QUICK SCAN

FRAUDE LOONT... nog steeds

Alex van Geldrop, MSc
Prof. dr. ir. Theo de Vries

Stichting Toekomstbeeld der Techniek

UNIVERSITEIT TWENTE.

QUICK SCAN

FRAUDE LOONT...
nog steeds

Colofon

Auteurs Alex van Geldrop, STT, Den Haag en Theo de Vries, UT, Enschede / STT, Den Haag
Taalredactie Annette Potting, STT, Den Haag
Zetwerk: Ellen Bouma, www.ellenbouma.nl
Drukwerk Quantes, Den Haag
Datavisualisatie, pagina 13 Meinou de Vries, Utrecht
Foto's Thinkstock/Gettyimages

ISBN/EAN: 978-94-91397-10-3

STT-publicatie
NUR 980

Trefwoorden: technologische ontwikkelingen; fraude; fraudebestrijding; fraudebeheersing; identiteitsfraude; cybercrime; datamining; big data; trends; economie; schade; belastingfraude; privacy; toekomstbeeld; toekomst; financieel; complexiteit; interconnectivity; data

Inhoud

Voorwoord

Onder de titel 'ICT & Fraude: Fraude Loont' organiseerden de Stichting Toekomstbeeld der Techniek (STT) en de Universiteit Twente (UT) drie jaar geleden een succesvolle topconferentie, waarbij ook een gelijknamige quick scan werd gepubliceerd. Die titel was veelbetekenend. Uit interviews en onderzoeken bleek dat de pakkans van fraudeurs bijzonder laag was, soms niet hoger dan 1%, en dat de geschatte schade in Nederland minimaal €10 miljard per jaar bedroeg. Er was grote behoefte aan gericht beleid, al was het maar om de vele miljarden die de overheid misliep boven water te krijgen.

Het bewustzijn over de ernst van fraude is sindsdien sterk gegroeid. Met de nota *Rijksbrede aanpak fraude (2013)*[1] heeft de overheid zich bereid getoond energie te steken in een integrale fraudeaanpak. Niet alleen vanwege de financiële schade, maar ook vanwege de maatschappelijke impact van fraude. In het bedrijfsleven zien we een vergelijkbare trend: men is zich beter bewust van de urgentie van het fraudeprobleem, al vinden stappen die leiden tot een concrete aanpak nog maar mondjesmaat plaats. Voortvloeiend uit deze conferentie is er bovendien ook een onderzoeksinstituut en samenwerkingsplatform opgericht, het Dutch Fraud Initiative. Dit heeft zich ten doel gesteld om nieuwe kennis over fraudedetectie te ontwikkelen en te delen, om zo de integrale samenwerking tussen overheid, wetenschap, bedrijfsleven en maatschappelijke organisaties te bevorderen.

Technologische ontwikkelingen gaan echter razendsnel en fraudeurs maken hier gretig gebruik van. Cybercrime en identiteitsdiefstal zijn voorbeelden van fraudes die worden gefaciliteerd door ICT-ontwikkelingen en waar nog geen passend antwoord op bestaat. Om deze uitdagingen het hoofd te bieden, moet vooruit gekeken worden. Temeer omdat er ook nieuwe methodes ontstaan om fraude te bestrijden. Vooral op het gebied van fraudedetectie is de technologische vooruitgang nauwelijks bij te benen.
Op 24 april 2015 is een tweede topconferentie georganiseerd om deze onderwerpen te adresseren. Dit boekje zal, net als bij de eerste conferentie in 2012, de nodige achtergrondinformatie geven. De sectorgewijze overzichten van het eerste boekje (*ICT & Fraude: Fraude Loont*) komen terug, maar dan als update anno 2015. Er lijken nog geen structurele fundamentele veranderingen te zijn. Terwijl de technologische mogelijkheden een revolutie doormaken. De mogelijkheden van geavanceerde methodes voor opsporing van fraude nemen nog steeds toe. De bewustwording en de positieve intenties voor het gebruik hiervan zijn ook aanwezig, maar vooralsnog is het wachten op grootschalige structurele resultaten. De titel 'Fraude Loont' wordt daarom wederom gehanteerd, maar nu met de ondertitel: 'nog steeds'.

Wij hopen dat dit boekje opnieuw aanleiding tot veel discussie zal geven.

Drs. Pierre Morin
Directeur Stichting Toekomstbeeld der Techniek

Prof. dr. ir. Theo de Vries
Hoogleraar Universiteit Twente / Stichting Toekomstbeeld der Techniek

1 *Rijksbrede aanpak fraude*, 20 december 2013, Nota van het Ministerie van Veiligheid en Justitie.

Inleiding

Wat is fraude?

Fraude is een complex begrip en een verzamelnaam voor een veelvoud van illegale activiteiten. Er is geen wet die fraude op zichzelf strafbaar stelt en toch weet iedereen gevoelsmatig wanneer iets als frauduleus bestempeld kan worden. Om toch een heldere scheidslijn te schetsen tussen fraude en andere criminele activiteiten hanteren we de volgende definitie:

> "Fraude betreft een opzettelijke handeling waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging ontstaat, waardoor er een onrechtmatig voordeel wordt verkregen." [Schimmel, 2004]

Een aantal kernvoorwaarden van fraude komen hierbij naar voren, waarbij de nadruk ligt op misleiding en opzet. Oftewel, fraude is altijd een bewuste actie om door misleiding voordeel te behalen.

Deze definitie is breed genoeg om een grote groep illegale activiteiten onder de noemer fraude te laten vallen (bv. phishing, identiteitsdiefstal, en valse zorgdeclaraties), maar ook eng genoeg om activiteiten als afpersing, diefstal en geweldsdelicten uit te sluiten.

Of er sprake is van opzet, nalatigheid, of onkunde is lang niet altijd helder. Wordt er bewust een onjuiste voorstelling van zaken gegeven of legt men slechts sterk de nadruk op een aantal specifieke aspecten? Wanneer is er sprake van oplichting en wanneer van slim overtuigen? De grens is smal en er zal altijd een grijs gebied zijn. De gekozen definitie helpt om een consequente lijn te volgen, maar gezond verstand zal uiteindelijk leidend moeten zijn in de beoordeling van de fraudevraag.

Met de aanhoudende ontwikkelingen binnen ICT groeit dit grijze gebied. De hoeveelheid data groeit nog steeds exponentieel en systemen blijven complexer worden. De noodzakelijke analysetools om fraude te determineren lopen achter bij deze ontwikkelingen. Het is, met andere woorden, steeds moeilijker om te bepalen of er opzet in het spel is.

Tegelijkertijd veranderen door technologische ontwikkelingen het karakter en de eigenschappen van fraude in rap tempo. Fraudeurs zijn extreem innovatief. Zij maken gretig gebruik van alle mogelijkheden die beschikbaar zijn en kennen geen morele dilemma's, bureaucratische obstakels of culturele belemmeringen.

Doordat de complexiteit van systemen de laatste decennia enorm toegenomen is, ontstaan er meer kwetsbaarheden waar fraudeurs op in kunnen spelen. Dit in combinatie met de nieuwe instrumenten die ICT aan fraudeurs biedt, maakt het zeer moeilijk om een compleet fraudebestendig systeem te bouwen. Daarnaast is het internet op zichzelf een waar Walhalla voor fraudeurs. Nagemaakte en verzonnen identiteiten, replica's van officiële websites, toegang tot ontelbare potentiële slachtoffers, gerichte e-mails om anderen om de tuin te leiden. Het is niet alleen mogelijk, maar zelfs betrekkelijk eenvoudig.

De potentiële financiële schade die een fraudeur tegenwoordig kan veroorzaken, is mede hierdoor vele malen groter dan in het verleden. Dit zien we onder andere terug in de omvang van enkele van de grotere fraudes die de afgelopen jaren aan het licht zijn gekomen en waarbij de schade in de miljarden euro's loopt.

Het mes snijdt gelukkig aan twee kanten en ook opsporingsdiensten en andere organisaties maken gebruik van technologische mogelijkheden om fraude te voorkomen en detecteren. Nieuwe beroepen ontstaan, wie had twintig jaar geleden gehoord van een ICT-detective?

Het maatschappelijk effect van fraude

Fraude is niet een recent fenomeen. Er zijn voorbeelden van fraude te vinden sinds de

eerste geschreven teksten. Er zijn altijd individuen geweest die door middel van list en bedrog onrechtmatig voordeel probeerden te behalen en die zullen er ook altijd blijven. Fraude vindt dan ook plaats in alle segmenten van de samenleving. Hoog- en laagopgeleid; man en vrouw; autochtoon en allochtoon; jong en oud. Fraude lijkt inherent aan onze maatschappij.

Naast de financiële gevolgen is er een ander aspect dat vaak onderbelicht blijft, maar dat misschien nog wel belangrijker is, namelijk de schade aan het vertrouwen in de samenleving.

Grote fraudezaken komen tegenwoordig onder de aandacht van een groot publiek en daarbij worden ook de omvang, de lage pakkansen en de relatief lage straffen belicht. Het is niet vreemd dat mensen het vertrouwen in de werking van het systeem verliezen als blijkt dat fraude simpel uit te voeren is en dat daders er vaak zonder serieuze consequenties vanaf komen.

Daarmee heeft fraude een eroderend effect op de maatschappij. De bevolking verliest het vertrouwen in de politiek en het samenhorigheidsgevoel neemt af. Waarom zou iemand belasting betalen als het blijkbaar eenvoudig en risicoloos is om deze te ontduiken? Ditzelfde fenomeen is te zien op menige verjaardag, wanneer er trots wordt verteld over de valse declaratie van een 'verloren' telefoon. Het gebrek aan consequenties maakt dat fraude nauwelijks de uitzondering, maar bijna de norm wordt. Het respect voor de rechtsstaat brokkelt daardoor af.

De grootte van dit effect is onbekend, maar het is duidelijk dat er bij een aantal fraudesoorten al een zekere mate van maatschappelijke acceptatie bestaat. Verzekeringsfraude en zwartwerken bijvoorbeeld komen niet alleen veelvuldig voor, maar worden zelfs zonder schroom openlijk besproken.

Deze sociale acceptatie is een serieus probleem. Fraude wordt vaak gezien als misdaad zonder slachtoffer (of met de anonieme verzekeraar, bank of overheid als slachtoffer), waarbij de omvang van de schade nauwelijks werkelijke impact heeft. Het besef ontbreekt dat het uiteindelijk over miljarden euro's per jaar gaat die door de samenleving zelf opgehoest moeten worden. Cultuurverandering is noodzakelijk. Hoe kan men anders de goedbedoelende burger uitleggen dat hij meebetaalt aan kosten die worden veroorzaakt door fraudeurs, terwijl er nauwelijks energie en middelen worden ingezet om dit tegen te gaan?

Deze cultuurverandering zal niet alleen bij de individuele burger moeten plaatsvinden. Jarenlang hebben overheid en bedrijven de preventie en het bestrijden van fraude een te lage prioriteit gegeven. Pas sinds enkele jaren lijkt er een tendens te zijn om meer energie en middelen toe te wijzen aan fraudebestrijding. Met de lancering van de *Rijksbrede aanpak fraude* is daar eind 2013 een goed signaal voor afgegeven. Dit is ook zeker noodzakelijk. Pakkansen van minder dan 1%, hoge winsten en lage straffen zijn nog steeds geen uitzondering. Een integrale aanpak van overheid, bedrijfsleven en bevolking, waarbij men anticipeert op toekomstige ontwikkelingen lijkt de enige weg naar een gezonde samenleving.

In de eerste uitgave van deze publicatie in 2012 werd de geringe aandacht voor fraude en de noodzaak voor verdere bewustwording al gesignaleerd. Sindsdien is de aandacht voor fraude zowel op maatschappelijk als politiek vlak sterk toegenomen, maar is er nog geen sprake van een samenhangend en werkend beleid dat zich niet alleen richt op repressie van fraude, maar ook op de preventie ervan. Dat is dé uitdaging voor de komende jaren.

Bronnen

- Schimmel, PJ (2004). *Fraudebeheersing: hoe doe je dat?* Deventer. Kluwer.

De invloed van ICT op fraude en fraudebestrijding

Door technologische ontwikkelingen is de toegankelijkheid, opslagcapaciteit, verwerkingssnelheid en ontsluiting van data de laatste decennia exponentieel toegenomen. Sociale media, bevolkingsregisters, kadasters, de gemeentelijke basisadministratie en de website van de lokale voetbalclub zijn slechts enkele voorbeelden van de duizenden databases waarin persoonlijke gegevens worden opgeslagen. Vaak zijn deze gegevens relatief eenvoudig in te zien voor derden en hierdoor ontstaat een digitale omgeving waar fraudeurs tot enkele decennia geleden slechts van durfden te dromen.

De toenemende hoeveelheid beschikbare data is echter ook op positieve wijze in te zetten. Door technologische ontwikkelingen kunnen grote bergen ongestructureerde datasets steeds effectiever geanalyseerd worden. Omdat fraude per definitie een afwijking betreft, biedt dit de mogelijkheid om veel sterkere fraudedetectiemethodes dan ooit tevoren te ontwikkelen.

In dit hoofdstuk beschrijven we de algemene invloed van ICT op fraude en fraudebestrijding. In het volgende hoofdstuk gaan we dieper in op de ontwikkelingen per fraudedomein.

ICT en fraude

Het effect van ICT op fraude is tweeledig. Allereerst bieden de ontwikkelingen in de informatie- en communicatietechnologie nieuwe instrumenten aan fraudeurs, waarmee zij bestaande vormen van fraude effectiever en efficiënter uit kunnen voeren. Daarnaast zorgen de ICT-ontwikkelingen er ook voor dat er volledig nieuwe vormen en methodes van fraude ontstaan die zonder deze ontwikkelingen niet mogelijk zouden zijn.

De nieuwe instrumenten zijn relatief eenvoudig te benoemen. Door middel van bijvoorbeeld trojans, rootkits,[2] virussen en phishing emails hebben fraudeurs een arsenaal aan wapens om gevoelige informatie binnen te halen. Met deze informatie kunnen vervolgens weer allerlei soorten fraudes plaatsvinden.

Cyberfraudeurs hebben vaak een technologische voorsprong op publieke en commerciële organisaties. Zonder de restricties van wetgeving, bureaucratische voorschriften en bedrijfscultuur zijn fraudeurs in staat om illegale activiteiten uit te voeren met minieme pakkansen en potentieel zeer hoge opbrengsten.

2 Trojan (horse): een verborgen functie in een programma dat door de gebruiker wordt geïnstalleerd. Deze functie kan aan kwaadwillenden toegang verschaffen tot de geïnfecteerde computer en zo schade toebrengen aan de computergegevens of de privacy van de gebruiker. Rootkit: een set softwaretools die wordt gebruikt door een derde partij na toegang te hebben verkregen tot een (computer)systeem.

Naast deze instrumenten zorgen de technologische ontwikkelingen ook voor een fundamentelere verschuiving in de wijze waarop fraude plaatsvindt. Dat heeft er in de eerste plaats mee te maken dat naarmate systemen complexer worden er meer kwetsbaarheden ontstaan. Met de wildgroei aan databases en de verregaande onderlinge koppeling hiervan ontstaan er systemen die zo complex zijn dat zij onbeheersbaar worden.

Voorbeeld: Een recent voorbeeld van de kwetsbaarheid van complexe systemen is het besturingssysteem 'Windows XP'. De complexiteit hiervan is zo groot dat er zelfs een decennium na vrijgave nog steeds nieuwe kwetsbaarheden gevonden en opgelost werden.[3]

De stelling dat het aantal kwetsbaarheden toeneemt naarmate de complexiteit toeneemt, geldt overigens niet alleen voor software-systemen, maar ook voor organisatorische systemen. Voorbeelden hiervan zijn het belasting- en zorgstelsel, waarbij de vele uitzonderingen, verschillende tarieven, en constante veranderingen hebben gezorgd voor systemen die nauwelijks te beheersen zijn met alle consequenties vandien. Bovendien rusten deze toch al complexe systemen vaak ook nog op een ingewikkelde ICT-infrastructuur.

