QUICK SCAN

FRAUDE LOONT

De toekomst van fraude en ICT

Alex van Geldrop, BSc
prof.dr.ir. Theo de Vries

Stichting Toekomstbeeld der Techniek

UNIVERSITEIT TWENTE.

QUICK SCAN

FRAUDE LOONT

De toekomst van fraude en ICT

INHOUDSOPGAVE

SAMENVATTING

De totale schade die door fraude wordt veroorzaakt is onbekend, maar loopt in de vele miljarden euro's. De rol van ICT hierin is enorm. Het gebruik van ICT is de onderliggende oorzaak van een aantal fraudesoorten en het biedt instrumenten aan die fraudeurs gebruiken. In een reactie op de schade die wordt geleden is te zien dat allerlei sectoren onafhankelijk van elkaar plannen maken en uitvoeren om de fraude in de eigen sector te beteugelen. Elke sector ontwikkelt zijn eigen informatiesystemen en 'best practices' om dit te bewerkstelligen.

Deze groeiende aandacht voor fraudebestrijding kan alleen maar toegejuicht worden. Gerichte investeringen die nu worden gedaan, zullen zichzelf op de lange termijn dubbel en dwars terugverdienen. Wel lijkt er een gebrek aan coördinatie te zijn tussen de verschillende sectoren. Ieder is bezig om fraudebeheersing in het eigen beperkte vakgebied te optimaliseren. Dit heeft tot gevolg dat veel tijd en middelen worden gestoken in onderwerpen die andere sectoren al uitgezocht hebben. Een samenwerking tussen deze sectoren leidt tot een uitwisseling van kennis. Het delen van ervaringen zorgt voor een win-winsituatie voor alle betrokken partijen.

Cybercriminelen hebben bewezen in staat te zijn om uiterst gecompliceerde en geavanceerde manieren te vinden om gegevens te bemachtigen. De verwachting is dat e-fraude zich alleen maar verder zal ontwikkelen. Dit zal gebeuren op nieuwe platforms zoals de smartphone, maar ook door huidige technieken te perfectioneren. In plaats van af te wachten en pas te reageren bij geslaagde online inbraken moet geprobeerd worden om producten dusdanig te ontwikkelen dat ze veilig genoeg zijn om niet langer een aantrekkelijke prooi te zijn voor fraudeurs. Absolute veiligheid kan nooit gegarandeerd worden, maar door voorop te lopen met veiligheidsmaatregelen wordt ervoor gezorgd dat fraudeurs zich minder zullen richten op deze producten.

Om dit voor elkaar te krijgen moet er een omslag in het denken plaatsvinden. ICT-systemen moeten minder complex worden. Het fraudebewustzijn van alle belanghebbende partijen moet stijgen. Zowel van de overheid, als van bedrijven, als van burgers. Als een van deze partijen niet zorgt voor voldoende veiligheidsmaatregelen, kan het hele systeem kwetsbaar worden.

In andere landen zien we een tendens waarbij een centrale partij de coördinatie verzorgt en samenwerking stimuleert. Deze samenwerking zorgt vervolgens ook weer voor een stijgend fraudebewustzijn en heeft zo een dubbelfunctie.

De vraag die we in Nederland nu moeten stellen is hoe we de verschillende initiatieven van een aantal sectoren zo effectief mogelijk kunnen benutten. Een verregaande samenwerking tussen de betrokken sectoren en onafhankelijke gespecialiseerde bedrijven met een overheid die een coördinerende rol heeft, lijkt hiervoor de meest optimale oplossing.

SUMMARY

The exact amount of damage that is caused by fraud is unknown but runs into billions of euros per year. The role that IT plays within this is enormous. The use of IT is either a direct cause of certain types of fraud or IT offers a range of instruments that fraudsters use. In response to the sustained damage sectors are independently of one another constructing and executing plans. Every sector develops its own 'best practices' to battle fraud.

The growing emphasis on fraud control can only be welcomed. Directed investments will repay themselves twice over in the long run. However, there seems to be a lack of coordination between the various sectors. All stakeholders continue to improve their practices on fraud control in their own limited areas. As a consequence a lot of time and resources are spent on subjects that have already been researched by others. Collaboration between these parties will lead to an exchange of knowledge. Sharing experiences creates a win-win situation for all parties.

Cybercriminals have proven capable of finding and using extremely complicated and advanced ways to acquire valuable data. It's expected that e-fraud will only get more advanced as time progresses. This will happen on new platforms, such as the smartphone, but also by optimizing current techniques. Instead of merely responding to new and increasingly more complex threats the focus should lie in creating 'products' in a manner that makes them unappealing for potential fraudsters. Absolute safety is an impossibility but by making sure that fraud control measures are fully optimized the required effort and the risk of getting caught is so high that the potential reward will no longer be worth it.

For this to be accomplished it is necessary that the current mindset changes. IT systems have to become less complex. The fraud awareness of all stakeholders and the priority that they give to fraud control has to rise. This applies to the government, organizations and citizens. If any of these parties does not take adequate safety precautions an entire system can be at risk.

