Quickscan Microsoftfraude

Opsteller: 10.2.e

Datum: 20 juni 2017

Betrokkenen: Eenheid Midden-Nederland (10.2.e), Fraudehelpdesk (mail dd. 18 juni 2017),

Bronnen: aangiften (BICC), CBA Horizontale fraude (NDB2012 en 2017), Tros Opgelicht (website)

Disclaimer: deze analyse diende binnen korte tijd opgeleverd te worden. Dit heeft tot gevolg dat sommige conclusies onder voorbehoud zijn genomen: dit geldt vooral voor uitspraken die gebaseerd zijn op analyse van de aangiften. Voor een gefundeerdere onderbouwing is meer onderzoek nodig.

Hoofdstuk 1. Inhoudelijke analyse fenomeen

1. Wat is de definitie?

Microsoftfraude is een goed voorbeeld van de overlap tussen fraude, cybercrime en *social engineering*:

Het slachtoffer wordt gebeld door een Engels sprekend persoon (met Indiaas accent) die zich voordoet als medewerker van Microsoft. Bijvoorbeeld een 'security-expert' of 'technician'. In het gesprek doet de crimineel het slachtoffer geloven dat er problemen op de computer zijn ontdekt met de software van Microsoft. De computer is altijd traag of geïnfecteerd met virussen en de medewerker zal aandringen op snelle maatregelen om het bestaande probleem te verhelpen om grote(re) problemen te voorkomen. Daarvoor zijner wel wat aanpassingen op de computer noodzakelijk en de medewerker krijgt toegang tot de computer. De dader/beller is bereid om tegen betaling de zogenaamde problemen te verhelpen.

Er is sprake van fraude omdat er een opzettelijke handeling in hat spel is waarbij een fraudeur gebruik maakt van valse voorwendselen met het oogmerk om zich op basis van deze bedrieglijke gegevens ten koste van anderen te bevoordelen dan wel te verrijken (CBA Horizontale fraude, NDB2012).

In het CBA Horizontale fraude voor het Nationaal Dreigingsbeeld 2017 is MF opgenomen als fraude met internetbankieren. Bij deze vorm van fraude doen fraudeurs transacties uit naam van een ander, dat zijn transacties die niet door de rekening- of pashouder zijn geïnitieerd. Dit gebeurt door het overnemen van de oorspronkelijk aan de kaarthouder uitgegeven (betaal)kaart, door het stelen van de kaartgegevens of door overname van de identiteit van een ander.

Fraude met internetbankieren gaat meestal over phishingactiviteiten[1] en dat valt onder computervredebreuk. Er is dan sprake van het hacken van de rekeningnummers van slachtoffers nadat deze een link heeft aangeklikt die zogenaamd afkomstig was van de bank. In werkelijkheid kreeg de dader toegang tot de bankgegevens van het slachtoffer. Bij MF krijgt de dader toestemming om software te installeren en kan daarmee meekijken op de computer van het slachtoffer. Daardoor krijgt hij toegang tot het internetbankieren en daarmee het bankrekening nummer van het slachtoffer en kan dan bedragen overschrijven naar eigen rekening.

Social engineering is als trend benoemd in het CBA Horizontale fraude (NDB2017). Het gaat om trucs die daders hanteren om slachtoffers te bewegen om gevoelige informatie te verstrekken (zoals bij MF het bellen van de slachtoffers). Vaak gaat het om een persoonlijke benadering via mail of telefoon.

2. Wat is de modus operandi ? Ontwikkeling van de m.o.

De modus operandi verloopt in verschillende stappen die in uitvoering enigszins kunnen variëren:

1. In de meeste gevallen krijgt het slachtoffer eerst een (soms gebrekkig) Engels sprekend persoon aan de telefoon. Hij stelt het beoogde slachtoffer een aantal vragen over de software op de computer en laat het slachtoffer zien dat er veel foutmeldingen zijn.