Mass Marketing Fraud

Ging traditionele fraude vaak om het benadelen van individuen of specifieke organisaties, tegenwoordig bieden de ontwikkelingen in ICT aan fraudeurs de mogelijkheid om potentiële slachtoffers massaal te benadelen. Types fraude die aan dit kenmerk voldoen, staan bekend onder de noemer *Mass Marketing Fraud* (MMF). MMF behelst alle activiteiten waarbij er sprake is van pogingen om massaal derden te benadelen. Zonder er verder specifiek op in te gaan, kan dit onder meer betrekking hebben op loterijfraude, datingfraude, *advance fee fraud*, en *Nigerian 419 fraud*.

De anonimiteit, de grote hoeveelheid potentiële slachtoffers en het grensoverschrijdende karakter zijn kenmerkend voor deze nieuwe vormen van fraude.

Cybercrime

Wanneer we het hebben over de rol van ICT binnen fraude wordt snel de link met cybercrime gemaakt. De twee begrippen zijn echter niet synoniem aan elkaar.

Cybercrime kan gedefinieerd worden als criminaliteit waarbij ICT het middel en/of het doelwit is [Jospeh, 2006]. De term cybercrime is daarmee veel breder dan fraude met behulp van ICT. Dit is ook terug te zien in het percentage mensen dat jaarlijks slachtoffer is van cybercrime, namelijk 8,5% van de bevolking [Domenie, 2014]. Het moge duidelijk zijn dat niet elke vorm van cybercrime fraude is.[4]

ICT en fraudebestrijding

Fraudeurs zijn niet de enigen die gebruik maken van technologische ontwikkelingen. Bedrijven, overheidsinstanties en particulieren die fraude willen voorkomen of detecteren, maken steeds vaker gebruik van de nieuwe mogelijkheden die ICT biedt. Deze maatregelen kunnen variëren van uiterst simpel tot zeer complex.

De meest effectieve vorm van preventie zal altijd het gebruik van gezond verstand blijven. Door gevoelige gegevens te bewaren in een afgeschermde ICT-omgeving (in plaats van op websites die niet te vertrouwen zijn), geen volledige kopieën van identiteitskaarten te verstrekken en door niet in te loggen op websites waar u indirect (bijvoorbeeld door te klikken op een link in e-mails) terecht bent gekomen, wordt de veiligheid al sterk verhoogd. Andere simpele maatregelen die misbruik bemoeilijken zijn het installeren en up-to-date houden van firewall, antivirussoftware en andere software.

3 Dit was althans het geval tot 8 april 2014, toen de ondersteuning voor Windows XP werd beëindigd. Sindsdien wordt aangeraden om een nieuwer besturingssysteem te installeren.

4 Eén voorbeeld van cybercrime die geen fraude is, is *ransomware*, waarbij de computer 'gegijzeld' wordt door een stukje software. De gebruiker moet een betaling verrichten om deze weer in eigen beheer te krijgen. Het verschil met fraude is dat er hierbij geen sprake is van een valse voorstelling van zaken.

Een iets complexere maatregel, maar nog steeds relatief eenvoudig is het bouwen van databases met zwarte lijsten van bekende fraudeurs. Namen van fraudeurs komen in een bestand dat toegankelijk is voor andere organisaties in dezelfde sector, waardoor deze personen niet langer welkom zijn of in een verhoogd risicoprofiel vallen waarvoor extra controlemaatregelen gelden.

Meer geavanceerde risicomodellen worden inmiddels gemeengoed. Deze modellen maken een inschatting van de kans dat er in een specifiek geval sprake is van frauduleuze activiteiten. De modellen variëren van simpele scoringslijsten tot data-analyse-instrumenten die op basis van enorme hoeveelheden data gewichten aan variabelen toekennen en vervolgens tot een *risicoscore* komen. Technieken als kunstmatige neurale netwerken spelen daarbij een dominante rol. Deze instrumenten zijn pas sinds enkele jaren operationeel beschikbaar en het is pas sinds kort mogelijk om enorme hoeveelheden ongestructureerde data in te zien en te analyseren (big data analysis). Daardoor kunnen de effectiviteit en nauwkeurigheid van fraudedetectie aanzienlijk worden verhoogd.

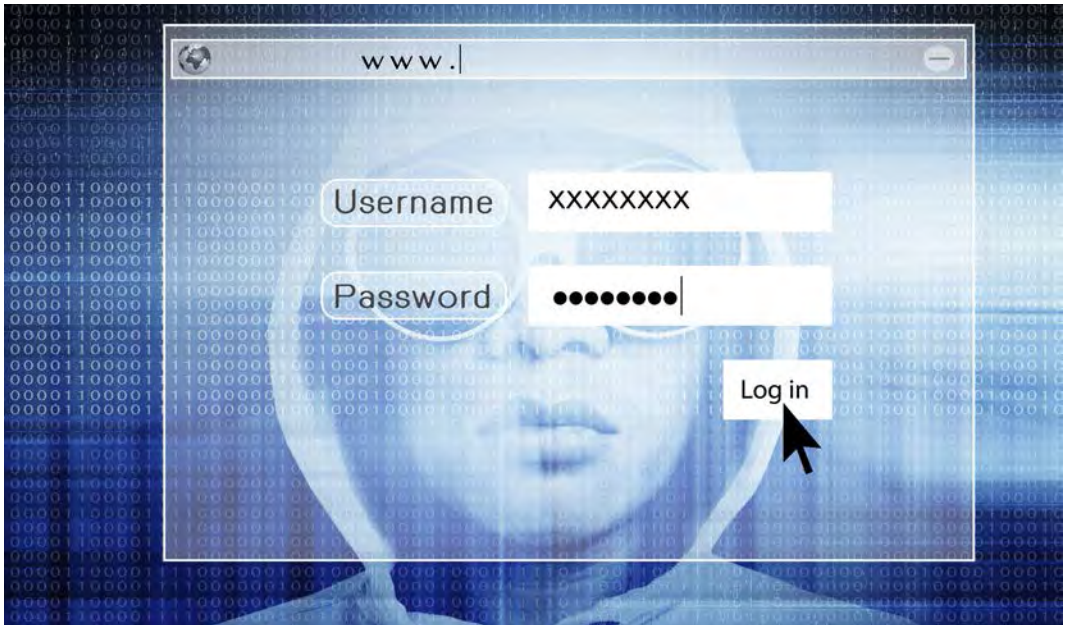
State-of-the-art zijn de modellen die real-time data interpreteren en verdachte afwijkingen detecteren en rapporteren. Het meest bekende voorbeeld is de bank die u belt wanneer u in het buitenland geld opneemt en dit als een afwijking van normaal gedrag bestempelt.

Bij de opsomming van deze opsporingsmethodes past een belangrijke kanttekening. De kwaliteit van de methodes en resultaten verschilt enorm per sector en per organisatie. *Best practices* worden slechts bij uitzondering gedeeld. Deels vanwege concurrentiegevoeligheid, maar vaak ook omdat, zoals bij de Rijksoverheid, een effectieve infrastructuur ontbreekt om tot deling van kennis te komen over de (ontwikkeling van) opsporingsmethodes. Een goede infrastructuur is een noodzakelijke voorwaarde voor het kunnen delen van dergelijke kennis.

Dit hoofdstuk heeft enkele algemene ontwikkelingen op het snijvlak van ICT en fraude(bestrijding) beschreven. In het volgende hoofdstuk wordt dieper ingegaan op specifieke fraudesoorten en bijbehorende ontwikkelingen.

Bronnen

- Joseph, A (2006). 'Cybercrime definition'. Computer Crime Research Center. http://www.crime-research. org/articles/joseph06/
- Domenie, MLL, ER Leukfeldt, JA van Wilsem, J Jansen & WPh Stol (2013). *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma Uitgevers.



Blik op het veld

Om tot een gerichte fraudeaanpak te komen, is het nodig inzicht in de aard en omvang van fraude te hebben. Daarvoor is meer nodig dan een momentopname, ook trends zijn belangrijk. Om deze in beeld te brengen is betrouwbare data nodig die met regelmaat opnieuw wordt gemeten. Zonder deze data is elke aanpak van fraude een schot in het duister.

Dit is een probleem. Aan de ene kant is fraudebestrijding prioritair, maar aan de andere kant is betrouwbare en up-to-date informatie over relevante aspecten van fraude een zeldzaamheid. Daardoor valt moeilijk te onderbouwen welke maatregelen de meeste baten zullen opleveren en zijn resultaten nauwelijks te meten. Er zijn weliswaar enkele positieve uitzonderingen van sectoren waar meer informatie beschikbaar is, maar niet voldoende om de omvang van het probleem nauwkeurig in beeld te brengen.

In deze publicatie wordt een indicatief beeld geschetst van de problematiek rondom fraude en de bestrijding daarvan en met name van de wijze waarop beiden worden beïnvloed door ontwikkelingen binnen de informatietechnologie. Het doel is om verdere bewustwording te versterken om zo tot de initiatie van relevant beleid te komen.

De publicatie heeft niet tot doel om tot een nauwkeurig en uitputtend overzicht te komen van de verschillende kenmerken van fraude. Daarvoor ontbreekt de benodigde data. Volstaan zal worden met een schets van het huidige veld op basis van openbare bronnen. Ondanks deze beperkingen is deze schets voldoende overtuigend om de noodzaak voor het verwerven van additionele kennis aan te geven.

Fraudebeleid is noodzakelijk en ook profijtelijk. Uit gesprekken met experts blijkt keer op keer dat investeringen gericht op de signalering van fraude ruimschoots terugverdiend worden. De kosten komen echter voor de baten en de effecten zijn moeilijk meetbaar. Mede hierdoor krijgt fraudepreventie en -bestrijding vaak niet de prioriteit die het zou moeten krijgen. Fraude wordt te vaak gezien als een vervelende maar onvermijdbare kostenpost.

Een essentieel probleem bij veel soorten fraude is het gebrek aan een eindverantwoordelijke. Fraudeurs maken geen onderscheid tussen sectoren en formele grenzen. Het is een overkoepelend probleem. Bovendien is de verwachting dat door de intensivering van ICT-gebruik grenzen in de toekomst nog verder zullen vervagen.

Er wordt vaak onderscheid gemaakt tussen verticale en horizontale fraude. Hiermee wordt gedoeld op fraude die betrekking heeft op de overheid (verticaal) of op het bedrijfsleven (horizontaal). Daarnaast is er ook sprake van fraude bij burgers. Deze onderscheiden zullen wij in deze publicatie verder niet hanteren. Fraude betreft een nationale problematiek, waarbij verkokering alleen maar begrenzend werkt. We volstaan er daarom mee de bestaande verschillen hier te benoemen.

Gezien de toenemende intersectorale (en internationale) eigenschappen van fraude en het gebrek aan een duidelijke eindverantwoordelijke zal de overheid een dominante rol moeten spelen bij de bestrijding ervan. Doet zij dit niet, of onvoldoende, dan ligt een sluipende erosie van het draagvlak voor de rechtstaat om de hoek. De overheid is de stakeholder die op basis van het grotere belang zal moeten handelen en zij zal dus zowel verantwoordelijkheid als initiatief moeten nemen. Een overheid die fraudebestrijding als prioriteit benoemt zal anderen meenemen in haar acties. Deze boodschap lijkt te zijn begrepen. Met de *Rijksbrede aanpak fraude* heeft de overheid in 2013 een veelbelovend begin gemaakt. Gegeven de grote belangen die op het spel staan, is een regelmatige *assessment* van de vorderingen van de *Rijksbrede aanpak fraude* een vereiste.

Omvang van fraude

Zoals eerder aangegeven is het slechts mogelijk om een zeer grove schatting te geven van de totale schade door fraude. Het komen tot nauwkeurige

schattingen is niet mogelijk op basis van bestaande data. Dit wordt onder andere geïllustreerd door twee publicaties die onlangs het nieuws hebben gehaald. Beiden geven hun eigen schatting van de fraudeomvang in Nederland. Waar het ene onderzoek [PWC, 2014] tot een bedrag van €11 miljard per jaar komt, zat het andere onderzoek [Schalke en Partners, 2014] daar bijna een factor drie boven met een schatting van minimaal €30 miljard per jaar.[5] Gaan we op basis van internationaal onderzoek extrapoleren dan komen er nog hogere bedragen naar voren. Onderzoek toont bijvoorbeeld aan dat er over de afgelopen 17 jaar gemiddeld 5,6% van het bruto nationaal product aan fraude verloren zou zijn gegaan [Gee & Button, 2015]. Dit zou in Nederland voor het jaar 2014 uitkomen op een verloren bedrag van maar liefst €49 miljard euro per jaar.[6] Hoe dan ook, schade als gevolg van fraude is substantieel.

De hoogte van de geschatte omvang van fraude hangt af van de gebruikte definities en de fraudedomeinen die worden meegenomen in de berekening. Zo is er vaak geen duidelijk onderscheid tussen de omvang van de schade door fraudeurs die daadwerkelijk vervolgd zijn, fraude die wel gedetecteerd maar niet vervolgd wordt, en schattingen van de totale fraude. Verder baseren bestaande onderzoeken zich voornamelijk op openbare bronnen en onderzoeken van derden, waarbij elk onderzoek zijn eigen methodes hanteert. Kortom, de genoemde bedragen zijn niet nauwkeurig genoeg om als solide richtsnoer te dienen. Ze zijn echter wel indicatief voor de enorme omvang van dit maatschappelijke probleem.

Ook deze publicatie moet zich helaas behelpen met de beperkte informatie zoals die beschikbaar is. Gestructureerde en terugkerende metingen zijn nauwelijks voorhanden en op dit moment ontbreekt er een instantie die zich hiervoor verantwoordelijk voelt of die hier de middelen voor (gealloceerd) heeft.[7]

Wel kan er op een gestructureerde wijze per fraudedomein worden aangeven welke informatie bekend is over het type fraude, de schadeomvang, en de rol van ICT bij het uitvoeren en bestrijden ervan.

In dit hoofdstuk geven we een overzicht van de kenmerken van een aantal fraudedomeinen. Het is hierbij van belang op te merken dat de genoemde fraudebedragen niet zonder meer bij elkaar opgeteld kunnen worden. Fraudeurs houden zich niet aan de grenzen en definities die wij opstellen. We proberen dus een gestructureerd en begrensd beeld te schetsen van een fenomeen dat chaotisch is, zich in de duisternis ophoudt en zich niet houdt aan formele grenzen.

Waarom dan toch dit overzicht? Allereerst om bewustzijn te creëren over de enorme economische betekenis van fraude en de maatschappelijke impact ervan. Ten tweede, om beleidsmakers en fraudebestrijders een overzicht te geven van de thans bekende eigenschappen van verschillende fraudedomeinen. En ten derde om de aandacht te vestigen op de vele noodzakelijke informatie die nog ontbreekt.

Mede hierom is het niet zinvol om een uitputtend overzicht op te stellen. Wij beperken ons tot een aantal van de meer aansprekende fraudesoorten. Een overzicht van onze bevindingen ziet u in de grafische weergave op de volgende pagina. Een aantal conclusies worden direct duidelijk. (1) De financiële schade is enorm, (2) ICT speelt een grote rol bij vele fraudesoorten en bij de bestrijding ervan, en (3) er is een groot gebrek aan betrouwbare data, waardoor we ons voornamelijk moeten behelpen met schattingen en extrapolaties.