In the countries around us there is a trend to place the responsibility for fraud control in the hands of a central organization that coordinates efforts and stimulates cooperation. This cooperation in turn causes a rise in fraud awareness as an extra bonus.

The question we have to ask ourselves in the Netherlands is how the various promising initiatives of several sectors can be coordinated in such a way that we achieve the best results. An intensive cooperation between the various stakeholders and the private sector with a coordinating role by the government appears to be the optimal solution.

OPZET

Deze Quick Scan is bedoeld als ondersteuning bij de conferentie 'Fraude en ICT' die de Universiteit Twente en STT op 20 januari 2012 organiseren in Den Haag. Het is een snelle voorverkenning met als doel een globaal overzicht te krijgen van fraude en fraudebeheersing, en de huidige en toekomstige rol van ICT hierin. Welke vormen van fraude zijn in opmars? Wat is de rol die ICT speelt in fraude? Welke technologische ontwikkelingen kunnen gebruikt worden bij het voorkomen en opsporen van fraude, en welke stappen zouden nu al gezet moeten worden om de fraudeurs van morgen voor te zijn. Een vooruitblik helpt om de discussie over het te volgen pad op gang te brengen. De middelen die nu worden geïnvesteerd in fraudebeheersing zullen zich in de toekomst dubbel en dwars terugbetalen.

Op de conferentie komen stakeholders van velerlei sectoren aan het woord. Zij zullen hun visie op verschillende aspecten geven en de discussie aangaan. Doel is het creëren van een gezamenlijk draagvlak, waardoor men zich er bewust van wordt dat fraude een probleem is waaraan meer aandacht moet worden besteed. Mogelijke ontwikkelingen worden geschetst, suggesties worden gegeven en basiselementen aangereikt. Concrete plannen om de huidige aanpak van fraude verder te verbeteren en om toekomstige ontwikkelingen voor te zijn zullen moeten ontstaan door samenwerking van de verschillende sectoren.

Auteurs:
Alex van Geldrop, BSc (Universiteit Twente)
prof.dr.ir. Theo de Vries (Universiteit Twente, tevens STT-hoogleraar) met begeleiding van
ir. Hans van der Veen (secretaris STT) en
drs. Pierre Morin (directeur STT).

Eindredactie:
Annette Potting, Rosemarijke Otten, STT.

Colofon
ISBN 978-94-91397-01-1

STT-publicatie nr. 2 in het kader van de STT Academy
NUR 950
Trefwoorden: fraude, ICT, techniek, maatschappij

INLEIDING

WAT IS FRAUDE?

Fraude is een complex begrip. In de wet is er geen artikel dat fraude op zich strafbaar stelt. Het gaat om een verzamelnaam voor een veelvoud aan illegale handelingen. Om duidelijkheid te verkrijgen over de misdrijven die in deze categorie vallen, is het praktisch een definitie te hanteren waaraan delicten getoetst kunnen worden. In de praktijk blijkt het niet eenvoudig een eenduidige definitie te vinden die zowel breed genoeg is om alle verschillende soorten fraude te omvatten, en toch beperkt genoeg om delicten die geen fraude zijn te weren. Er zijn veel pogingen gedaan om dit duidelijk af te bakenen. Een van de meest recente pogingen komt van Schimmel [2004]. Deze definitie luidt als volgt:

"Fraude betreft een opzettelijke handeling waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging voor de handeling ontstaat, waardoor een onrechtmatig voordeel wordt verkregen."

Deze brede definitie geeft ruimte om een grote hoeveelheid verschillende misdrijven onder de categorie fraude te bundelen. Van zorgfraude tot identiteitsdiefstal tot het 'skimmen' van pinpassen. Aan de andere kant is de definitie ook streng genoeg om andere misdaden zoals afpersing of chantage te weren. Verder is het mogelijk om aan deze definitie toe te voegen dat fraude gaat om een niet-fysieke handeling. Er is geen sprake van een directe bedreiging of lichamelijk contact. Ondanks de definitie blijkt er nog regelmatig veel discussie mogelijk over de vraag of een bepaald misdrijf onder de noemer 'fraude' kan worden geplaatst. Dit grijze gebied is niet te voorkomen en er zullen altijd zaken blijven waarbij per geval moet worden beslist of deze in de categorie fraude vallen. De definitie is slechts een leidraad en zal nooit de plaats van gezond verstand kunnen innemen, maar het geeft ons een handvat om een eenduidig beeld te verkrijgen.

De afgelopen decennia is de rol van ICT in alle aspecten van de samenleving gegroeid. Fraude is hierop geen uitzondering. ICT heeft zijn weerslag gehad op de manier waarop fraude wordt bestreden, maar ook op de manier waarop deze wordt gepleegd. Het is interessant om te kijken welke effecten deze technologische ontwikkelingen hebben op het veld van fraude en fraudebeheersing. Verdere toekomstige technologische ontwikkelingen zullen ongetwijfeld lijden tot nieuwe manieren van fraude en meer geavanceerde methoden van fraudebestrijding. Een vooruitblik op fraude in de toekomst is een sleutelelement om gericht en concreet beleid te maken om fraude tegen te gaan.