2. Na deze eerste scan wordt het slachtoffer doorverbonden of het gesprek overdragen aan een collega met de mededeling dat die de persoon verder zal bijstaan met technische oplossing van het probleem. De dader vraagt het slachtoffer de computer op te starten. De dader krijgt toestemming om Teamviewer te installeren (software om op het scherm mee te kijken), zodat ze samen het probleem kunnen oplossen. Hiermee kunnen de daders meekijken wat er gebeurt en de controle van de computer overnemen.

3. Het slachtoffer wordt tijdens het gesprek ook gevraagd om eventuele virusscanners tijdens het gehele proces uit te zetten.

4. Meestal krijgen de slachtoffers gedurende het gesprek bestanden te zien die op hun computer staan, waaruit zou blijken dat de computer problemen heeft (geïnfecteerd is) en er dus direct gehandeld moet worden.

5. Vervolgens vraagt de dader aan het slachtoffer om naar de website van de bank te gaan, in te loggen, en hij vraagt via sms naar een 10.2.g om een klein bedrag over te maken. Dit gebeurt vaak buiten het zicht van het slachtoffer bijvoorbeeld door de snelheid waarmee schermen elkaar opvolgen (en het slachtoffer het niet meer kan volgen) of omdat het beeldscherm even wegvalt.

[1] Phishing is een verzamelnaam van technieken die criminelen gebruiken om vertrouwelijke gegevens, bijvoorbeeld inlogcodes, te bemachtigen om daarmee vervolgens te frauderen. Meestal gebeurt dat via ongevraagde e-mails (spam). Ongeveer 90 procent van het e-mailverkeer in de wereld bestaat uit spam (NVB, 2011).

6. Tot slot komt het moment van afrekenen. Voor de technische 'hulp' of bijvoorbeeld het verlengen van de Microsoft-licentie dient te worden betaald. Soms wordt het slachtoffer verzocht om enkele euro's over te boeken maar regelmatig worden hier al hogere bedragen gevorderd. De hoogte van het bedrag is afhankelijk van wat aan het slachtoffer is 'verkocht'. De oplichter vraagt het slachtoffer om in te loggen op internetbankieren of vraagt om geld over te boeken via iDeal, MoneyGram of Western Union. In al deze gevallen krijgen de slachtoffers ook hier 'hulp' van degenen die hen belt. Vaak verhoogt de oplichter het afgesproken bedrag ongemerkt tijdens het betaalproces. Er zijn gevallen bekend waarbij het slachtoffer ziet dat het bedrag verhoogd wordt maar niet meer kan ingrijpen. Wanneer daar een opmerking over wordt gemaakt volgen niet zelden bedreigingen. Daarna verbreekt de oplichter de verbinding.

7. Slachtoffers krijgen instructies die ze moeten volgen na de oplichting. Soms wordt slachtoffers gevraagd online te blijven, of nog een dag in de buurt van de computer, of 24 uur niet te internetbankieren of alle verbindingen af te sluiten.

Er zijn verschillende manieren van betalen geconstateerd:

1. Geld wordt via iDeal overgeschreven naar een ander slachtoffer (Nederlandse tegenrekening, waarschijnlijk worden deze slachtoffers als katvangers ingezet maar hiernaar zou onderzoek moeten plaatsvinden). En dit tweede slachtoffer maakt het geld over via Western-Union of Moneygram. Het geld gaat overal naar toe: Togo, Marokko, Turkije etc. Daar wordt het eraf gehaald en is dan niet meer te volgen (vroeger kon dat wel, omdat het doorgestort werd).

2. Naast directe betalingen wordt ook geld van de spaarrekening naar de betaalrekening van het slachtoffer overgemaakt (waardoor de schade flink kan oplopen).