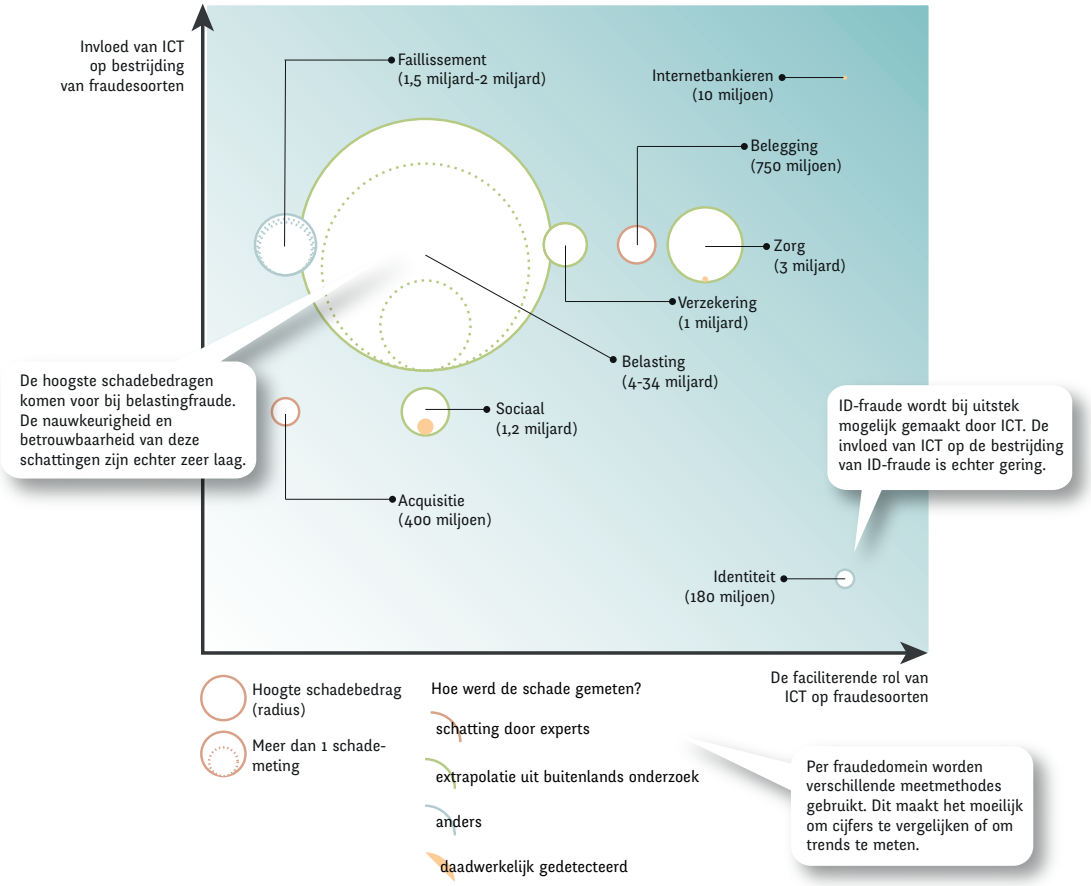
5 Veel van de bedragen bij met name het onderzoek van Schalken & Partners zijn gebaseerd op de bevindingen van de 1e druk van deze quick scan uit 2012.

6 Uiteraard zijn de resultaten niet één op één overdraagbaar naar de situatie in Nederland en daarom benadrukken we dat dit niet gezien moet worden als een poging om de omvang te becijferen, maar slechts als indicatie om de ernst van het probleem verder te verduidelijken.

7 Naar aanleiding van de quick scan en conferentie uit 2012 is het Dutch Fraud Initiative opgericht dat zich onder andere ten doel heeft gesteld om tot betrouwbare en wetenschappelijk accurate metingen te komen. Daarnaast zijn ook andere initiatieven ontplooid.

We benadrukken nogmaals dat het hier slechts om een indicatief overzicht gaat, waarbij we met name de rol van ICT willen aantonen. In de komende hoofdstukken zullen we deze bevindingen nader uitleggen.

Financiële omvang fraudedomeinen en de rol van ICT



» ACQUISITIEFRAUDE

Definitie

Misleidende handelspraktijken tussen organisaties, waarbij bepaalde verkooptechnieken worden gebruikt, gericht op het winnen van vertrouwen en het wekken van verwachtingen teneinde de ander te bewegen tot het aangaan van een overeenkomst, waarbij de tegenprestatie niet of nauwelijks naar behoren wordt geleverd [Huisman & van de Bunt, 2009].

Alle gevallen van acquisitiefraude hebben met elkaar gemeen dat de malafide aanbieders er op gericht zijn om een handtekening of instemming te ontfutselen, zodat er een rechtsgeldige vereenkomst tot stand komt en er dus voor de klant een betalingsverplichting ontstaat. Het maakt in principe niet uit wat er aangeboden wordt, want de actoren zijn nimmer van plan een deugdelijke tegenprestatie te leveren. Na ontvangst van de eerste factuur realiseren de meeste klanten zich pas waarvoor ze hebben getekend.

Omvang

Het Steunpunt Acquisitiefraude (SAF) schat de schade van acquisitiefraude jaarlijks op €400 miljoen. Dit is gebaseerd op de mening van de initiatiefnemers van het SAF [SAFECIN, 2009]. Onderzoek van het Wetenschappelijk Onderzoek- en DocumentatieCentrum (WODC) dat zich richt op acquisitiefraude concludeert:

> "Omdat bij het onderzoek is uitgegaan van een beperkt aantal rekeningen (een selectie) en de bestudeerde periode per rekening verschilt, is het niet verantwoord om op basis van onze uitkomsten uitspraken te doen over de totale schade van acquisitiefraude" [Huisman & van de Bunt, 2009]

Ondanks dat de geschetste bedragen dus met enige voorzichtigheid benaderd moeten worden, heeft acquisitiefraude onbetwistbaar een grote financiële omvang en is het bovendien moeilijk aan te pakken. Er is immers sprake van een overeenkomst die de ondernemer zelf heeft ondertekend. Strafrechtelijke ontwikkelingen zijn gaande om tot betere instrumenten voor vervolging te komen [Initiatiefnota Acquisitiefraude, 2013].

De rol van ICT bij acquisitiefraude

ICT-ontwikkelingen bieden fraudeurs nieuwe instrumenten om acquisitiefraude te plegen. Met behulp van ICT is het eenvoudig om een grote groep potentiële slachtoffers in een keer te bereiken (*Mass Marketing Fraud*) en het is relatief eenvoudig om platforms te creëren met een officiële uitstraling die vertrouwd overkomen.

De rol van ICT bij de bestrijding van acquisitiefraude

Om acquisitiefraude tegen te gaan is er een online meldpunt opgericht vanwaar ondernemers hun cases kunnen deponeren en waaruit informatie wordt verspreid. De kamer van koophandel waarschuwt ondernemers door middel van nieuwsberichten voor bekende spookfacturen. De grootste uitdagingen bij het bestrijden van deze vorm van fraude zitten hem vooralsnog echter niet in de technologische mogelijkheden maar in de juridische instrumenten om deze fraudeurs aan te pakken.

Desalniettemin lijken wetenschappelijke ontwikkelingen om fraudedetectie te verbeteren in dit veld zeer gewenst. Het grote probleem bij acquisitiefraude is dat het zeer moeilijk is om frauduleuze facturen van werkelijke facturen te onderscheiden. Zeker voor de drukke ondernemer. Als er instrumenten kunnen worden ontwikkeld die ondernemers vooraf wijzen op een verhoogd risico op fraude bij bepaalde facturen dan zou dit een grote stap vooruit zijn. Ontwikkelingen rondom identificatie van fraude bij faillissementen en fraude bij jaarverslagen lijken een hoopvolle richting te bieden. Er is echter nog geen sprake van operationele activiteiten.

» BELASTINGFRAUDE

Definitie

Vanwege het gebrek van een algemeen geaccepteerde definitie gebruiken we hier de volgende omschrijving: het bewust verzwijgen of onjuist doorgeven van genoten inkomsten en/of eigendom, of het onterecht opvoeren van aftrekposten om zodoende een financieel voordeel te verkrijgen met betrekking tot het belastingstelsel.

In het verlengde van belastingfraude liggen weer andere fraudesoorten, zo kan bijvoorbeeld het opgeven van een onjuist inkomen leiden tot het onterecht ontvangen van uitkeringen.

Omvang

Er zijn geen openbare metingen over gedetecteerde of geschatte fraude met betrekking tot de inkomensbelasting. De meeste informatie kunnen we halen uit andere landen. In Groot-Brittannië is er een 'belastinggat' van 40 miljard pond per jaar. Zij zien 'slechts' 15 miljard hiervan als fraude. De resterende 25 miljard is in hun ogen niet aan te merken als opzettelijke fraude en wordt onder de noemer 'error' geplaatst [HMRC, 2011]. Dit is een conservatieve manier van schatten omdat de aanname dat een dusdanig groot belastinggat per abuis veroorzaakt zou zijn twijfelachtig is, maar wanneer we het uiterst conservatieve bedrag van 15 miljard pond extrapoleren aan de hand van het aantal volwassen inwoners in beide landen, dan komen we voor Nederland op een schatting van €4,4 miljard per jaar. Dit bedrag geeft op zijn best de ordegrootte aan, omdat de verschillen tussen beide landen niet verdisconteerd zijn heeft dat bedrag een grote onzekerheidsmarge.

Wanneer we kijken naar het inkomen in de 'verborgen economie'[8] geeft onderzoek aan dat dit in Nederland een jaarlijks bedrag van €58 miljard betreft [Schneider, 2010]. Wanneer hierop het gemiddelde percentage aan inkomstenbelasting en sociale verzekeringen van 39,1% wordt losgelaten, komt er een afgerond bedrag van €23 miljard[9] uit dat de staat elk jaar misloopt. Ook dit is weer een uiterst grove schatting omdat het onduidelijk is of de opbrengsten in de verborgen economie met name in de onderste, bovenste of middelste segmenten vallen of dat het representatief verdeeld is over de samenleving.

Het Europees Parlement geeft aan dat er in Europa maar liefst een triljoen (€1.000.000.000.000) euro per jaar verloren gaat aan belastingontduiking, oftewel €2.000 per inwoner.[10] Onder de aanname dat dit gemiddelde ook voor Nederlanders geldt, zou de belastingontduiking hier bijna €34 miljard euro zijn.[11] Wederom moeten we hier echter bij vermelden dat de gebruikte definitie van het Europese parlement niet duidelijk wordt verwoord en dat hun gebruikte methodes ook niet nader worden toegelicht, waardoor dit bedrag zeker met een korrel zout moet worden genomen.

Hoe dan ook, de omvang van belastingfraude is enorm. Deze bedragen zijn naar alle waarschijnlijkheid ruim voldoende om het jaarlijkse begrotingstekort volledig te vullen. Des te nijpender is het dat er vrijwel geen betrouwbare onderzoeksresultaten bestaan om tot nauwkeurige schattingen te komen. Positief is dat de staatssecretaris van Financiën de Tweede Kamer heeft beloofd om voor een deel van de belastingontvangsten, namelijk de btw, een berekening van de *tax gap*[12] te maken. Hierover is in 2014 een rapport verschenen [Ministerie van Financiën, 2014] waarin dit op basis van een macro-aanpak is gebeurd. Er wordt ook aangegeven dat deze methode mogelijk geschikt is

8 Het 'zwarte circuit', dienstverlening buiten de belasting om.

9 Gebaseerd op *Reformatorisch Dagblad*. 'Staat loopt 24 miljard mis door zwart werk', 20-12-2010.

10 Zie onder meer: http://www. europarl. europa. eu/news/en/news-room/content/20130527STO10562/html/A-taxing-problem-the-cost-of-failing-to-act-on-fiscal-evasion.

11 Gebaseerd op het gegeven dat Nederland in juli 2014 volgens het CBS 16.859.353 inwoners had, vermenigvuldigt met €2.000.

12 De tax gap is het verschil tussen het bedrag waar de Rijksoverheid recht op heeft als iedereen zich houdt aan de geldende wetgeving en het bedrag dat daadwerkelijk binnenkomt. De tax gap beslaat dus niet alleen fraude, maar ook bijvoorbeeld onjuist ingevulde aangiftes.

voor andere deelgebieden van belastingfraude.

De rol van ICT bij belastingfraude

Van oudsher speelt ICT geen fundamentele rol in belastingfraude. Veelal betreft het inkomen uit zwartwerk ('*beunhazen*') dat nergens op papier staat. Sinds enkele jaren zijn er wel ontwikkelingen gaande die van invloed zijn op belastingfraude. Zo is er tegenwoordig de 'vooringevulde aangifte'. Deze geeft particulieren de mogelijkheid om hun gegevens automatisch in te laten vullen vanuit verschillende databases. Dit heeft onder andere tot gevolg dat er een verminderd verantwoordelijkheidsgevoel is voor de juistheid van de gegevens. Mensen verwachten nauwkeurigheid van de overheid. Dit zorgt voor een verminderde controle en daardoor potentiële onnauwkeurigheden.

Daarnaast wordt de digitale aangifte verzonden via de DigiD-code. In 2011 bleek echter dat er mogelijk frauduleuze ssl-certificaten in omloop waren waardoor de veiligheid niet gegarandeerd kon worden.

De rol van ICT bij de bestrijding van belastingfraude

De detectie van belastingfraude is complex omdat het in plaats van op onjuiste gegevens, vaak berust op het *weglaten* van data. Daarentegen heeft de belastingdienst toegang tot een indrukwekkend aantal databases, waarmee zij complexe analyses kunnen uitvoeren.

Er zijn zeer interessante ontwikkelingen gaande waarbij opmerkelijke patronen uit verschillende databases met elkaar worden vergeleken. Denk hierbij aan personen met een zeer laag belastbaar inkomen, maar met meerdere auto's. Of mensen die hypotheekrente als aftrekpost opvoeren terwijl uit de *BasisRegistratie Personen* (BRP) blijkt dat er een ander gezin in de woning verblijft.[13] Profilering is belangrijk en de voordelen daarvan kunnen worden verbeterd indien gebruik gemaakt wordt van moderne mathematische technieken.

Belastingfraude is moeilijk op te sporen, maar met behulp van de massale hoeveelheid beschikbare data bestaat er goede hoop dat instrumenten gecreëerd kunnen worden die hier ondersteunend in kunnen zijn. Grote obstakels hierin zijn de bestaande wetgeving, ethische vraagstukken en huidige complexe structuur van het belastingstelsel.

13 Het kabinet heeft per december 2014 €13 miljoen beschikbaar gesteld om adresfraude tegen te gaan. Dit moet uiteindelijk €42 miljoen opleveren.

» BELEGGINGSFRAUDE

Definitie

Geld dat verkregen wordt door de belofte van hoge niet-haalbare rendementen. De illusie wordt gewekt dat deze rendementen behaald worden doordat zij betaald worden vanuit de inleg van nieuwe beleggers.

Omvang

De grootste internationale beleggingsfraudezaak ooit was die van Bernard Maddoff. De totale schade wordt geraamd op $65 miljard, waarvan $2 miljard uit Nederland. Beleggingsfraudezaken in Nederland zijn in de regel kleiner van omvang. Toch betreft het hier honderden miljoenen euro's schade per jaar. In onderzoek [Roest & Stijnen, 2009] wordt de jaarlijkse schade geschat op €750 miljoen per jaar.

De rol van ICT bij beleggingsfraude

Beleggingsfraude is een interessant voorbeeld van de invloed die ICT kan hebben op fraude. De instrumentele invloed betreft de mogelijkheden van ICT om derden te misleiden. Zo worden investeerders gelokt met de beloftes van goede rendementen tegen een laag risico. De rol van ICT hierin is voornamelijk dat de perceptie naar buiten toe veel sterker kan worden uitgedragen door middel van professionele websites en informatievoorziening.

Er is echter ook een zeer sterke fundamentele invloed van ICT, waardoor een compleet nieuwe vorm van fraude ontstaat. Deze wordt uitstekend beschreven in het boek *Flitshandel* [Lewis, 2014]. De schrijver omschrijft de wijze waarop obscure organisaties alle grondbeginselen waar beleggers op vertrouwen onderuit halen door een verbinding met de beurzen te creëren die net iets korter en daardoor sneller is. Dit minieme tijdsvoordeel zorgt voor een informatievoorsprong van milliseconden waarop speciaal ontworpen softwareprogramma's reageren door de beleggers letterlijk te snel af te zijn.

Voorbeeld: Er worden één kooporder en drie verkooporders geplaatst voor één aandeel door één handelaar. Door de invloed van de drie grote verkooporders daalt de prijs licht. Op dat moment wordt de kooporder verwerkt tegen de iets lagere prijs. Vrijwel direct daarna worden de drie verkooporders geannuleerd, waardoor de prijs weer stijgt naar het normale niveau.Dit alles gebeurt in de tijdsspanne van een milliseconde. Het gaat om kleine effecten die met het blote oog nauwelijks waarneembaar zijn, maar doordat de frequentie zo enorm hoog is, kan dit om enorme bedragen gaan.

