'vreselijk krappe capaciteit van rechters'*, dus ook daar moeten keuzes gemaakt worden. Er zijn ook andere typen interventies mogelijk zoals 'stopgesprekken'. Een 'goed gesprek' met een verdachte, bedoeld om hem voor verder afglijden te behoeden.

Deze keuze is begrijpelijk en praktisch zeer goed verdedigbaar, maar conflicteert wel enigszins met de *Aanwijzing voor opsporing,* die stelt dat als de (mede)dader bekend is ,opsporing plaats moet vinden om het rechtvaardigheidsgevoel te respecteren.

Yoanne Spoormans ziet ook verbanden met andere vormen van criminaliteit. 'Met de cash flow van digitale oplichting, kan je weer een drugstransport financieren'. Ook is er wel degelijk sprake van geweld in kringen van gedigitaliseerde criminaliteit. Zij is ook duidelijk in wat anders en beter zou moeten en dat is niet alleen meer mankracht voor dit onderwerp, stelt zij nog eens nadrukkelijk. Die reflex moet je enigszins onderdrukken. Wat zeker wel moet: betere informatie uitwisseling met alle partijen die de gevolgen van cybercrime ondervinden. Ook: meer aandacht vanuit de politiek. Zo is het haar een doorn in het oog dat in Nederland nog steeds anonieme sim kaarten verkocht worden. Dit probleem is al eerder aangekaart in het kader van terrorisme bestrijding, toen werd het risico als te laag ingeschat om hier stappen te zetten. Bovendien was de gedachte dan men in het buitenland anonieme sim kaarten zou gaan kopen. Overigens is in België deze verkoop inmiddels geblokkeerd. Momenteel agendeert de politie het weer, maar dan gelet op andere criminele activiteiten zoals cybercrime

Het is ook een belemmering als je geen goede data hebt over de omvang van criminaliteit, daar wordt ook regelmatig om gevraagd vanuit de maatschappij en de politiek. De politie is bezig hier verbeteringen aan te brengen.

En ten slotte bepleit zij internationaal samen werken en ook internationaal agenderen. Van klachten naar bijv. Meta en Google alleen uit Nederland over het gevaar dat kleeft aan digitale anonimiteit, zijn deze techgiganten niet onder de indruk. Je moet het samen doen , bijv. als EU via Europol.

De volgende stap is vervolging door het OM. Het OM geeft in de *Aanwijzing voor de opsporing* aan welke zaken zij voor opsporing in aanmerking vindt komen en dus ook aangeleverd wil krijgen. Het OM beslist vervolgens of er tot vervolging overgegaan wordt. Die bevoegdheid ligt uitdrukkelijk niet bij de politie. Er zijn verschillende categorieën qua prioriteit. Veel internet fraudezaken vallen in de categorie 'veel voorkomende criminaliteit' (VVC). Al dan niet vervolging wordt afgewogen tegen een aantal andere factoren.

Een misdrijf waarbij sprake is van lichamelijk letsel of een zeden misdrijf wordt altijd in behandeling genomen voor opsporing en bij voldoende bewijs vindt vervolging plaats. En ook als de mogelijke dader makkelijk is te achterhalen bij andere vormen van criminaliteit inclusief VVC, vindt vervolging plaats bij voldoende bewijs, omdat anders het rechtvaardigheidsgevoel van de burger in het geding is. Hier kan van afgeweken worden als het om een excessief aantal zaken gaat. Tenzij deze vorm van criminaliteit juist prioriteit krijgt, bijvoorbeeld omdat het deel uitmaakt van een groter ondermijnend geheel. Het OM maakt hierover dan afspraken met de politie. Cijfers over gedigitaliseerde criminaliteit zijn niet leverbaar door het OM volgens woordvoerder Desirée Wilhelm omdat:

'De gezamenlijke landelijke aanpak van gedigitaliseerde criminaliteit is pas in ontwikkeling. Het OM vindt het daarom te vroeg om cijfers te delen. Ook omdat de wijze waarop in het heden en toekomst gedigitaliseerde criminaliteit wordt geregistreerd afwijkt van het (recente) verleden. Dit komt omdat het onderwerp sinds dit jaar prioriteit heeft in de Veiligheidsagenda.'

Een getalsmatige definiëring ontbreekt op dit moment dus, terwijl het probleem al langer speelt.