3. Geld moet worden overgemaakt naar Western Union – Money gram.

4. Kopen van ITunes kaarten: de nummers worden doorgegeven aan de daders, die deze kunnen verzilveren in de Apple Store. ITunes kaarten zijn waardevol omdat ze niet te traceren zijn. Kaarten kunnen worden doorverkocht en een kaart van bv 500 euro kan worden doorverkocht voor 300 euro. Mogelijk worden ze gebruikt om *credits* te kopen bij games en is er sprake van witwassen. Omdat slachtoffers grote hoeveelheden moeten aanschaffen is met diverse **aanbieders** contact gezocht (Jumbo, Primera, HEMA) en zij verstrekken niet langer zonder meer veel kaarten). Kaarten zijn ook rechtstreeks bij Apple/ iTunes besteld en dat is voor het verzilveren een Apple ID nodig. Dit zijn echter fake-adressen.

5. Recent: Bitcoins (zie voorbeeld hierna: *punt 4, slachtoffergroep*)

6. Computer wordt gegijzeld (ransomware) en kan alleen tegen betaling worden ontgrendeld. Komt minder vaak voor.

Ontwikkeling modus operandi.

In het CBA Horizontale Fraude (NDB2012) was phishing de belangrijkste fraudevorm binnen de categorie fraude met betaalmiddelen. Microsoftfraude is een variant hierop, alleen is de wijze

waarop contact wordt gezocht indringender, het leunt zwaar op *social engineering*, waardoor het slachtoffer gemakkelijk meewerkt. De werkwijze verschilt niet van de hiervoor beschreven modus operandi; het openen van een link naar een frauduleuze website is vervangen door installatie van TeamViewer, waarmee de dader toegang krijgt tot alle codes en overschrijvingen kan uitvoeren.

De schade als gevolg van fraude met internetbankieren is door allerlei maatregelen die banken hebben genomen drastisch afgenomen. De Betaalvereniging Nederland en de Nederlandse Vereniging van Banken (NVB) verzamelen en analyseren fraudecijfers. Sinds 2012 is de totale schade gezakt van 82 miljoen euro in 2012 en 33 miljoen euro in 2013 naar ruim 17 miljoen euro in 2014 en 2015.

Sinds 2011 is Microsoft fraude een opkomend probleem, maar niet als zodanig aangemerkt in het CBA Horizontale Fraude en de oorzaak daarvan ligt in de registratie: Microsoftfraude wordt vooral gezien als cybercrime en als zodanig weggeschreven (ook binnen de resultaatafspraken met het OM). Uit de analyse van aangiften in dit onderzoek kwam een beperkt aantal aangiften naar voren waarin MF de hoofdmoot vormde en deze waren wel als fraude geregistreerd. Een uitgebreidere analyse zou licht moeten werpen op de werkelijke omvang van het probleem. In een toekomstig NDB zou onderzocht kunnen worden of genomen maatregelen (hierna een voorstel) hebben geholpen.

3. Hoe ziet de dadergroep er uit?

Daders verblijven in India (uitzending Tros Opgelicht), maar het is niet duidelijk of dat voor alle daders geldt. Ze werken vanuit callcenters en in de uitzending bleek deze in Calcutta, India, te zijn gevestigd. Het ging om het callcenter Kreador Infotech, een van de locaties waaruit de Microsoftfraude gepleegd werd. Tros Opgelicht legde contact met een dader en deze gaf de oplichting toe. Daar is het bij gebleven (de Indiase politie was er niet bij betrokken). In de beperkte analyse van de aangiften die is gedaan, is ook sporadisch deelname aan deze fraude door Nigerianen aangetroffen. Daders verblijven vooral in landen waarmee (nog) geen samenwerkingsverbanden bestaan, wat opsporing en uitwisseling bemoeilijkt.

4. Hoe ziet de slachtoffergroep er uit?

Wie worden het slachtoffer van deze vorm van fraude. Probeer hier een profiel te schetsen van – eventueel verschillende- slachtoffergroepen. Zijn dit bijvoorbeeld overwegend burgers of bedrijven? Zijn er specifieke kenmerken van de slachtoffergroep(en). Denk hierbij bijvoorbeeld aan geslacht, kwetsbaarheid, opleiding etc.. Geef ook aan wat de impact is op het slachtoffer (financieel, emotioneel etc.).