De rol van ICT bij de bestrijding van beleggingsfraude

De rol van ICT bij het bestrijden van beleggingsfraude is in eerste instantie voornamelijk faciliterend. Het biedt mogelijkheden om (potentiële) beleggers bewust te maken van de risico's rondom beleggingen boven de vrijstellingsgrens (sinds 2012 ligt deze op €100.000), waarbij er wordt verondersteld dat de belegger voldoende vaardig en kundig is om zelf te kunnen inschatten of een belegging veilig is of niet. Prospecti worden getoetst door de AFM, maar dit is geen garantie. Ook hier geldt dat wetenschappelijke ontwikkelingen op het gebied van toetsing door toepassing van ICT in de toekomst een rol van betekenis kunnen spelen, met name in het creëren van risicoprofielen of het detecteren via mathematische modellen.

Het grootste gevaar bij beleggingsfraude zit hem in de sterke aantrekkingskracht van snel, risicoloos geld. Het belangrijkste signaal voor beleggers om op af te gaan is dat als het er te goed uit ziet om waar te zijn, het dat waarschijnlijk ook is. In deze situaties is extra waakzaamheid geboden.

De vorm van beleggingsfraude die in het voorbeeld wordt beschreven (*high-frequency trading* genoemd) kan vrijwel uitsluitend met ICT gedetecteerd worden. Hier is duidelijk te zien dat de toezichthouders sterk moeten blijven investeren in de laatste technologische ontwikkelingen om te kunnen reageren op de geavanceerde nieuwe modus operandi van fraudeurs.

» FAILLISSEMENTSFRAUDE

Definitie

Een opzettelijke handeling vóór of tijdens een faillissement waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging voor deze handeling ontstaat, waardoor een onrechtmatig voordeel wordt verkregen en faillissementsschuldeisers opzettelijk of culpoos kunnen worden benadeeld [Tromp, Snippe, Bieleman & de Bie, 2010].

Omvang

Uit onderzoek uit 2005 [Knegt et al., 2005] blijkt dat de geschatte maximale schade door faillissementsfraude op €1,5 miljard per jaar ligt. In de loop der jaren is dit bedrag door bewindslieden meermaals naar boven bijgesteld, tot circa €2 miljard. Toch is een fikse kanttekening hier op zijn plaats. Het betreft namelijk niet per definitie de schade die door fraude wordt veroorzaakt. Het betreft de omvang van de verliezen binnen faillissementen waar fraude een rol heeft gespeeld.

Een groot verschil. Wanneer een organisatie failliet gaat en besluit een gedeelte van de inboedel wederrechtelijk te verkopen, is er weliswaar sprake van fraude, maar het grootste deel van de schade komt voort uit het rechtelijke faillissement en niet uit de fraude. Dit is uiteraard anders in situaties waarbij een bedrijf bewust en opzettelijk wederrechtelijk failliet gaat. De gemiddelde schadelast per case is in dit laatste geval ook duidelijk hoger.

De rol van ICT binnen faillissementsfraude

Bij het plegen van faillissementsfraude spelen ICT-ontwikkelingen nauwelijks een rol.

De rol van ICT bij het bestrijden van faillissementsfraude

Het blijk mogelijk om door middel van risicodetectiemodellen met een hoge mate van zekerheid te kunnen voorspellen bij welke faillissementen fraude plaatsvindt. Zo bleek uit onderzoek dat de detectiegraad bijna met een factor tien kon worden verhoogd [Veldkamp & de Vries, 2008] en dat van een bepaald gedeelte van de faillissementen met een kans van 80% kon worden gesteld dat er sprake zou zijn van fraude [van Geldrop, 2011].

» IDENTITEITSFRAUDE

Definitie

Identiteitsfraude is het opzettelijk (en wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan [de Vries et al., 2007].

Omvang

Recent onderzoek [PWC, 2013] concludeert dat in 2012 meer dan 600.000 Nederlandse burgers slachtoffer zijn geweest van een vorm van identiteitsfraude. Niet alle slachtoffers ondervonden hierdoor financiële schade, maar bij diegenen waar dit wel het geval was (meer dan de helft), is het schadebedrag gemiddeld €600 per persoon, waardoor het totaalbedrag de €180 miljoen benadert. In 2008 was het gemiddelde schadebedrag zelfs boven de €3.500. De trend is dat het aantal personen dat met identiteitsdiefstal te maken krijgt aan het stijgen is, maar dat het gemiddelde schadebedrag per persoon aan het dalen is. Bij deze bedragen wordt enkel nog gekeken naar de schade van het directe slachtoffer. Veelal zijn derde bedrijven de indirecte slachtoffers van burgers doordat zij producten of diensten leveren die uiteindelijk niet vergoed worden. Ander onderzoek [Dynamics, 2012] komt overigens tot een significant hoger schadebedrag van gemiddeld €5.943 per persoon. Waar dit grote verschil hem in zit, is onduidelijk.

Rol van ICT bij identiteitsfraude

De ontwikkelingen in ICT spelen een erg grote rol bij identiteitsfraude. Op hoofdlijnen is het idee achter identiteitsfraude hetzelfde gebleven, maar de modus operandi is fundamenteel veranderd.

Waar in het verleden identiteitsfraude plaatsvond door *dumpster diving*, waarbij men letterlijk door afval ging om bonnetjes, afschriften en andere persoonlijke gegevens te bemachtigen, gebruiken fraudeurs tegenwoordig vrijwel uitsluitend digitale middelen om persoonlijke gegevens van derden te verkrijgen. Geen enkel digitaal instrument wordt hierbij geschuwd. Valse websites, phishing e-mails en telefoontjes, virussen, keyloggers, et cetera.

Doordat onze gegevens tegenwoordig in honderden databases terug te vinden zijn, is het slechts een kwestie van zoeken naar het meest kwetsbare systeem. Vaak is het mogelijk om met behaalde gegevens weer nieuwe informatie te verkrijgen over een persoon.

Rol van ICT bij de bestrijding van identiteitsfraude

Identiteitsfraude kan het best voorkomen worden vanuit een mix van gezond verstand en softwarematige hulpmiddelen. Zo weet iedereen dat het onverstandig is om hetzelfde wachtwoord voor verschillende websites te gebruiken, maar is het tegelijkertijd ondoenlijk om voor elke registratie een nieuw wachtwoord te bedenken en te onthouden. Hiervoor bestaan oplossingen in de vorm van programma's die unieke gecompliceerde wachtwoorden genereren en onthouden. De gebruiker hoeft slechts het master-wachtwoord te onthouden. Deze programma's worden nog niet breed gebruikt en niet iedereen is ermee bekend.

Ook het up-to-date houden van de gebruikte antivirussoftware en firewall hebben een groot effect op de digitale veiligheid.

Andere maatregelen zijn meer praktisch van aard. Bij een veelvoud aan activiteiten wordt bijvoorbeeld gevraagd om een kopie van het identiteitsbewijs mee te sturen. Dit is ten eerste vaak onnodig, maar ook zeer onveilig. Daarom is het verstandig om gevoelige informatie die niet relevant is, weg te laten uit de kopie. Hiervoor bestaan simpele pasjes die men over een identiteitsbewijs kan schuiven, waardoor relevante informatie zichtbaar blijft, maar gevoelige informatie verborgen wordt.

Wanneer er ondanks al deze maatregelen toch identiteitsfraude plaatsvindt, zit het slachtoffer met een serieus probleem. Systemen zijn niet berekend op dergelijke vormen van fraude en in de praktijk blijkt dat door de grote connectiviteit van vele databases het effect in allerlei systemen doorwerkt en nauwelijks om te keren is. De gevolgen kunnen jaren voortduren. Het Expertisecentrum Identiteitsfraude en Documenten (ECID) houdt zich bezig met de verbetering van deze procedures.

» FRAUDE MET INTERNETBANKIEREN

Definitie

Fraude met internetbankieren vindt plaats wanneer derden ongeoorloofd toegang tot de online bankomgeving van een persoon of organisatie verkrijgen en geldbedragen wederrechtelijk overmaken.

Omvang

De schade die ontstaat door internetbankieren is sinds 2008 bijgehouden door de Nederlandse Vereniging van Banken. Waar er in eerste instantie een sterke stijging plaatsvond, heeft een grote publieke bewustwordingscampagne in combinatie met nieuwe technische veiligheidsmaatregelen geleid tot een sterke daling van de schadeomvang. De bedragen die het betreft zijn te vinden in onderstaande tabel [Nederlandse Verenging van Banken, n.d.].

Jaar	Omvang schade
2008	€ 2.100.000
2009	€ 1.900.000
2010	€ 9.800.000
2011	€ 35.000.000
2012	€ 34.800.000
2013	€ 9.700.000

Gegeven de negatieve publieke belangstelling die de banken doormaken, is de vraag gerechtvaardigd of de sector met deze cijfers het achterste van de tong laat zien. Alles valt of staat immers bij de door deze sector gehanteerde definitie. Wij achten de gegevens echter voldoende indicatief.

Rol van ICT bij fraude met internetbankieren

Vanwege de aard van internetbankieren speelt ICT per definitie al een grote rol binnen dit fraudedomein.

De voornaamste wijze waarop fraude met internetbankieren plaatsvindt, is door middel van *phishing*. Phishing is een verzamelnaam van technieken die criminelen gebruiken om vertrouwelijke, persoonlijke gegevens, bijvoorbeeld inlogcodes, te bemachtigen om daarmee vervolgens te frauderen. Meestal gebeurt dat via ongevraagde

e-mails (spam) of door telefonisch contact waarbij gevraagd wordt om (inlog)codes [Ned. Ver. Van Banken, n.d.].

Iedereen kent de e-mails in gebrekkig Nederlands met een vage boodschap waarin wordt aangemoedigd om op een dubieuze link te klikken en vervolgens de inloggegevens in te voeren. Dat deze niet beantwoord moesten worden, was voor de meeste gebruikers direct duidelijk.

Tegenwoordig zijn deze e-mails echter nauwelijks van echt te onderscheiden. Taalgebruik, lay-out en logo's zijn immers snel nagemaakt. Om mensen tot ondoordacht handelen te bewegen wordt soms ook nog verwezen naar actuele ontwikkelingen die een snelle reactie vereisen.

Er zijn nu ook gevallen bekend van e-mails van de banken zelf die doorverwijzen naar websites van derden. Hierdoor is het voor gebruikers niet meer mogelijk om het onderscheid tussen een goed gemaakte vervalsing en een echte e-mail te zien. De oplossing zit hem erin om nooit via een link in de e-mail naar de website van de bank te gaan, maar om deze altijd zelf handmatig in te typen in de adresbalk.

Rol van ICT bij de bestrijding van fraude met internetbankieren

Ondanks de steeds geavanceerdere praktijken van fraudeurs zien we toch een sterke daling in de omvang van de schade. Dit heeft twee aanwijsbare oorzaken. Allereerst heeft de bankensector de laatste jaren sterk geïnvesteerd in een campagne om mensen bewust te maken van de gevaren van phishing.

Ten tweede zijn technologische obstakels opgeworpen om misbruik lastiger te maken. De twee-stap-authenticatie[14] bestaat al langer, maar is nog steeds een effectief middel om fraude tegen te gaan. Daarnaast heeft ook onlangs een bank de slimme stap gezet om het betalingsproces te scheiden van het overzicht. Nu kan de inlogcode niet meer gebruikt worden om een betaling te verrichten. Een gebruiker moet dus bewust kiezen voor de verificatiecode om te betalen. Dit maakt het voor fraudeurs die een gebruiker proberen te misleiden[15] een stuk moeilijker om geld te verplaatsen.

14 Twee-staps-authenticatie is een extra beveiliging. Naast het invoeren van een gebruikersnaam en wachtwoord moet een gebruiker nog een tweede code invoeren die vaak ter plekke wordt gecreëerd en die slechts korte tijd geldig is. Dit kan door middel van bijvoorbeeld een sms of een onafhankelijk apparaat.

15 Het misleiden van slachtoffers door middel van zogenaamde babbeltrucs wordt *social engineering* genoemd.

» SOCIALE FRAUDE

Definitie

Het opzettelijk geven van onjuiste informatie of het verzwijgen van informatie om onterecht aanspraak te maken op een sociale uitkering of om deze te behouden.

Sociale fraude is niet alleen ernstig vanwege de kosten die ermee gemoeid gaan, maar ook vanwege de aantasting van het sociale stelsel. Nederland heeft ervoor gekozen om te zorgen dat iedereen in ieder geval de minimale middelen heeft om voor zichzelf te zorgen. Door misbruik te maken van deze regelingen wordt het maatschappelijke draagvlak ervan aangetast. De goeden leiden onder de slechten.

Omvang

De gedetecteerde uitkeringsfraude in 2011 bedroeg 153 miljoen euro. Hiervan werd €64 miljoen gedetecteerd door het UWV, €22 miljoen door de SVB en €67 miljoen door gemeenten [Min. SZW, 2012]. Het gaat hier echter om gedetecteerde fraude en er is geen schatting over het totale fraudebedrag. Sindsdien zijn er meerdere pilots geweest om de detectiegraad te verhogen.[16] Resultaten zijn nog niet optimaal (voornamelijk wegens obstakels bij bestandskoppeling), maar bieden goede perspectieven voor verbetering.

In Groot Brittanië werd de omvang van fraude op een continue basis bijgehouden en bovendien was er sprake van een periodieke en grootschalige steekproef. De omvang van sociale fraude (*benefits fraud*) wordt daar geschat op €1,4 miljard (£1,2 miljard) oftewel 0,7% van alle uitkeringen [Department for Work and Pensions, 2012].

Zouden we dit percentage toepassen op de Nederlandse situatie dan levert dat gebaseerd op de €169 miljard aan uitkeringen in 2009 [CBS, 2009] een fraudeomvang van bijna €1,2 miljard op.

Zonder verder onderzoek valt niet te zeggen of het percentage van 0,7% in Nederland vergelijkbaar is, maar gezien de bijzonder goede fraudeprogramma's die in Groot-Brittannië met betrekking tot sociale fraude worden gehanteerd valt te verwachten dat het percentage zeker niet lager zal zijn.

Rol van ICT bij sociale fraude

Fraude met uitkeringen treedt onder andere op wanneer een fraudeur uitkeringen aanvraagt en ontvangt op andermans naam. Dit kan op naam van een bestaande derde zijn, maar ook op een fictieve rechtspersoon. Er is hier sprake van digitale identiteitsdiefstal (of identiteitscreatie).

Ook hier geldt dat de complexiteit van het systeem zorgt voor extra kwetsbaarheden. Controle vooraf is tijdrovend. Daardoor ontstaat er een spagaat tussen de noodzaak om vooraf een grondige controle te doen plaatsvinden en de wens om verzoeken snel en efficiënt af te handelen.

Rol van ICT bij de bestrijding van sociale fraude

Technologische ontwikkelingen bieden instrumenten aan ten behoeve van de detectie van sociale fraude. Door middel van datamining is aangetoond dat deze detectie vele malen effectiever kan worden uitgevoerd dan nu het geval is. Er zijn momenteel proeven gaande om te kijken in hoeverre deze instrumenten in de praktijk ingezet kunnen worden.

16 Zie o. a. *Bestandskoppeling bij fraudebestrijding* (2012) van het ministerie SZW.

» VERZEKERINGSFRAUDE

Definitie

Het plegen of trachten te plegen van valsheid in geschrifte, bedrog, benadeling van schuldeisers of rechthebbenden en/of verduistering, door bij de totstandkoming en/of bij de uitvoering van een overeenkomst van schade-, levens- of zorgverzekering, of bij een natura uitvaart-, hypotheek- of spaarkasproduct betrokken personen en organisaties, en gericht op het verkrijgen van een uitkering of prestatie waarop geen recht bestaat, of een verzekeringsdekking te verkrijgen onder valse voorwendsels [Verbond van Verzekeraars, 1998].

Verzekeringsfraude kan op een viertal manieren plaatsvinden:

- **majoreren**: het met opzet meer schade claimen dan daadwerkelijk is geleden;
- **fingeren**: doen alsof er schade is voorgevallen die onder de dekking valt;
- **ensceneren**: het opzettelijk veroorzaken van schade voor het krijgen van een uitkering;
- **niet voldoen aan de mededelingsplicht**: het aanvragen en/of sluiten van een verzekering op grond van het opzettelijk verstrekken van verkeerde of onvolledige informatie.