Een internationaal probleem

Nederland staat zeker niet alleen als het om gedigitaliseerde criminaliteit gaat. Jorij Abraham, van de Global Anti Scam Alliance, publiceert jaarlijks een rapport. Hij noemt oplichting ook wel het op één na oudste beroep ter wereld. Als het om de bestrijding gaat dan doet Nederland het nog niet zo slecht. Relatief dan. Wereldwijd is de pakkans 0,05 %. Nederland heeft wel de grootse schade per hoofd van de bevolking, waarbij hij wel de cynische kanttekening plaatst: Nederland is één van de landen waar de geleden schade nog het beste bijgehouden wordt. België staat onderaan, maar daar zijn ook 24 gewesten die allemaal zelfstandig opereren.

Ook hij heeft een verlanglijstje. Punt één, zorg dat je over betrouwbare data beschikt, daar is nog een weg te gaan. Ten tweede: maak internationaal samenwerken en vervolgen mogelijk. Nu kan een dader nog vrij moeiteloos van het ene land opereren in een ander land. Het valt hem wel op dat sommige landen in de EU meer in verband worden gebracht met cybercrime dan andere landen. En ten slotte: het gemak waarmee criminelen anonieme kunnen opereren in de digitale wereld is vragen om problemen . Hij vraagt zich af of de ultieme bescherming van privacy niet te veel doorgeslagen is.

Deze mening deelt hij met Marianne Junger. Zij heeft zich tijdens haar carrière uitgebreid met onlinecriminaliteit en informatiebeveiliging bezig gehouden. Er zijn zeker bemoedigende initiatieven gaande, zoals de rol van banken bij preventie maar zij denkt toch dat er meer nodig is. Een breder plan waaraan alle betrokken partijen gezamenlijk opereren. En zij ziet dezelfde verbeterpunten: meer en betere data. En de extreme aandacht voor privacy maakt het criminelen wel erg makkelijk.

Zowel Yoanne Spoormans als Jorij Abraham en Marianne Junger, zeggen dat gedigitaliseerde criminaliteit te lang als een 'onschuldige' vorm van criminaliteit is gezien.

Wat wordt de toekomst?

Er is sprake van een groeiend bewustzijn en nieuwe initiatieven, maar de grote vraag blijft dan toch, gaat het helpen? Zullen we die 2,5 miljard langzaam zien verminderen? De fraudehelpdesk signaleert voor bepaalde type fraudes een daling ten opzichte van de corona jaren. Tegelijkertijd is het niveau nog altijd substantieel hoger dan in de jaren voor corona. Een minder geruststellend signaal is wat de Nederlandse Vereniging van Banken, afgeeft, die ziet een stijging voor de 'bankhelpdeskfraude': over het eerste halfjaar van 2022 zou de schade al 30,3 miljoen euro bedragen, ter vergelijking over het hele jaar 2021 was dat 47,6 miljoen euro.

Het digitale domein, is niet alleen maar een nieuwe vorm van gezellig winkelen in de Kalverstraat. Het is ook wandelen op een mooi bergpad met een prachtig uitzicht, maar waar je diep kunt vallen als je niet uitkijkt.

Hoe dan ook, zonder meer zicht op aantallen aangiftes en vervolgingen, èn geleden schades, is het ook lastig om een objectief oordeel uit te spreken. Als je het ophelderingspercentage van horizontale fraude met dat van de categorie Overige fraude vergelijkt, dan is dat nu in ieder geval opvallend laag, 7 % bij horizontale fraude tegenover 62 % bij overige fraude in 2022. Overigens gaat hier wel om veel lagere getallen. Aandacht maakt alles dus effectiever, maar kost ook tijd. Tijd die er lang niet altijd is.

Slachtoffers ondervinden ten onrechte schaamte

Bij digitale criminaliteit kan er sprake zijn van schaamte bij het slachtoffer zodra deze merkt dat hij misleid of bedrogen is. Alle partijen zeggen dat het een fout is om het slachtoffer zelf verantwoordelijk te stellen Criminelen kunnen psychologisch zeer geraffineerd op hun slachtoffer inwerken.

Een ding is wel duidelijk: het je bewegen in het digitale domein, is niet alleen maar een nieuwe vorm van gezellig winkelen in de Kalverstraat. Het is ook wandelen op een mooi bergpad met een prachtig uitzicht, maar waar je diep kunt vallen als je niet uitkijkt.

René Lesuis

Leesverderr – Journalistiek

https://leesverderr.nl