Vooral individuele burgers zijn in toenemende mate slachtoffer. Experts melden dat het vooral om 50-plussers gaat, en dit blijkt ook uit een snelle analyse van de aangiften. Meestal gaat het om 50-plussers, mannen en vrouwen, en sporadisch om jongere mensen.

Na 2012 is de schade als gevolg van internetbankieren sterk afgenomen door maatregelen die de banken hebben genomen (vooral skimmen ging terug naar nagenoeg nul). Maar nu neemt het weer toe en met deze vorm van oplichting is het vaak raak: veel slachtoffer die aangifte of melding doen zijn waarschijnlijk ook daadwerkelijk benadeeld. Maar dit zal nader onderzocht moeten worden (bij andere vormen van fraude melden mensen vaak maar blijken dan niet betaald te hebben, dit dankzij intensieve voorlichtings – en waarschuwingscampagnes, zoals bij acquisitiefraude waar het MKB zich behoorlijk bewust is van de gevaren). Soms blijft het bij een poging en wanneer slachtoffers zich heel snel bij de bank melden, kunnen de betalingen direct geblokkeerd worden en ontvangen zij deze retour. Op dit moment bestaat geen zicht op het aantal waarbij dit plaatsvindt.

De schadebedragen variëren tussen 500 en 10.000 euro met uitschieters naar boven en naar beneden (afhankelijk van wat er op de rekening van slachtoffers staat). Op 13 juni 2017 meldde zich een slachtoffer bij de eenheid Midden-Nederland, waarvan de rekening helemaal is leeggehaald. Het ging om totaal 76.000 euro en dit is een trieste uitschieter, maar de reden om er in te trappen, zoals omschreven in de aangifte, is waarschijnlijk exemplarisch voor alle slachtoffers:

Samengevat was het scenario was zoals hiervoor beschreven. Het slachtoffer in kwestie, leeftijd 58 jaar, was gebeld door een Engels sprekende persoon met Indiaas accent die hem vertelde dat er problemen waren. Het slachtoffer gaf in de aangifte aan:

'Ik heb zelf niet heel veel verstand van computers, ik kon niet inschatten of het noodzakelijk was om het meteen op te lossen. Ik heb vervolgens gedaan wat mij werd gevraagd '.

En zoals hij daaraan toevoegde: **wat de oplichter vroeg klonk logisch (toestemming geven om mee te kijken, mobiele nummer geven) en hij zag geen rare dingen.**

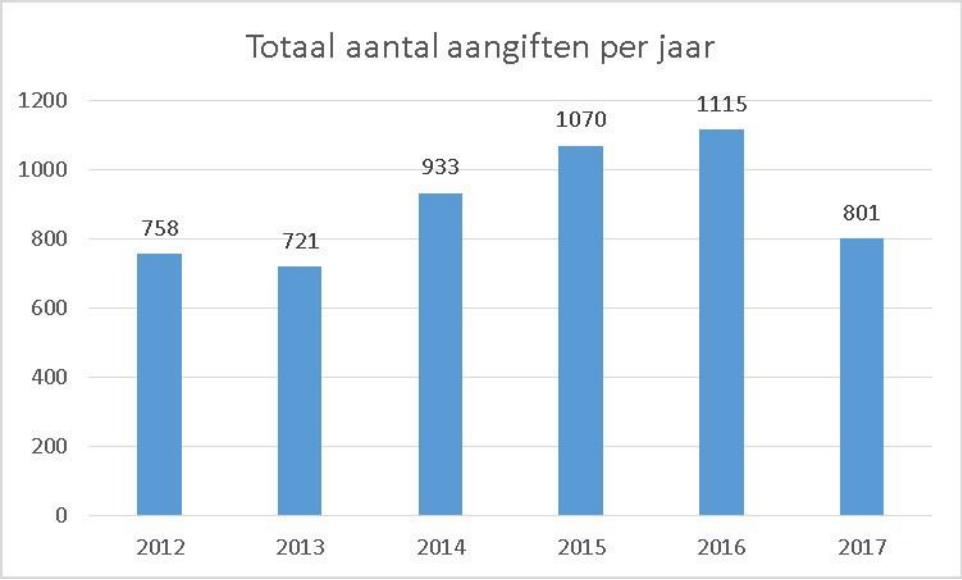
De oplichters nemen ruim de tijd: na twee uur 'oplossingen' te hebben geboden en verkocht, ging het scherm op zwart ging (het slachtoffer mocht zich even ontspannen) en kwam via de sms het verzoek om een iDeal-betaling te doen aan een bitcoinmaatschappij, waarbij een 10.2.g nodig was. Aan dat verzoek voldeed het slachtoffer. Daarna heeft hij het hele weekend, van vrijdag tot en met zondag, dit soort verzoeken gehad (totaal meer dan 60) en kreeg toen het vage idee dat er iets niet klopte. Hij moest wel in de buurt van zijn computer blijven, zodat de betalingen niet stagneerden en de oplichters konden blijven bellen. Op een gegeven moment deed hij normale aankopen en bleek er niets meer op zijn rekening te staan. Hij begrijpt niet hoe het zover heeft kunnen komen, omdat hij (zoals hij in de aangifte aangeeft) altijd overwogen uitgaven doet. Doordat hij zolang wachtte kon de bank niets meer betekenen.