Omvang

Concrete cijfers ontbreken, maar op basis van schattingen wordt er jaarlijks ongeveer voor een miljard euro gefraudeerd bij verzekeraars. Uit onderzoek van het Verbond van Verzekeraars blijkt dat 12% van alle verzekerden (anoniem) aangeeft wel eens te frauderen. De pakkans van deze vorm van fraude is zeer laag. In 2006 schatte het Verbond van Verzekeraars deze op ongeveer 1% en zij formuleerden de ambitieuze doelstelling om deze met een factor 10 te verhogen. In hoeverre dit heeft geleid tot een verhoogde pakkans is echter nog niet duidelijk. Structureel onderzoek ontbreekt.

Rol van ICT bij verzekeringsfraude

Verzekeraars gebruiken de opkomst van smartphones, tablets en andere mobiele apparatuur om het declaratieproces te vereenvoudigen. Een nobele doelstelling, maar ook een potentiële verzwakking van het systeem. Door de toenemende digitalisering van het declaratieproces is het eenvoudiger om valse declaraties in te dienen. Het is immers makkelijker een digitaal bestand op een geloofwaardige wijze aan te passen dan een fysiek document. Dit effect lijkt echter gering te zijn, waardoor de invloed van ICT op verzekeringsfraude beperkt blijft.

De rol van ICT bij de bestrijding van verzekeringsfraude

Bij de bestrijding van verzekeringsfraude spelen de ontwikkelingen in ICT een grotere rol. Een bestaande maatregel is een database met een zwarte lijst van gepakte fraudeurs.

Een andere, complexere methode is het gebruiken van data-analyse-instrumenten. Voor vele gevallen van verzekeringsfraude zijn indicatoren te vinden. Hierdoor is het mogelijk instrumenten te ontwikkelingen die de cases eruit kunnen pikken waarbij de waarschijnlijkheid van fraude hoog is.

» ZORGFRAUDE

Definitie

Het opzettelijk overtreden van een wet, regel of voorwaarde, waardoor een onterecht voordeel (zoals vergoeding of dekking) wordt behaald. Fraudeurs in de zorg halen een onterecht financieel voordeel uit de Nederlandse gezondheidszorg [Zorgverzekeraars Nederland, n.d.]. Dit kan particulieren betreffen die valse declaraties naar hun verzekeraar versturen, maar ook zorgverleners die niet-uitgevoerde behandelingen in rekening brengen.

Omvang

In de afgelopen drie jaar hebben zorgverzekeraars in totaal ongeveer 18 miljoen euro aan fraude opgespoord.[17] Dit is slechts het topje van de ijsberg. Uit internationaal onderzoek komt naar voren dat 3% tot 10% van alle financiële middelen die in de zorg worden gestopt frauduleus wordt verwerkt [NHCAA, 2009]. Een extrapolatie zou voor Nederland leiden tot een bedrag van €2,8 tot €9,4 miljard aan schade per jaar. Ook hier geldt weer dat extrapolatie slechts leidt tot indicatieve cijfers. Door het gebrek aan betrouwbare informatie is het onmogelijk om met enige betrouwbaarheid tot stellingen te komen. Uit eigen onderzoek hebben ziekenhuizen en behandelcentra €276,7 miljoen aan onjuiste declaraties gevonden (waarbij men in het midden laat of dit fraude of vergissingen betreft) [NZA, 2014]. Duidelijk is in ieder geval dat het om enorme bedragen gaat.

Recentelijk is er een Expertisecentrum Zorgfraudebestrijding opgericht om dit tegen te gaan. Hierin werken onder andere de Nederlandse Zorgautoriteit, FIOD, Belastingdienst en het Openbaar Ministerie samen aan de aanpak van zorgfraude. Ook is er een programmaplan opgezet om fouten en fraude binnen de zorg verder aan te pakken [Min. VWS, 2015].

Rol van ICT bij zorgfraude

Het systeem waarbij er een interactie is tussen zorgverzekeraars, zorgverleners en zorgnemers (patiënten) is van nature al complex. De ICT-omgeving waarbinnen codes voor behandelingen worden opgegeven, versterkt dit proces verder.

Hierdoor ontstaat een zeer complex systeem dat veel kwetsbaarheden kent, met weinig transparantie en met financiële prikkels die misbruik faciliteren en stimuleren. Oftewel, de gehele wijze waarop de organisatie van de zorg is opgezet, brengt de beheersbaarheid in het geding. Dit systeem is mogelijk door ontwikkelingen in de ICT en daardoor speelt informatie- en communicatietechnologie een fundamentele rol bij de totstandkoming van fraude in de zorg.

Rol van ICT bij de bestrijding van zorgfraude

ICT is dus één van de oorzaken van de complexiteit en kwetsbaarheid van het zorgsysteem, maar daarnaast kan het ook gebruikt geworden om tot een effectievere anti-fraude aanpak te komen.

Eén van de grootste problemen zit hem op dit moment in het gebrek aan transparantie. Verzekeraars zien behandelingen binnenkomen, maar weten niet of deze ook echt uitgevoerd zijn. Patiënten krijgen geen duidelijk overzicht en moeten zich actief inspannen om hier zicht op te krijgen. Een oplossing waarbij de patiënt een overzicht krijgt van alle uitgevoerde handelingen in begrijpelijke bewoordingen met daaraan de kosten verbonden is een belangrijke stap voorwaarts. Geavanceerde patroonherkenning zal hier ook een belangrijke rol kunnen spelen. Uitvoering van dergelijke methodes vraagt gerichte kennisverwerving door de koepel van concurrerende organisaties.

Ook een vorm van het elektronische patiëntendossier kan een belangrijke rol spelen. Uiteraard zitten hier de bekende haken en ogen aan, zoals privacy en technische vraagstukken, maar de verwachte toename van de zorgkwaliteit tegen gereduceerde kosten is een wenkend perspectief.

Samenvattend: De rol van ICT

In dit hoofdstuk hebben we geprobeerd een indicatief overzicht te geven van fraude en de economische gevolgen ervan. We hebben ons met name gericht op de rol die ICT speelt. De geschatte hoogte van de bedragen in combinatie met

17 https://www.zn.nl/consumenteninfo/fraude-in-de-zorg/

marginale pakkansen zijn voor een belangrijk deel het gevolg van de mogelijkheden in de ICT.

De verschillende fraudedomeinen in ogenschouw nemend, zien we dat ICT bij het merendeel van de fraudes een belangrijke rol inneemt. Reden is dat fraudeurs dezelfde soorten fraude als vroeger uitvoeren, maar dan met behulp van ICT-instrumenten. Hierdoor is het aantal potentiële slachtoffers vrijwel grenzeloos en de zichtbaarheid van de fraudeur is nihil. Hier komt bij dat ICT een fundamentele verschuiving veroorzaakt in enkele van de terreinen die zojuist beschreven zijn, waardoor compleet nieuwe modi operandi ontstaan en systemen worden gecreëerd die randvoorwaarden voor fraude scheppen.

Langzaam maar zeker is er echter ook een verschuiving te zien in de energie en middelen die overheid en bedrijven stoppen in het toepassen van technologie om fraude tegen te gaan.

Met name bij fraudedetectie speelt informatietechnologie nu al een grote rol. In veel gevallen is het daardoor mogelijk de detectiegraad significant te verhogen. Op zichzelf is dat nog niet voldoende. Om optimaal gebruik te maken van de mogelijkheden die technologie biedt, moet de gehele keten van fraudebestrijding hierop ingericht worden. Nu zijn er nog verschillende praktische bezwaren, waardoor verbeterde detectie niet automatisch leidt tot minder fraude. Onder andere het gebrek aan voldoende capaciteit voor opsporing en vervolging, de wet- en regelgeving omtrent privacy, en het aantonen van opzet spelen een rol..

In de praktijk zien we daardoor dat er nu prioriteit wordt gegeven aan de vervolging van de grootste fraudes. Deze keuze is logisch, maar om een echte slag te slaan in de nationale fraudeproblematiek moet de volledige keten van fraudepreventie, -detectie en -bestrijding versterkt worden.

Dat begint bij preventie. Momenteel zien we dat het gebruik van ICT vrijwel zonder uitzondering leidt tot een toename in de complexiteit van systemen, en daarmee tot een toename in de kwetsbaarheid ervan. In veel gevallen zijn er echter mogelijkheden om ICT zo in te zetten dat systemen transparanter, simpeler en beter beheersbaar worden. Dit betekent echter dat er aan de voorkant investeringen nodig zijn terwijl het onduidelijk is waar de baten komen te liggen.

Na de preventie komt de detectie. Ontwikkelingen hierin volgen elkaar nu al razendsnel op. De middelen om grote hoeveelheden ongestructureerde data te analyseren (*big data*) zorgen voor allerlei initiatieven om fraude effectiever te detecteren, zoals het analyseren van sociale media en het scannen van jaarverslagen. Geavanceerde mathematische technieken vervullen hierbij een belangrijke rol.

Zo heeft ICT in samenwerking met geavanceerde analysemiddelen de potentie om zowel op het gebied van preventie als detectie een belangrijke rol te spelen. Daarmee is men er echter nog niet. Zo is bijvoorbeeld het aantonen van opzet vaak een struikelblok, maar simpele digitale middelen kunnen hier ingezet worden om bij onopzettelijke onjuistheden het bewustzijn daaromtrent te stimuleren.

Zo is in Groot-Brittannië een onschuldige brief vanuit de belastingdienst verzonden naar een groep mensen die met behulp van data-analyse-software als risicogroep was gekenmerkt. In deze brief werd medegedeeld dat er een onregelmatigheid was gevonden met daarbij de vraag om dit, indien nodig, zelf te corrigeren. Gebeurde dit niet dan kon er mogelijk nader onderzoek plaatsvinden. Het gevolg was dat het merendeel van de groep zelf al een aanpassing deed voordat verdere maatregelen noodzakelijk waren. Dit wordt 'nudging' genoemd.

Zo speelt technologie een grote rol in de keten rondom fraudebestrijding en zijn er nog vele verbeteringen mogelijk. Om tot werkelijk effectievere methodes te komen, is wel een omslag in het denken nodig. Fraude moet niet een probleem zijn dat men achteraf oplost wanneer het delict heeft plaatsgevonden. Ongeacht of het gaat om het belastingstelsel, een declaratiesysteem voor de zorg, of geavanceerde software; de focus moet liggen op transparantie en beheersbaarheid. Vanuit deze gedachte kunnen systemen worden ontworpen die effectief zijn en toch beheersbaar.

In dit hoofdstuk is een blik geworpen op de huidige situatie. Om tot een goede strategie te komen, moet er ook vooruit gekeken worden. Het volgende hoofdstuk geeft een schets weer van ontwikkelingen die in de toekomst belangrijk zullen zijn of kunnen gaan worden.

Bronnen

- CBS, Centraal Bureau voor Statistiek (2009). *Sociale bescherming kost 169 miljard euro*. Available from: http://www. cbs. nl/nl-NL/menu/themas/macro-economie/publicaties/artikelen/archief/2010/2010-3175-wm. htm.
- Department for Work and Pensions, (2012). *Fraud and Error in the Benefit System: 2011/2012 Estimates (Revised Edition) (Great Britain)*.
- Dynamics (2012) *ID Fraud Prevention Research*.
- Europees Parlement, *A taxing problem; the cost of failing to act on fiscal evaion room*.
- Gee, J, Button, M. (2015) *The financial Cost of Fraud*, PKF.
- Geldrop, AJ van (2011) *Indicators of Bankrupcy Fraud*. Universiteit Twente.
- Geldrop, A.J. van (2012) Fraude loont. STT.
- HM Revenue & Customs (2011). Measuring the Tax Gap, 2011.
- Huisman, K. and H.G. van de Bunt, (2009). *Misleidende handelspraktijken. Een onderzoek naar de aard, achtergronden en aanpak van acquisitiefraude in Nederland*, WODC, Rotterdam.
- *Initiatiefnota Acquisitiefraude* SP (2013). Initiatiefnota van de Leden Gesthuizen (SP) en van Oosten (VVD).
- Knegt, R., Beukelman, A.M., Popma, J.R., van Willigenburg, P. & Zaal I. (2005). *Fraude en misbruik bij faillissement: Een onderzoek naar hun aard en omvang en de mogelijkheden van bestrijding*. Amsterdam: Hugo Sinzheimer Instituut.
- Lewis, M. (2014) *Flitshandel*.
- Ministerie van Financiën, Directoraat-generaal Belastingdienst (2014) *Onderzoek naar macro-economische schatting van gemiste omzetbelasting (btw gap)*.
- Ministerie van Sociale Zaken en Werkgelegenheid (2012) *Bestandskoppeling bij fraudebestrijding.*
- Ministerie van Sociale Zaken en Werkgelegenheid (2012) *Integrale Rapportage Handhaving 2011*
- Ministerie van Volksgezondheid, Welzijn en Sport (2015)
- National Health Care Antifraud Association. (2009) *The Problem of Health Care Fraud.*
- Nederlandse Vereniging van Banken (n.d.) *Vragen en antwoorden: Fraude met internetbankieren en oprichting ECTF.*
- NZA (2014) *Voorkom declaratiefouten bij ziekenhuizen en behandelcentra.* http://www. nza. nl/publicaties/nieuws/NZa-voorkom-declaratiefouten-bij-ziekenhuizen-en-behandelcentra/
- PWC (2013) *2013-update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland'.*
- PWC (2014) *Naar een fraudebeeld Nederland: Inzicht in fraude draagt bij aan bewustwording en effectieve prioriteitsstelling in de aanpak.*
- Roest, F. & Stijnen, R. (2009). *Beleggen in gebakken lucht*. Functioneel Parket Openbaar Ministerie. SAFECIN (2009). Stichting Aanpak Financieel-Economische Criminaliteit in Nederland, Protocol. 2009.
- Schalke & Partners (2014) *Fraude kost Nederland jaarlijks 30 miljard. Aanpak loont.*
- Schneider, F. (2010). *The Shadow Economy in Europe.*
- Tromp, N., Snippe, J., Bieleman, B. (2010) *Preventieve maatregelen horizontale fraude*. WODC.
- Veldkamp, B.P., & De Vries, T. (2008). *Identification of Bankruptcy Fraud in Dutch Organizations*. In IADIS European Conf. Data Mining (pp. 63-66).
- Verbond van Verzekeraars (1998) *Fraudeprotocol.*
- Vries, Th. de, Tigchelaar, H, van der Linden, M, Hol, A.M. (2007). '*Identiteitsfraude: een afbaking, een internationale begripsvergelijking en analyse van nationale strafbepalingen'*. WODC: Den Haag.
- Zorgverzekeraars Nederland (n.d.) https://www. zn. nl/consumenteninfo/fraude-in-de-zorg

Kansen en risico's: de toekomst van fraude

Een publicatie van STT is niet compleet zonder vooruit te blikken. Technologische ontwikkelingen versnellen exponentieel en claims over hoe de wereld er over twintig jaar uitziet, zijn per definitie gebaseerd op assumpties en op onze (beperkte) fantasie. De toekomst voorspellen is dus onmogelijk, maar door grondige analyse en input van experts kunnen bepaalde ontwikkelingen wel verkend worden.

Verkenningen zijn echter niet zonder risico's. Zo sloeg de invloedrijke rapportage van de WRR *De komende vijfentwintig jaar* [WRR, 1977] op het punt van de invloed van informatietechnologie de plank nog behoorlijk mis, terwijl vrijwel op datzelfde moment de Franse sociologen Nora en Minc [Nora & Minc, 1978] de toekomstige effecten van de informatisering redelijk in kaart konden brengen. Bescheidenheid is geboden.

Ontwikkelingen rondom fraude en fraudebestrijding zijn bovendien inherent moeilijk te voorspellen. Fraudeurs zoeken kwetsbaarheden waar tijdens de ontwerpfase niet aan gedacht is. Daarom wagen we ons niet aan het voorspellen van concrete nieuwe fraudesoorten die de komende decennia kunnen opkomen. In plaats daarvan kijken we op een hoger abstractieniveau naar specifieke ontwikkelingen en beschrijven we de impact die deze op het veld kunnen hebben. Onze nadruk ligt daarbij op technologie, maar ook niet-technologische ontwikkelingen komen aan bod om zo tot een realistisch beeld te komen.

Naast het identificeren van relevante trends wordt er in dit hoofdstuk ook gekeken naar zogenaamde *game changers*. Disruptieve ontwikkelingen die niet per se een hoge waarschijnlijkheid hebben, maar die niet uit te sluiten zijn en die een schokeffect teweeg kunnen brengen.

De toekomst wordt verkend zonder waardeoordeel. Op de vraag of bijvoorbeeld een samenleving met minimale privacy maar met hoge veiligheid gewenst is, zullen wij geen antwoord geven. De geschetste beelden zijn wel bedoelt te inspireren en om deze discussies te faciliteren.

Trends en ontwikkelingen met impact op fraude en fraudebestrijding

Soms zien we bewegingen waarvan we met redelijke zekerheid durven te beweren dat ze de komende jaren zullen voortduren. We voelen ons zeker en het voelt dan logisch om de opties en gevolgen van een bepaalde ontwikkelingen te verkennen. Andere keren lijkt het vrijwel onmogelijk dat een bepaalde ontwikkeling zal plaatsvinden, maar zijn de potentiële gevolgen zo revolutionair dat deze de moeite van het verkennen toch meer dan waard zijn.

Hieronder vindt u een aantal ontwikkelingen die gaande zijn en die (potentieel) een sterke impact op fraude en fraudebestrijding hebben. Net als in het vorige hoofdstuk proberen we complexe fenomenen op een overzichtelijke wijze weer te geven. Daardoor is het onvermijdelijk dat er overlap ontstaat tussen de verschillende trends die we beschrijven.

» EXPONENTIËLE TOENAME VAN DATA

Waarschijnlijkheid: hoog	+
Invloed op fraude: hoog	+
Invloed op fraudebestrijding: hoog	+

De hoeveelheid bestaande data neemt razendsnel toe. Met name de hoeveelheid ongestructureerde data die we als privé persoon toevoegen, valt nauwelijks meer voor te stellen. De lijst met voorbeelden is ellenlang, maar ter illustratie:

- Elke twee dagen creëren we net zoveel data als de hoeveelheid data vanaf het begin der tijden tot en met 2003.[18]
- In 2003 produceerden we als globale samenleving 4.4 zetabytes (1 Zb=10^{21} byte). In 2020 zal

18 Op basis van de CEO van Google: Eric Schmidt bij de Lake Tahoe Techonomy Conference 2014.

dit 44Zb bedragen [EMC², 2014].
- Het 'Internet of Things' duidt op de tendens om vanuit steeds meer *items* data te verzamelen. Alles wordt met elkaar verbonden. Van koelkasten tot boerderijdieren[19] en van lasapparaat tot smartphone. Elk van deze verbindingen levert weer nieuwe data [De Vries, 2014].

Zowel fraudeurs als fraudebestrijders kunnen profiteren van de toenemende hoeveelheid informatie.

Voor fraudeurs betekent de toename van data dat het steeds eenvoudiger is om aan persoonlijke gegevens van derden te komen. Daarmee is het bijvoorbeeld een koud kunstje om een tweede, online identiteit te creëren. Met name vormen van identiteitsfraude zullen daarom naar verwachting in de (nabije) toekomst vaker voorkomen.

Op het gebied van fraudebestrijding biedt de enorme toename in data kansen. De laatste jaren is de term *big data* sterk in opmars. Kort gezegd, behelst dit het analyseren van grote hoeveelheden ongestructureerde data. Deze analyses kunnen zeer effectief ingezet worden bij de detectie van fraude.

Fraude is per definitie een afwijking van het normale proces, maar de moeilijkheid zit hem erin om deze afwijking te detecteren. Voor een groot deel heeft dit te maken met de menselijke beperkingen wanneer het aankomt op het zien van complexe verbanden met het blote oog. Onderzoek heeft al aangetoond dat de effectiviteit van fraudedetectie sterk verbeterd kan worden door geavanceerde wiskundige modellen op onder andere faillissementsfraude [van Geldrop, 2011; Veldkamp & de Vries, 2008] en zorgverzekeringsfraude. Met de toenemende connectiviteit van verschillende databronnen, de verbeterende kwaliteit van data-analyse-modellen en de groei van de hoeveelheid beschikbare data zullen de mogelijkheden voor effectieve fraudedetectie sterk toenemen.

19 Zo krijgen koeien bijvoorbeeld al chips die meten wat hun locatie is en wanneer zij voor het laatst gemolken zijn. De term 'Internet of Things' is dus eigenlijk al achterhaald door het 'Internet of Everything'. Er zijn zelfs al chips ingebracht bij patiënten in het kader van gezondheidsmetingen.

» AFNAME PRIVACY INDIVIDUEN EN ORGANISATIES

Waarschijnlijkheid: onzeker	**?**
Invloed op fraude: hoog	**+**
Invloed op fraudebestrijding: hoog	**+**

Gerelateerd aan de toename van de hoeveelheid data is de afname van individuele privacy. Met name sinds de opkomst van het internet is de mate waarin persoonlijke gegevens openbaar worden weergegeven sterk toegenomen. Misschien nog wel meer vanwege een tendens van gebruikers om alles openbaar te zetten dan vanuit onzorgvuldige beveiliging van officiële instanties. Waar het begon met statische profielen op bijvoorbeeld CU2.nl, zijn er tegenwoordig volledig interactieve sociale media die constant de locatie en activiteiten van gebruikers doorgeven.

Hoewel veel gebruikers een gevoel van anonimiteit ervaren wanneer zij online zijn, is het vaak mogelijk allerlei persoonlijke informatie over hen af te leiden uit hun online activiteiten. Alleen al bij Twitter kan met TweetGenie het geslacht en de leeftijd van Nederlandse Twitteraars voorspeld worden op basis van hun 200 meest recente tweets.[20] Dit is een veelbetekenend voorbeeld. Ontwikkelingen op het vlak van de-anonimisering gaan mogelijk veel verder. Anonieme data verzamelingen worden vergeleken met verzamelingen met bekende persoonsgegevens, waarna de anonieme gegevens weer aan personen gekoppeld kunnen worden.

Momenteel zijn er grofweg twee reacties te zien op deze afname van de privacy. Aan de ene kant staat de groep gebruikers die zich weinig zorgen maakt. Deze groep is zich ofwel onbewust van de hoeveelheid data over hen die online beschikbaar komt, of bekommert zich hier simpelweg niet om. Aan de andere kant is de groep die deze ontwikkeling wel zorgwekkend vindt. Deze tweede groep is vooralsnog een kleine minderheid, maar lijkt de afgelopen jaren groeiende te zijn.

20 Nguyen, D, R Gravel, D Trieschnigg and T Meder: *"How Old Do You Think I Am?": A Study of Language and Age in Twitter* at ICWSM 2013.

Het is moeilijk te voorspellen welke kant deze ontwikkeling op zal gaan. Hoewel er steeds vaker protesten te horen zijn over het misbruiken van persoonlijke gegevens vinden de alternatieve programma's die hier oplossingen voor bieden nog geen massale aftrek.

Voor fraudeurs is de verdere afname van privacy een geschenk. Hoe meer informatie over personen, organisaties, procedures, systemen, etc., hoe meer kansen er liggen. De groep mensen of organisaties die zo min mogelijk gegevens openbaar zet, zal minder snel het slachtoffer van fraude worden.

Wat betreft fraudebeheersing zijn de verbanden complexer. Hoewel er steeds meer data en informatie gegenereerd wordt, mogen lang niet al deze data gebruikt worden voor fraudebeheeringsdoelen. Privacywetgeving speelt hierin een beperkende rol. Er ontstaat daardoor een ongelijk speelveld omdat fraudeurs zich niet gebonden voelen aan wet- en regelgeving en gebruik kunnen en zullen maken van alle informatie die hun activiteiten ondersteunt, terwijl fraudebestrijders gebonden zijn aan de beperkingen die voor een formele organisatie gelden. Met het gebruik van data uit sociale media zou de detectie van bijvoorbeeld uitkeringsfraude in potentie sterk verbeterd kunnen worden.

» TOENAME COMPLEXITEIT VAN SYSTEMEN	
Waarschijnlijkheid: hoog	**+**
Invloed op fraude: hoog	**+**
Invloed op fraudebestrijding: neutraal	**±**

Naarmate systemen complexer worden, ontstaan er meer kwetsbaarheden. Dit is weliswaar geen wet van meden en perzen, maar wel een theorie die in zijn algemeenheid wordt onderschreven door de ondervraagde experts en de onderzochte literatuur [Kakareka, 2009]. Niet alleen technologische systemen worden kwetsbaarder naarmate zij complexer worden, maar ook systemen die vanwege andere redenen – zoals wet- en regelgeving, cultuur en een gebrek aan transparantie – complexer worden, ontkomen hier niet aan.

Systemen evolueren in de loop der tijd. Dit kan allerlei oorzaken hebben. Technologische vorderingen maken nieuwe toepassingen mogelijk; er ontstaat een roep om aanpassingen vanuit gebruikers[21] of bestaande gaten en kwetsbaarheden worden gedicht met aanvullingen ('patches') die weer extra complexiteit creëren.

Uiteindelijk komt er een moment waarop een systeem niet langer volledig beheersbaar is. Dan staat men voor een belangrijke keus. Gaat men door met het ad-hoc opsporen van kwetsbaarheden? Laat men een bepaalde mate van fraude toe vanuit een kosten-baten overweging? Of wordt er gekozen om het systeem volledig opnieuw te herontwerpen om zo vanuit de basis te werken aan een systeem dat weer beheersbaar is, met alle kosten van dien?

Ter illustratie twee voorbeelden. Hoe complexiteit zijn weerslag heeft op verschillende systemen.

Voorbeeld 1: Het belastingstelsel is opgezet met de intentie om een ieder een redelijke bijdrage aan de nutsvoorzieningen te laten leveren. De politieke keuze is gemaakt om een progressief stelsel te hanteren met oplopende tarieven voor hogere inkomens. Vanuit een maatschappelijke wens wordt er rekening gehouden met uitzonderingen. Bijvoorbeeld ziektekosten als aftrekpost, aandelen in maatschappelijke beleggingen, of kortingen vanwege een alleenstaand ouderschap. In de loop der jaren veranderen de externe omstandigheden (bijvoorbeeld de economie of de maatschappelijke wens om extra korting te geven aan rijders van een elektrische auto) en op basis van deze ontwikkelingen worden verdere aanpassingen gedaan. Uiteindelijk neemt de complexiteit van het stelsel zover toe dat de beheersbaarheid in het geding komt, en er excessen als de bulgarenfraude en de perikelen rondom de recente pgb-fraude kunnen optreden.

21 Gebruikers kunnen in dit geval individuen zijn, maar ook bijvoorbeeld de maatschappij als totaalgebruiker van het zorgverzekeringstelsel.

Voorbeeld 2: Een complex technologisch systeem met veel kwetsbaarheden is bijvoorbeeld het besturingssysteem van Windows. De versie die in 2007 uitkwam (Vista) had al meer dan 50 miljoen regels code.[22] Dit komt onder andere doordat elke nieuwe versie weer bovenop de oude wordt gebouwd. Hoewel het aantal regels code voor de laatste Windowsversie niet openbaar is, kunnen we er vanuit gaan dat deze op zijn minst niet veel lager zal liggen dan het aantal regels voor Vista. Dit is terug te zien in het aantal nieuwe kwetsbaarheden dat in 2013 is ontdekt. Alleen in het jaar 2013 zijn er voor alle Windowssystemen in totaal 625 kwetsbaarheden ontdekt en gerapporteerd [Florian, 2014].

Het herontwerpen van systemen vanaf het nulpunt is een kostbaar proces en veel organisaties zijn huiverig om dit te initiëren. De algemene trend is daarom dat bestaande systemen steeds complexer en moeilijker beheersbaar zullen worden en dat nieuwe aanbieders die alternatieve systemen ontwikkelen de sleutel bezitten om werkelijk beheersbare systemen te ontwikkelen. Hiervoor is het wel noodzakelijk dat het grote publiek actief prioriteit geeft aan veiligheid, privacy, en beheersbaarheid. Tot op heden lijkt de voorkeur voor gebruiksgemak nog altijd het gedrag te leiden, waardoor bedrijven niet de incentives hebben om sterk in te zetten op andere aspecten.

» PROFESSIONALISERING ILLEGALE NETWERKEN RONDOM CYBERCRIMINALITEIT

Waarschijnlijkheid: hoog +
Invloed op fraude: hoog +
Invloed op fraudebestrijding: hoog +

Cybercriminelen verschillen van *traditionele* criminelen omdat ze in het algemeen rationeler te werk gaan. Traditionele criminaliteit komt vaak voor bij probleemgroepen waar zaken als armoede, analfabetisme, verslaving en werkloosheid een grote rol spelen. We zien dat cybercrime vaak wordt gepleegd door technisch vaardige mensen uit arme landen, waarbij er sprake is van uitgebreide voorbereiding en waar minder uit impulsiviteit wordt gehandeld [Anderson, 2010].

Het gevolg is dat er professionele netwerken bestaan van cybercriminelen, waarbij taken onderverdeeld zijn op basis van expertise en vaardigheden. Daardoor ontstaan nieuwe *business models* onder de naam *Fraud as a Service* (*FaaS*) of *Cybercrime as a Service* (*CaaS*).[23] Deze netwerken zijn transnationaal en vallen vaak buiten Europese jurisdictie. Zo kan er relatief eenvoudig een derde persoon of organisatie worden ingeschakeld om *botnets*[24] te gebruiken, data te stelen, of voor *password cracking* [Europol, 2014]. Deze professionele netwerken zullen zich blijven ontwikkelen en zullen steeds eenvoudiger toegankelijk worden voor buitenstaanders.[25]

» ANONIMITEIT BETALINGSMIDDELEN

Waarschijnlijkheid: Onzeker ?
Invloed op fraude: Onzeker ?
Invloed op fraudebestrijding: Onzeker ?

Het betalingsverkeer zoals we dat nu kennen wordt gecoördineerd door banken en de overkoepelende organen daarvan. Hierdoor is er een relatief stabiel systeem ontstaan, waarbij grote schommelingen zeldzaam zijn en waarbij er een groot vertrouwen is dat betalingen goed verlopen. De afgelopen jaren hebben echter aangetoond dat het stelsel verre van perfect functioneert[26] en erg gevoelig is voor interne factoren. Mede als reactie hierop zijn alternatieve betalingsmethodes genaamd *cryptocurrencies* in populariteit gestegen. De bekendste variant hiervan is de *Bitcoin*, maar er bestaan er vele meer. Het betreft betalingsmethodes waarbij er geen

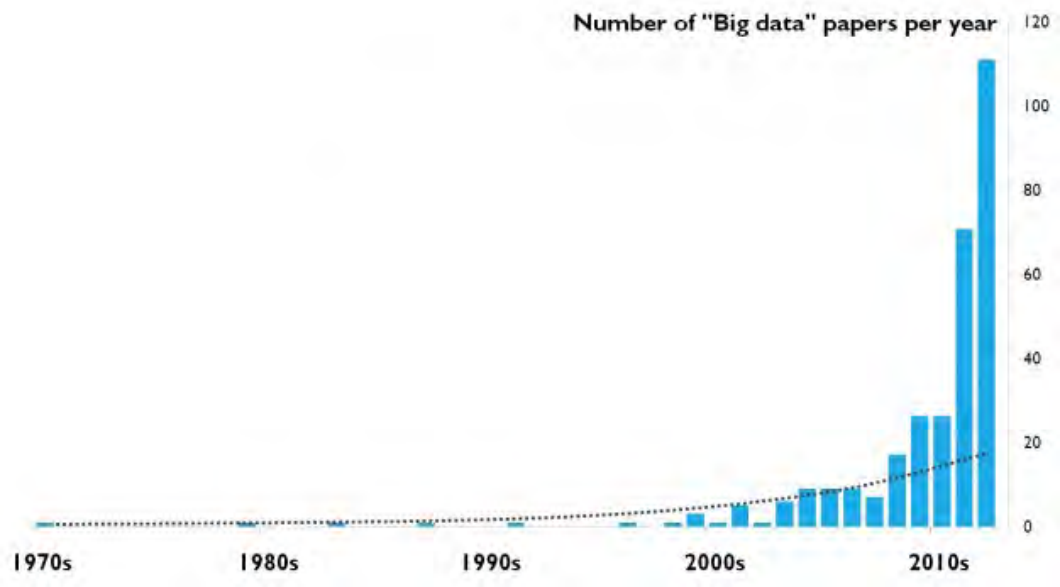
22 *Information is beautiful – Codebases: Million lines of code*. http://www.informationisbeautiful.net/visualizations/million-lines-of-code

23 Beide afkortingen zijn afgeleid van de maatschappelijk beter geïntegreerde term Software as a Service (SaaS).

24 Een collectie van aan elkaar gekoppelde computers die software gebruiken die meestal is geïnstalleerd door een computerworm, Trojaans paard, of achterdeurtje. Wordt in het algemeen ingezet voor illegale activiteiten.