Op de korte termijn is het niet mogelijk om (op een betrouwbare manier) alle aangiften door te nemen op specifieke kenmerken van het delict. Later zou meer ingezoomd kunnen worden op de hoogte van de schadebedragen, of de bedragen toenemen en hoe de slachtoffers worden benaderd.

5. Wat is de (geschatte) omvang van deze fraude?

Probeer op basis van harde gegevens een zo goed mogelijke inschatting te maken van de omvang van deze fraudevorm: hoeveel slachtoffers zijn er en wat is de impact op een individueel slachtoffer. Hoeveel economische schade wordt er aangericht in zijn totaliteit.

In de onderstaande tabel is de ontwikkeling van het aantal aangiften/meldingen te zien tussen 2012 en 2017. Dit is op basis van een aangepaste query die op Cognos (BVH) is gedraaid. In totaal ging het om 5398 aangiften over alle jaren. Vanaf 2013 is een stijging te zien, met in 2016 een totaal van 1115 meldingen/aangiften. Op basis van de voorlopige cijfers in 2017 is te verwachten dat dit aantal ook in dit jaar zal worden gehaald. Na iets minder dan 6 maanden staat de teller op 801 incidenten.

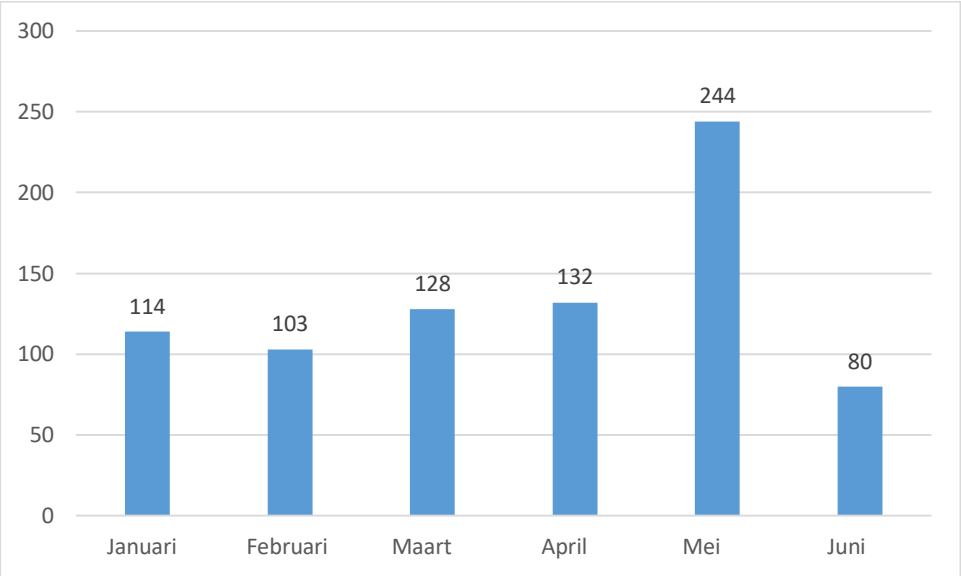


Er blijken grote verschillen te bestaan in **het aantal incidenten per eenheid**. Vooral in Oost-Nederland komen de meeste aangiften naar voren. Deze eenheid krijgt ongeveer twee keer zoveel meldingen/aangiften (890) dan in de meeste andere eenheden, zoals bijvoorbeeld Amsterdam, Limburg, Noord-Holland of Rotterdam.

De oorzaak is onbekend, het kan toevallig zijn en het gevolg van het grote werkgebied van deze eenheid. Daarnaast kunnen ook andere factoren een rol spelen, zoals meer aandacht op het onderwerp vanuit de politie, zijn de potentiele slachtoffers minder alert of mogelijk richten de daders zich (al dan niet tijdelijk) meer op deze regio.

Eenheid naam	2012	2013	2014	2015	2016	2017	Eindtotaal
Amsterdam	34	21	36	28	76	53	248
Den Haag	102	82	120	181	153	96	734
Limburg	61	44	73	86	77	53	394
Midden-Nederland	100	93	97	111	141	104	646
Noord-Holland	54	49	74	92	98	82	449
Noord-Nederland	75	78	99	105	111	69	537
Oost-Brabant	86	68	83	94	98	53	482