25 Zo worden fraude-services al aangeboden via Facebook

26 Waarbij we o. a. doelen op de perikelen rondom de bankencrisis van 2008, waarbij banken die 'too big to fail' waren gered moesten worden door nationale overheden en waarbij enkele toch omvielen.



Big data growth [Halevi & Moed, 2012]

centraal coördinerend orgaan is. Het vermoeden bestaat dat dit vanwege de toegenomen anonimiteit extra mogelijkheden biedt aan fraudeurs voor bijvoorbeeld het witwassen van geld. Aan de andere kant is de technologie die fundamenteel is voor cryptocurrencies er juist op gespitst om zoveel mogelijk transparantie binnen het systeem te creëren [Rushman, 2014]. Het is nog onzeker of decentrale betalingsmiddelen een volwaardige plek in de maatschappij dan wel in de ondergronds netwerken zullen veroveren en veel zal afhangen van de stabiliteit die het systeem blijkt te hebben.

» EFFECTIEVERE METHODES OM INFORMATIE UIT ONGESTRUCTUREERDE DATA TE HALEN

Waarschijnlijkheid: zeer hoog	**++**
Invloed op fraude: laag	**–**
Invloed op fraudebestrijding: zeer hoog	**++**

Een zeer grote rol in toekomstige fraudebestrijding is weggelegd voor *big data*, oftewel het analyseren van enorme hoeveelheden ongestructureerde data. Zoals eerder betoogt, neemt de hoeveelheid data exponentieel toe. Echter is dit veelal data die niet netjes in tabellen wordt gestructureerd, maar betreft het vaak een chaos van (op het oog) willekeurige informatie die door een veelheid aan actoren op relatief arbitraire wijze wordt ingevoerd. Er kan dan gedacht worden aan data die in sociale netwerken wordt ingevoerd, data uit sensoren in diverse apparaten, data uit beveiligingscamera's en zo zijn er nog ontelbare voorbeelden te bedenken.

Big data hangt ten nauwste samen met *big data analytics*. Zonder deze hebben grote datahoeveelheden nauwelijks betekenis. Het aantal analysemethodes hiervoor is de laatste vijf jaar eveneens meer dan exponentieel gestegen (zie ook de grafiek hierboven voor de toename in de academische aandacht voor big data). Dat betekent dat kennis van die methodes van cruciaal belang is voor het vergaren van informatie uit big data. Moderne criminelen zijn zich hier van bewust en zullen flink investeren in dit soort kennis. Dat die kennis duur zal worden blijkt onder andere uit de te verwachten tekorten aan 'personeel met diep analytisch inzicht' in de VS: in 2018 worden tekorten van 140.000 tot 190.000 personen verwacht.[27]

27 Deze getallen komen voort uit het *McKinsey Global Institute Report 2011*. Uit gesprekken met verschillende experts blijkt dat deze cijfers inmiddels als conservatief worden gezien.

Vanuit *big data analytics* kunnen risicofactoren worden berekend. Eén van de mogelijke toepassingen van deze technologische ontwikkeling is het berekenen van risicomodellen van fraude.

Dit is niet zonder obstakels. Door de enorme complexiteit is het vaak niet mogelijk aan te geven *waarom* een bepaalde combinatie van factoren leidt tot een verhoogd risico op fraude. Er is dan sprake van een zogenaamde 'black box': er kan aangegeven worden welke cases een hoog risico op fraude hebben, maar niet *waarom* dit zo is. Deze onmogelijkheid hangt direct samen met de aard van de nieuwe analyse-instrumenten, waarbij er enkel wordt gezocht naar correlaties en niet naar causale verbanden.

Gamechangers

Naast de geschetste trends die we redelijkerwijs kunnen verwachten (met variërende mate van waarschijnlijkheid), zijn er ook echte gamechangers. Gebeurtenissen die we niet direct verwachten, maar die wel denkbaar zijn en die potentieel leiden tot een complete revolutie in de wijze waarop fraude en fraudebestrijding plaatsvindt.

» ENCRYPTIESYSTEMEN VAN DE BANKEN WORDEN GEHACKT

Op het moment dat bestaande encryptiesystemen niet langer veilige betaling kunnen garanderen ontstaat er een geheel nieuwe maatschappij. Zullen we alternatieven zoeken in de vorm van cryptocurrencies, volledig nieuwe betalingsmethodes ontwikkelen of verliezen we het vertrouwen in digitaal geld en gaan we op een andere wijze de samenleving in? Of staat ons nog compleet iets anders te wachten?

Het effect zal in ieder geval enorm zijn. Zonder veilige encryptiesystemen is er een grote kans op een zogenaamde *bank run*. Banken die failliet gaan, overheden die deze niet kunnen redden, burgers en bedrijven die al hun spaargeld kwijt zijn. Het verdwijnen van vertrouwen zou het hele systeem opblazen.

Het effect hiervan op fraude zal minstens evenredig groot zijn. In een wereld waar de beveiliging van transacties niet langer gegarandeerd kan worden hebben fraudeurs de vrije hand. Bovendien stimuleert een wereldbeeld met veel wanhoop en armoede fraude. Zowel omdat fraudeurs misbruik zullen maken van de situatie (schaarste beïnvloedt beslisprocessen op negatieve wijze en maakt mensen vatbaarder voor foute beslissingen [Mullainathan & Shafir, 2013]) en omdat er een omgeving wordt gecreëerd waarbij de potentiële opbrengsten van fraude aantrekkelijker worden ten opzichte van mogelijke risico's.

Voorbeeld: Voor beveiliging van transacties wordt wel een asymmetrisch encryptiesystemen gebruikt. Dit hangt op dit ogenblik samen met de bepaalbaarheid van twee priemgetallen uit een product ervan. Zolang het niet mogelijk is om dat binnen een kort tijdsbestek te bepalen is er niets aan de hand. Vanaf het moment dat dat wel mogelijk is, zullen er problemen ontstaan. Een dergelijke mogelijkheid lijkt niet direct waarschijnlijk, maar is niet uit te sluiten.[28] Voor andere systemen zoals McEliece zal dit ook gelden.

» GEEN LIMIETEN EN REGELGEVING OP DE ANALYSE EN MEETBAARHEID VAN DATA

Complexere systemen en de toenemende hoeveelheid data bieden zoals beschreven kansen voor geavanceerde data-analyse-instrumenten. Er ontstaan echter ook maatschappelijke vraagstukken die nog niet beantwoord zijn. Hoe zit het bijvoorbeeld met het eigenaarschap van data, de traceerbaarheid van data naar de oorspronkelijke bron, en de ethische vragen die spelen bij het *minen* van persoonlijke data. Met de toenemende koppeling van databases en het gebruik van de *cloud* is data bovendien vaak niet meer in een bepaald land te plaatsen. De vraag is dan of controle en regelgeving nog wel mogelijk is.

Fraudeurs zullen zich niet door deze vraagstukken laten vertragen. Instrumenten die analyseren welke doelwitten de hoogste opbrengst opleveren tegen het laagste risico zullen zonder aarzelen gebruikt worden.

28 Gesprek prof. dr H. Lenstra en prof dr ir T. de Vries (2013).

Het is niet ondenkbaar dat vanuit politieke motieven, met steun van de publieke opinie, privacy wordt opgeofferd voor veiligheid. Hoe valt er immers een strijd te winnen tegen cybercriminelen die niet belemmerd worden door regelgeving, als wij ons houden aan zelfopgelegde beperkingen? Privacy kan dan iets uit het verleden worden. Alles wat we doen levert data en deze is analyseerbaar voor iedereen. Hoe beïnvloedt dit onze manier van leven?

Dit klinkt misschien vergezocht, maar de huidige privacywetgeving is al ingehaald door technologische ontwikkelingen. Een nieuwe, Europese, richtlijn is al ontwikkeld en zal aanzienlijk beter en strenger zijn dan de huidige Nederlandse wetgeving. Verwacht wordt dat in 2017 deze wet van kracht wordt. Maar de vraag blijft of deze wetgeving adequaat zal zijn tegen de achtergrond van de technologische ontwikkelingen. Onder de maatschappelijke druk zal veel water bij de wijn moeten worden gedaan wat betreft rigiditeit tegenover toepasbaarheid. Hierover zal, naar verwacht, eerst nog intens gedebatteerd worden.

Bronnen

- Anderson, R. (2010) *In their words: Experts weigh in on Mac vs. PC security*. http://www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security
- Domenie, MLL, ER Leukfeldt, JA van Wilsem, J Jansen & WPh Stol (2013). *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma Uitgevers.
- EMC² Infobrief, *The Digital Universe of Opportunities*, 2014.
- European Cyber Security Perspective (2015).
- Europol (2014) *2014 Internet Organised Crime Threat Assessment.*
- Florian (2014) Report: *Most vulnerable operating systems and applications in 2013*; GFI.
- Geldrop, AJ van (2011*) Indicators of Bankrupcy Fraud*. Universiteit Twente.
- Halevi, G, & Moed, H. (2012). *The evolution of big data as a research and scientific topic: overview of the literature*. Research Trends, 30(1), 3-6.
- Jansen, J, ER Leukveld, J Jansen & WPh Stol (2013). 'Onlinegedragingen.' *Tijdschrift voor Criminologie*, 2013 (55) 4 pp 394-401.
- Kakareka, A. (2009). '23'. In Vacca, John. *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 393. ISBN 978-0-12-374354-1.
- *McKinsey Global Institute Report 2011*.
- Mullainathan, S & Shafir, E. (2013) *Scarcity: Why Having Too Little Means So Much. MacMillan.*
- Nora S en A Minc: *L'informatisation de la société,* Éditions du Seuil 1978 ISBN 2 02 00494 0.
- Rushman, J (2014) *Bitcoin, fraud and your health.* http://www. newbusiness.co. uk/%5Bvocab-raw%5D/bitcoin-fraud-and-your-health
- Veldkamp, BP, & de Vries, T. (2008) Identification of bankruptcy fraud in Dutch organizations IADIS European Conference Data Mining pp 63-66
- Vries T. de (2014), *ICT en privacy*, Liberaal Reveil dec.
- *WRR-rapport 15: 'De komende vijfentwintig jaar'. Een toekomstverkenning voor Nederland.* (1977) ISBN: 90 12 01948 6.

Toekomstbeelden

We hebben nu een aantal ontwikkelingen en gamechangers verkend. Om dit aansprekender te maken, zijn hier twee toekomstige wereldbeelden geschetst waarin enkele van deze ontwikkelingen hebben doorgezet.

» Toekomstbeeld 1

Het is 2035 en het bestrijden van fraude wordt wereldwijd erkend als één van de kernuitdagingen voor de komende twintig jaar. Door steeds slimmer gebruik van de mogelijkheden uit de informatietechnologie wisten fraudeurs het afgelopen decennium op massale schaal misbruik te maken van hiaten in de bestaande ordehandhaving. Illegale activiteiten werden uitgevoerd vanuit verschillende continenten en er is nooit overeenstemming bereikt tussen overheden over de eindverantwoordelijke hiervoor. Daardoor is echte actie altijd uitgebleven. Nu, onder massale druk van het publiek dat de apathie meer dan zat is, is er eindelijk een wereldwijde dienst ingesteld die grensoverschrijdend te werk gaat en die op zoek gaat naar oplossingen.

Nederland geldt op dit gebied als een voorbeeldland. In 2013 ontstond het eerste signaal dat fraude niet langer aanvaardbaar was in de *Rijksbrede aanpak fraude*. Hoewel dit document op zichzelf slechts een beperkt effect had, was dit het begin tot stevigere maatregelen.

Toen men in 2017 inzag dat men af moest van het ouderwetse denken over fraude werd de samenwerking met de High Tech Crime Unit van de politie geïntensiveerd. Zo werd Nederland het eerste land dat expliciet aandacht besteedde aan de nieuwste vormen van fraude. Al eerder was aangetoond dat digitale criminaliteit te weren is door te zorgen voor hogere pakkansen [European Cyber Security Perspectives, 2015]. Door de pakkans te verhogen, gingen criminelen op zoek naar andere locaties waar dit risico lager was.

Doordat de meeste andere landen achterbleven bij deze ontwikkelingen verdwenen veel fraudeurs naar het buitenland waar het voor hen beter toeven was. In 2020 kwam een volgende stap toen besloten werd de financiering van het zorgstelsel radicaal om te gooien. De prioriteit hierbij was het verbeteren van de kwaliteit van de zorg, maar vanaf het eerste moment is er ook ruime aandacht geschonken aan het beheersbaar maken van het nieuwe systeem.

Toen een aantal jaar later bleek dat de toename in beheersbaarheid zorgde voor een scherpe daling van misbruik, waarbij de baten voor de samenleving vele malen hoger bleken dan de gemaakte kosten werden er plannen gemaakt om ook andere systemen volledig te herzien. Er was nu immers aangetoond dat de baten hoger waren dan de kosten en de overheid was nu bereid hierin verantwoordelijkheid te nemen.

Nu is het 2035 en is Nederland samen met enkele landen het voorbeeld waar naar gestreefd wordt. Uiteraard vindt er nog steeds fraude plaats. Zowel impulsieve en traditionele fraude als innovatieve varianten die in 2015 nog niet denkbaar waren, maar doordat de beheersbaarheid evenals de transparantie sterk is vergroot en men zich veel beter bewust is van de gevaren zijn de verliezen marginaal ten opzichte van andere landen waar nooit concrete acties zijn ondernomen. Nederland kan oprecht zeggen dat fraude niet langer loont!

» Toekomstbeeld 2

De laatste tien jaar zien we een kentering in fraude in relatie tot ICT. Fraude is nu meer sophisticated en gesystematiseerd. Wat voorheen gelikt leek is thans kinderspel. Fraude wordt nu op bijna industriële schaal toegepast, criminele organisaties zijn actief.

"Brute force, social engineering, sophisticated malware – all these tools, and so many more are being applied every day to cracking various security systems. The criminal underworld is awash in credentials, which are being used to create accounts, take over accounts and commit fraudulent transactions".[29]

Gegevens in digitale systemen zijn niet langer veilig en de *cloud* is niet te vertrouwen. Het vertrouwen in de digitale omgeving is op een dieptepunt en niet meer herkenbaar ten opzichte van de situatie in 2015.

Een typische Amerikaanse overdrijving? Onwaarschijnlijk. Deze trend zal zich doorzetten in de komende vijf tot tien jaar. Belangrijk is hierin dat er steeds meer kennis beschikbaar is die gericht is op het de-anonimiseren van databases: de garantie van anonimiteit lijkt steeds moeilijker te geven.

Is de geschetste trend te mitigeren of zelfs te stoppen? We staan niet geheel met lege handen. Experts verwachten dat het toepassen van nieuwe analytische methodes en betere organisatie en beheer van dataverzamelingen een goede ontwikkeling zullen blijken. Verdachte patronen kunnen daarmee worden opgespoord en geïdentificeerd. Of dat voldoende is, is vooralsnog een open vraag. Zonder effectief ketenbeheer (opsporing, vervolging en veroordeling) zal het effect van nieuwe technieken suboptimaal zijn en blijven.

29 Eisen O. 'The future of fraud', *Wired* 2014.

Afsluiting

Bij de eerste publicatie van 'Fraude Loont' in 2012 was de primaire doelstelling om meer bewustwording rondom fraude te creëren. Uit de assessment die we nu voor de tweede maal hebben uitgevoerd blijkt dat er een positieve ontwikkeling gaande is. Zowel bij overheid, universiteit, bedrijfsleven als bevolking lijkt de afgelopen jaren het besef over de ernst van fraude gegroeid te zijn. De bereidheid tot samenwerking neemt daardoor toe.