Oost-Nederland	101	122	166	189	166	146	890
Rotterdam	42	56	79	95	106	73	451
Zeeland-West-Brabant	101	107	106	85	85	70	554

Hierna is de ontwikkeling te zien van het aantal incidenten in 2017. Het eerste dat opvalt, is de toename in de maand mei, namelijk bijna twee keer zoveel dan in de andere maanden. In de eerste helft van juni lijkt deze toename nog niet door te zetten en zal naar verwachting ongeveer de omvang van maart en april krijgen.



De hoogte van de schadebedragen is al eerder beschreven: er zijn geen aanwijzingen dat de bedragen die worden buitgemaakt toenemen. De Fraudehelpdesk geeft aan dat de fraudeur zich een paar jaar geleden tevreden stelde met betalingen, maar zich nu toegang tot de rekening verschaft. Daardoor is de hoogte van de bedragen wel verandert, maar is wat ze buit maken afhankelijk van het bedrag dat op de rekening van het slachtoffer staat (en dat kan oplopen).

Een aantal keer heeft een bank een van de overschrijvingen kunnen tegenhouden. Bij een van de slachtoffers werd een tweede afschrijving van 9000 euro gestopt na een eerste storting. Het geld was wel al van de spaarrekening naar de betaalrekening overgeschreven. Banken zijn de afgelopen tijd alerter geworden op afwijkingen in betalingspatronen. De daders laten als gevolg hiervan hun slachtoffers steeds op andere manieren betalen. Zo worden slachtoffers aangezet om via Western Union te betalen. Dit gebeurt vaak door de slachtoffers in de war te brengen en/of allerlei onwaarheden te verkondigen. Bijvoorbeeld dat zij via Western Union moeten betalen omdat het internetbankieren plat zou liggen. Omdat Western Union geen kleine bedragen zou accepteren, wordt door 'Microsoft' zogenaamd (fictief) een bedrag overgemaakt die het slachtoffer inclusief het overeengekomen bedrag voor een abonnement dient over te maken. De storting van dit bedrag laat de dader dan meestal zien aan het slachtoffer om het verhaal geloofwaardig te maken. In werkelijkheid komt het hele bedrag van de rekening van het slachtoffer en zijn er geen stortingen door Microsoft gedaan.