Deze toename in bewustwording komt met name tot uiting in een aantal veelbelovende initiatieven, waarbij de *Rijksbrede aanpak fraude* er zoals gezegd uitspringt. Maar ook buiten de overheid zijn sectorgewijze aanzetten gesignaleerd en naar aanleiding van de conferentie van 20 januari 2012 is er zelfs een 'Dutch Fraud Initiative'[30] geïnitieerd, bedoeld om de ontwikkeling en deling van nieuwe kennis te stimuleren. Deze initiatieven zijn bittere noodzaak omdat fraudeurs zich blijken te organiseren en steeds professioneler en vindingrijker worden. Effectievere deling van methoden en technieken is daarom cruciaal.

Er zijn echter ook kanttekeningen. De veelbelovende initiatieven moeten uiteindelijk leiden tot concrete resultaten. Een belangrijke handicap daarbij is het ontbreken van een nulmeting die als referentie kan dienen. Een periodieke assessment die betrouwbare informatie over de omvang, het slachtofferschap en de modus operandi aanlevert, is hiervoor bittere noodzaak. Bovendien kan hierin aandacht worden geschonken aan de laatste innovatieve ontwikkelingen op het gebied van fraude en fraudebestrijding. Een integrale strategie die geen rekening houdt met deze ontwikkelingen zal nooit duurzaam kunnen zijn.

Kortom, er zijn goede stappen gezet, maar verdere actie is zeker nodig. De komende jaren zullen aantonen of de genomen maatregelen slechts symbolisch zijn of dat zij echt zullen leiden tot een effectievere aanpak van de fraudeproblematiek.

Het bijeenbrengen van kennis en ervaring is in ieder geval de eerste noodzakelijke voorwaarde om fraude niet langer te laten lonen.

Dankwoord

Voor de totstandkoming van dit boekje zijn ontelbare documenten gelezen en is er gecommuniceerd met een breed scala aan experts. De belangrijkste literatuur vindt u terug in de bronvermeldingen. Via deze weg willen wij de volgende mensen nogmaals bedanken voor hun waardevolle tijd en ideeën.

Edward Nkune (voormalig director of knowledge van het National Fraud Authority), Elmer Lastdrager (Universiteit Twente), Fred Noordam (Cisco), Janine Hoogendoorn (AFM), Frans Roest (Openbaar Minsterie), Jeannine de la Bursi (Ministerie van Economische Zaken), Joris Hulstijn (TU Delft), Marc Schuuring (Nationale Politie), Marianne Junger (Universiteit Twente), Marijn Janssen (TU Delft), Maurice van Keulen (Universiteit Twente), Paul-Willem van Gerwen (AFM), Perjan Moors (VVD), Ruud Hardenbol (TNO), Stan Hegt (KPMG), Tore ter Horst (Alliander), Anoniem (SIDN).

30 Gehuisvest bij de Universiteit Twente.

Over Universiteit Twente

Universiteit Twente. De plek waar talent zich het best ontplooit. Studenten en medewerkers staan centraal. 2.900 wetenschappers en professionals zorgen samen voor baanbrekend onderzoek, relevante innovatie en inspirerend onderwijs voor meer dan 9.000 studenten. Ondernemerschap zit in onze genen. Op de campus zijn zo'n 100 (student)-bedrijven gevestigd. Daarnaast heeft Universiteit Twente al meer dan 800 succesvolle spin-off-bedrijven voortgebracht! Kennispark Twente stimuleert en faciliteert startende ondernemers. Op onze prachtige, groene campus gebeurt echter veel meer. De faciliteiten voor sport en cultuur zijn uniek en met evenementen als 's werelds grootste denktank Create Tomorrow en het grootste studentensportevenement de Batavierenrace is de campus een begrip. De campus inspireert en bruist!

Universiteit Twente, de ondernemende universiteit.

Postadres
Postbus 217
7500 AE Enschede

Bezoekadres
Drienerlolaan 5
7522 NB Enschede

info@utwente.nl
www.utwente.nl
053 489 9111

Over STT

De Stichting Toekomstbeeld der Techniek (STT) organiseert al meer dan 45 jaar brede, participatieve toekomstverkenningen op het snijvlak van technologie en samenleving. De stichting biedt enthousiaste belanghebbenden een vrije ruimte om elkaar te ontmoeten en op creatieve wijze inspirerende toekomstbeelden te bouwen.

De onderwerpen voor de toekomstverkenningen worden geselecteerd uit een rolling agenda met thema's. Die agenda wordt voornamelijk gevoed door voorstellen van leden van het Algemeen Bestuur van STT en door de STT Horizonscan. Dat laatste is een explorerende verkenning, breder dan de andere STT-verkenningen. Zij schetst vanuit een langetermijnperspectief een domein-overstijgend en interdisciplinair beeld van mogelijke ontwikkelingen, kansen en bedreigingen, *weak* en *strong signals* en de verbindingen daartussen.

De stichting heeft in de afgelopen decennia mooie resultaten bereikt. Het gaat bij de resultaten niet alleen om bijdragen aan visievorming, beleidsontwikkeling of *risk assessment* en agenda's voor de toekomst. Uit de toekomstverkenningen zijn bijvoorbeeld ook onderzoeksprogramma's en netwerken voortgekomen.

Het Algemeen Bestuur van STT bestaat uit ruim zestig personen uit de top van de overheid, het bedrijfsleven, de onderzoekswereld en de maatschappij. STT is een non-profitorganisatie. De activiteiten worden gefinancierd via bijdragen van overheid en bedrijfsleven.

Informatie over STT, haar activiteiten en haar producten is te vinden op de website www.stt.nl

Postadres
Postbus 30424
2500 GK Den Haag

Bezoekadres
Prinsessegracht 23
2514 AP Den Haag

info@stt.nl
www.stt.nl
070-3029830

UNIVERSITEIT TWENTE.

Stichting Toekomstbeeld der Techniek

Samenstelling bestuur STT

per maart 2015

Ir. R. Willems, **voorzitter**, Voormalig President-directeur Shell Nederland
Ir. C.C.J. Vincent MBA, **vicevoorzitter**, Managing partner PwC Consulting Indonesia, COO PwC South East Asia Consulting
Mevr. dr. ir. N. Buitelaar MBA, **secretaris**, Chief Business Officer, BiosanaPharma
Ir. J.H.J. Mengelers, **penningmeester**, Voorzitter College van Bestuur TU Eindhoven
Drs. M. Remerie, **lid DB**, Voormalig directeur Business Development Siemens Nederland
Prof. dr. E.H.L. Aarts, Decaan faculteit Wiskunde & Informatica, Hoogleraar TU Eindhoven
Drs. ir. J. van den Arend Schmidt, CEO Capgemini Consulting Nederland
H. Blokhuis, CTO & Director for Collaboration & Video, Cisco
Jhr. ing. M. Boreel, CTO Sogeti Group
Drs. J. van Breukelen, Voormalig Voorzitter Raad van Bestuur KPMG
Dr. E.E.W. Bruins, Directeur Technologiestichting STW
Dr. K.H. Chang, Voormalig Algemeen Directeur Koninklijke Nederlandse Akademie van Wetenschappen (KNAW)
Drs. Ch. Evers, Lid Raad van Bestuur en CFO Atrium Orbis Medisch Centrum en Zorgconcern
Ir. J.P. Fontijne MBA, Executive Vice President Power TIC, DNV GL - Energy
Ir. B.C. Fortuyn, Lid Raad van Bestuur van Siemens Nederland NV
Mevr. prof. dr. V.A.J. Frissen, Hoogleraar ICT en Sociale Verandering Erasmus Universiteit; directeur Stichting SIDN Fonds
Ir. J.F.M.E. Geelen, Senior Vice President R&D Océ-Technologies BV
Drs. J.H. de Groene, Algemeen Directeur Nederlandse Organisatie voor Wetenschappelijk Onderzoek
Dr. B. ter Haar, Directeur-generaal Participatie en Inkomenswaarborg ministerie van SZW
Drs. F.P.U. Haffmans, Head of Corporate Coverage Benelux, Country Executive Bank of America Merill Lynch The Netherlands
F. Herrebout, Senior Strategy Manager T-Mobile
Drs. A.J. van den Hoogen, Director R&D Products and Applications, Tata Steel Research, Development & Technology
Dr. H. van Houten, Executive Vice President, Philips Research
Ir. E.H.M. Hoving, CTO KPN Group
Ir. C.M. Jaski, CEO Grontmij
Dr. ir. C.P. Jongenburger, CTO & Lid van Raad van Bestuur Wuppermann Staal Nederland
Dr. T. Jongsma, Directeur Stichting Public Private Partnership Institute for Sustainable Process Technology (ISPT)
Mevr. dr. M.J. Jonkman, Corporate director R&D Koninklijke FrieslandCampina
Prof. dr. ir. J.T.F. Keurentjes, CSO, lid Raad van Bestuur TNO
Ir. P.A.O.G. Korting, CEO ECN
Ir. G.A. Kroon, Algemeen directeur ARCADIS Nederland
Dr. B. Leeftink (waarnemer), Directeur-generaal Bedrijfsleven en Innovatie, Ministerie van Economische Zaken
Mevr. drs. E.P.J. Lemkes-Straver, Algemeen Directeur ZLTO
Mevr. ir. M. van Lier Lels, Lid Raad van Commissarissen Reed Elsevier, Imtech en Eneco; diverse bestuursfuncties
Mevr. drs. M. Mettes, Directeur Innovatie RWE/ Essent
Ir. P.C. Molengraaf MBA, Voorzitter Raad van Bestuur Alliander
P.W. Mollema MSc, Director Environmental Management, Port of Rotterdam Authority
Mevr. prof. mr. A. Oskamp, Rector magnificus van het College van Bestuur van de Open Universiteit
Ing. M.C.J. van Pernis, President KIVI
Mevr. dr. J.W.A. Ridder-Numan (waarnemer),

Plv. hoofd Wetenschapsgebieden, directie OWB, Ministerie van OCW
Ir. P. van Riel, CEO Fugro
Ir. P.W.F. Rutten MBA, Partner McKinsey and Company
Mevr. drs. J.H. Scholten, Directeur VSNU
Ir. Y. Sebregts, Executive Vice President Innovation, R&D, CTO Projects & Technology Royal Dutch Shell
Mevr. ir. C.M. Sluis, Algemeen directeur Witteveen+Bos Raadgevende ingenieurs BV
Drs. ing. G.E.A. Smit, CTO IBM Benelux, IBM Distinguished Engineer
F. E. Smith, Director Public Affairs, ANWB
Dr. J.M.A. Verbakel, Vice President Global R&D Operations Unilever
Prof. dr. M. Verkerk, Bestuurslid VitaValley, Bijzonder hoogleraar Christelijke Wijsbegeerte TU/e
Mevr. prof. dr. ir. M.P.C. Weijnen, Hoogleraar TU Delft, faculteit Techniek, Bestuur en Management, lid WRR
Mevr. mr. J.S. van der Woude, Company Secretary and Legal Director Continental Europe, Reed Elsevier NV
Dr. M. Wubbolts, CTO Royal DSM
Drs. R. Zandbergen, CEO USG People
Prof. dr. A.N. van der Zande, Directeur-Generaal Rijksinstituut voor Volksgezondheid en Milieu (RIVM)

Adviserende leden uit de STT-Academy

STT hoogleraren

Prof. dr. ir. M.F.W.H.A. Janssen, TU Delft: ICT en Governance
Prof. dr. ir. V.A.W.J. Marchau, Radboud Universiteit: onzekerheid en adaptiviteit van maatschappelijke systemen
Mevr. prof. dr. M.H. Martens, Universiteit Twente: Intelligent Transport Systems (ITS) en Human Factors
Prof. dr. W.J. de Ridder, Universiteit Twente: toekomstonderzoek
Prof.dr.ir. T. de Vries, Universiteit Twente: ICT en gezondheidszorg, ICT en fraude, data-analytics

Research fellow

Dr. P. van der Duin, TU Delft: methodiek van verkenningen en innovatie; Lector Futures Research & Trendwatching bij Fontys Academy for Creative Industries

Directeur bureau

Drs. P. Morin

STT-publicaties sinds 2005

STT 81 Van Autonome robots tot Zilte aardappels; Een toekomstverkenning naar de invloed van technologische otwikkelingen op de agri- & foodsector tot 2050
Silke de Wilde, 2015 (ISBN 978 94 91397 09)7
STT 80 Horizonscan 2050, Anders kijken naar de toekomst
Jacintha Scheerder, Rene Hoogerwerf, Silke de Wilde, 2014
(ISBN 978 94 91397 07 3)
STT 79 Aspirine op je brood. Voeding en geneesmiddelen in de toekomst
Ellen Willemse, 2013 (ISBN 978 94 91397 05 9)
STT 78 Het vervoer van morgen begint vandaag. (Ver)voer tot nadenken en doen Marie-Pauline van Voorst tot Voorst en Rene Hoogerwerf, 2013
(ISBN 978 94 91397 06 6)
STT 77 Samen Slimmer. Hoe de 'wisdom of crowds' onze samenleving zal veranderen
Redactie: Maurits Kreijveld (2012) (ISBN 978 94913970 2 8)
STT 76 Serious Gaming (serie van 3 publicaties).
Serious Gaming: Vergezichten op de mogelijkheden
Play On: Serious Gaming voor de nieuwe generatie senioren
Serious Games, Playful Business: Toekomstbeelden van de spelende organisatie
Jacco van Uden, 2011 (ISBN 978 90 809613 0 2)
STT 75 Futures of Technology in Africa
Jasper Grosskurth (2010) (ISBN 978 90 809613 7 1)
STT 74 Bargaining Norms – Arguing Standards
Edited by Judith Schueler, Andreas Fickers, Anique Hommels, 2008 (ISBN 978 90 809613 4 0)
STT 73 Brain Visions. How the Brain Sciences. Could Change the Way We Eat, Learn, Communicate and Judge
Edited by Ira van Keulen (2008)(ISBN 978 90 809613 6 4)
STT 72 Deus et Machina. De verwevenheid van technologie en religie
Redactie: Michiel D.J. van Well, 2008 (ISBN 978 90 809613 5 7)
STT 71 Converging Technologies: Innovation patterns and impacts on society
Edited by Maurits Doorn, 2006 (ISBN 978 90 809613 3 3)
STT 70 Genomics 2030: Part of Everyday Life
Edited by Mark de Graef, 2005 (ISBN 978 90 809613 2 6)
STT 69 Techniek als menselijk ontwerp; nieuwe opleidings- en loopbaanroutes voor jongeren
Redactie: Dr. ir. Remke M. Bras-Klapwijk, 2005 (ISBN 90 809613 1 0)

FRAUDE LOONT...
nog steeds

QUICK SCAN

Miljarden euro's aan schade, lage pakkansen, hoge criminele opbrengsten en dramatische gevolgen voor zowel individuele slachtoffers als de samenleving als geheel. De ernst van de omvang en consequenties van fraude werden al eerder benoemd in de eerste quick scan *Fraude Loont* uit 2012.

In die publicatie werd voor het eerst een blik geworpen op de huidige en toekomstige rol van ICT binnen verschillende fraudes en hoe deze zorgt voor nieuwe fraude-instrumenten en zelfs voor compleet nieuwe fraudesoorten. Daarentegen biedt diezelfde ICT ook enorme kansen voor overheid en bedrijfsleven door de ontwikkeling van steeds effectievere methodes voor fraudedetectie.

De invloed van ICT op fraude en fraudebestrijding zal blijven groeien en een gerichte aanpak is noodzakelijk. De laatste jaren zijn een aantal veelbelovende initiatieven opgezet om deze uitdaging aan te gaan. Het is echter de vraag in hoeverre deze initiatieven inspelen op de invloed van voortdurende technologische ontwikkelingen. Kunnen we de aanpak van fraude toekomstbestendig maken?

In *Fraude Loont… nog steeds* bestuderen we de ontwikkelingen per sector en identificeren we belangrijke trends. Samen willen we met alle stakeholders een discussie daarover aangaan, zodat er bij een volgende editie van deze publicatie een andere titel gehanteerd kan worden.

ISBN 978-94-91397-10-3

Stichting Toekomstbeeld der Techniek

UNIVERSITEIT TWENTE.