Bron (BICC, 10.2.e): http://preproductie-bvi-cognos.politie.local/cognos10/cgi-bin/cognosisapi.dll?b_action=xts.run&m=portal/cc.xts&m_folder=i3CC52B23CB064479B4C3AF99D52FD001

6. Wie spelen een rol als facilitator van deze fraude?

Om fraude te kunnen plegen zijn vaak een aantal zaken nodig. Denk hierbij bijvoorbeeld aan een adres, een valse identiteit, een bankrekening, een website et cetera. Deze zaken worden vaak door andere partijen geleverd. Probeer een overzicht te schetsen en geef indien mogelijk daarbij aan of het hier om bewuste of onbewuste facilitators gaat.

Ofschoon het niet uit de aangiften blijkt, lijkt het erop dat wel katvangers ingezet worden om geld weg te sluizen. In het CBA Horizontale Fraude (NDB2017) is het als een probleem omschreven, het komt bij nagenoeg alle fraudevormen terug (een ook bij andere vormen van criminaliteit zoals witwassen) en werd door een expert als een plaag aangemerkt.

Katvangers worden vaak ingezet om crimineel verkregen geld weg te sluizen: jongeren die tegen een geringe vergoeding hun bankrekeningnummer beschikbaar stellen. Ze worden ingezet zodat leden en leiding van groeperingen dan buiten beeld kunnen blijven.

Ook het overschrijven van bedragen in bitcoins of andere virtuele valuta lijkt zijn intrede gedaan te hebben. Handel in deze *currency* is niet illegaal, maar stelt fraudeurs wel in de gelegenheid om met minder risico – door het anonieme karakter - frauduleus verkregen gelden weg te sluizen. Daarnaast verleiden de criminelen slachtoffers om online geld te versturen via partijen als Western Union. Tot slot vragen ze aan slachtoffers om iTuneskaarten te kopen en de nummers aan ze door te geven, maar hoe ze deze verzilveren of gebruiken is speculatief.

Hoofdstuk 2. Analyse aanpak fraude fenomeen

7. Welke partijen spelen een rol bij het voorkomen en bestrijden van deze vorm van fraude?

Vaak zijn er al partijen in beeld die een bijdrage –kunnen- leveren aan het bestrijden van deze vorm van fraude. Denk hierbij niet alleen aan politie en OM, maar ook bijvoorbeeld aan partijen die potentiële slachtoffers weerbaarder kunnen maken door middel van bijvoorbeeld voorlichting, of bonafide partijen die een vergelijkbare dienst aanbieden en belang hebben bij bestrijding van deze fraudevorm of dienstverleners die al dan niet bewust diensten verlenen aan/voor de fraudeur.

Tros Opgelicht en Fraudehelpdesk, en aandacht in andere media. Ondanks de vele voorlichting neemt het aantal slachtoffers en daarmee het aantal aangiften toe.

9. Wat is de gemeenschappelijke visie (publiek en privaat) op de aanpak van de inhoudelijke problematiek ?

Geef daarbij ook aan hoe de publiek-private samenwerking binnen het domein vorm is gegevens. Welke rolverdeling is daarbij aan de orde ?

Een gemeenschappelijk visie ontbreekt, terwijl experts aangeven dat Microftfraude al twee jaar een probleem is. Wanneer een vergelijking wordt getrokken met Marktplaatsfraude, dat al jaren 40.000 aangiften/meldingen per jaar oplevert, dan had Marktplaats er in de eerste plaats zelf belang bij om geen reputatieschade op te lopen. Zodoende investeerde Marktplaats in voorlichting, ook stelselmatig op de website, samenwerking met de politie (resulterend in oprichting LMIO, Landelijk Meldpunt Internetoplichting) en een eigen afdeling fraude waarbij de medewerkers actief fraude opsporen op Marktplaats. Marktplaats is gevestigd in Nederland en dat maakte deze aanpak laagdrempeliger en het bereik groot. Microsoft lijkt meer een *ver-van-mijn-bed -show*, omdat het hoofdkantoor in Amerika is gevestigd en in het algemeen communicatie met buitenlandse software bedrijven moeilijk is. Voorlichting over MF gebeurt via verschillende media, Tros Opgelicht en de Fraudehelpdesk spelen een actieve rol, en daar blijft het bij. Microsoft vertoont geen actie: de aanpak beperkt zich tot voorlichting op de eigen website, maar dit werpt de retorische vraag op wie dat leest. Waarschijnlijk alleen personen die zich toch al bewust zijn van de gevaren.

Microsoft zou zijn waarschuwing kunnen uitbreiden door een persoonlijke boodschap via mailing of pop-up op de website of wanneer de Teamviewer in beeld komt. Ook Microsoft zou meer beducht kunnen zijn op negatieve aandacht in de media in deze met als gevolg imagoschade.

Tot slot is het aannemelijk om contact te zoeken met de Nederlandse Vereniging van Banken en de Betaalvereniging (beiden hebben diverse malen bijgedragen aan het NDB). In het verlengde van alle activiteiten die ze al uitvoeren, waardoor de schade sterk is teruggelopen, zouden ze ook kunnen waarschuwen op de betalingssite van klanten (klanten worden tot nu toe regelmatig gewaarschuwd voor phishing).

10. Welke integrale aanpak / interventiestrategie wordt er op dit moment gehanteerd?

Beschrijf de totale (reeds bestaande) interventiestrategie, van preventie tot repressie, incl. vergroting bewustwording en weerbaarheid bij de verschillende modus operandi van de fraudeur. Beschrijf voorts welke actie door welke partij wordt/is opgepakt, Kortom welke afspraken zijn er m.b.t. preventie en repressie (civiel, bestuurs- en strafrechtelijk)?
Dit onderdeel dient gezamenlijk (publieke en private partners) te worden ingevuld.

Voorlichting tot nu toe voornamelijk via media. Tros Opgelicht en de Fraudehelpdesk spelen een actieve rol, waaraan ook de eenheid Midden-Nederland heeft bijgedragen. De Nederlandse politie wordt bemoeilijkt in de opsporing, omdat de dadergroepen in landen verblijven waarmee geen uitwisselingsverdragen of samenwerking bestaat.

Er is geen integrale aanpak:

Vanuit het OM bestaat het voornemen om contact te zoeken met Microsoft.

THTC: bevindt zich in een netwerk met Microsoft. Er is contact gelegd met Teamviewer in Duitsland.

Er zou contact gezocht moeten worden met de NVB en Betaalvereniging (banken zijn eerder heel succesvol geweest in het terugdringen van de financiële schade van fraude)

FBI: probleem bestaat ook naar verluidt in de Verenigde Staten. Contact leggen door THTC.

11. Hoe kan deze integrale aanpak/ interventiestrategie effectiever worden vormgegeven?

Op welke wijze kan de aanpak van de fraude effectiever worden vormgegeven? Denk daarbij aan samenwerking binnen de keten, maar ook aan een betere toerusting van individuele schakels in de keten. Kortom wat is er nog te doen?
Dit onderdeel dient gezamenlijk (publieke en private partners te worden ingevuld.

Geen suggesties

Bijlage. Contactpersonen en gebruikte literatuur

A. Contactpersonen (organisatie, naam en contactgegevens)

Betaalvereniging Nederland, 10.2.e , 10.2.e @betaalvereniging.nl Nederlandse Vereniging van Banken: 10.2.e (contact leggen via auteurs van deze quickscan; deze personen maken deel uit van het netwerk horizontale fraude en zijn geïnterviewd voor het NDB). 10.2.e , Fraudehelpdesk (gemaild op 18 juni 2017).

B. Gebruikte literatuur (bij voorkeur directe weblinks opnemen) en andere bronnen

CBA Horizontale Fraude (NDB2012 en NDB2017) Cijfers Fraudehelpdesk opgevraagd (18 juni 2017) BICC (aangiften BVH)