ACHTERGROND

Fraude is een fenomeen dat door onze geschiedenis heen loopt. Vanaf het moment dat er mogelijkheden zijn geweest om door middel van list en bedrog persoonlijk voordeel te behalen, zijn er altijd mensen geweest die hier misbruik van maakten. Het is een probleem dat in alle sectoren van de samenleving plaats vindt. Fraude lijkt inherent aan onze menselijke cultuur.

De laatste jaren hebben technologische ontwikkelingen en vooral de opkomst van ICT voor fundamentele veranderingen gezorgd. Nu grenzen steeds meer vervagen en er door middel van ICT steeds meer 'non-fysiek' geld ontstaat, blijkt de schade die aangericht kan worden vele malen groter dan in het verleden. Mogelijke kostenposten kunnen tot gigantische bedragen oplopen. Behalve directe schade zorgt het gebruik van ICT ervoor dat iedereen door middel van massamedia op de hoogte kan zijn van grote fraudezaken. Elk nieuwsbericht over een malafide organisatie of een corrupt bestuur wordt groot uitgemeten en kan wereldwijd gevolgd worden. De laatste jaren zijn een aantal grote fraudezaken in de media gekomen waar het letterlijk over tientallen miljarden dollars gaat[1]. Er zijn ook andere zaken breed

1 Met als grootste voorbeeld de Ponzi Fraude van Bernard Madoff met een totale schade die wordt geschat op 65 miljard. Zie ook http://www.washingtonpost.com/wp-dyn/content/article/2008/12/12/AR2008121203970_2.html?hpid=topnews verkregen op 20-04-2011.

in de media uitgemeten die niet direct frauduleus zijn, maar die ethisch in een dubieus gebied vallen. Banken die jarenlang boven hun stand geleend hebben, gerespecteerde bedrijven die negatief in het nieuws komen vanwege hoge bonussen, terwijl de bedrijfsresultaten tegen vallen en zo zijn er nog een aantal voorbeelden te noemen waarbij men zich kan afvragen in hoeverre er 'correct' gehandeld is. De perceptie die hierdoor ontstaat is dat de grote organisaties die een voorbeeldrol moeten uitoefenen, het niet al te nauw nemen met ethische normen en waarden. Het is niet verwonderlijk dat mensen zich afvragen waarom zij zich wel zouden laten binden door normen en waarden, wanneer de grotere spelers dit niet doen.

Het effect dat wordt veroorzaakt door deze constante aandacht voor fraudegevallen is niet bekend, maar het is duidelijk dat er al jaren een zekere mate van acceptatie van fraude is. Belastingontduiking en verzekeringsfraude zijn normale gespreksonderwerpen aan de eettafel. De maatschappelijke acceptatie is zodanig dat deze vormen van fraude niet als echte misdrijven worden gezien.

Deze verandering in het morele aspect is terug te zien bij nieuwe technologische ontwikkelingen. Met de invoering van de OV-chipkaart werd snel duidelijk dat deze eenvoudig te kraken is. Met ingang van 2011 is het voor een consument mogelijk om via internet voor slechts € 30 de spullen online aan te schaffen om dit zelf voor elkaar te krijgen[2]. Dit is een voorbeeld waarbij een verschuiving te zien is van fraude op de achtergrond – waar het zich van oudsher altijd heeft opgehouden – naar fraude in de openbaarheid. Waar vroeger een fraudeur zijn praktijken niet of nauwelijks kon delen met anderen omdat dit het risico van ontmaskering met zich meebracht, is het nu een kleine moeite om methoden aan een groot publiek door te geven of te verkopen.

De sociale acceptatie van fraude is een groot probleem. Het besef moet aanwezig zijn dat fraude geen misdaad zonder slachtoffer is, maar dat er werkelijk grote bedragen verloren gaan die hun impact hebben op de gehele samenleving. Indirect betaalt iedereen mee aan de kosten die gemaakt worden. Het is moreel niet uit te leggen dat een eerlijke burger mee betaalt aan kosten die door fraudeurs worden veroorzaakt, terwijl er niets aan wordt gedaan om dit te bestrijden.

Een extremere variant op de verschuiving van fraude naar de openbaarheid is al te zien geweest in Griekenland. De strenge bezuinigingen daar worden in de ogen van de bevolking als onrechtvaardig gezien. Er is een gevoel dat de burger moet opdraaien voor de fouten van de regering. Als reactie hierop is een zogenaamde 'Den Pliroro'-beweging ontstaan. Deze beweging roept burgers op niet te betalen voor het (hun inziens) falen van de overheid. In eerste instantie bleef dit nog beperkt tot het niet betalen van de verhoogde tolbedragen, maar dit is overgeslagen naar zwart rijden met het openbaar vervoer en een oproep om elektriciteitsrekeningen niet langer te voldoen[3]. Het morele aspect is in Griekenland zo geraakt dat het wel betalen van tol juist wordt gezien als moreel verkeerd.

Ondanks dat er in Nederland ook grootschalige bezuinigingen plaats vinden op bijvoorbeeld defensie en een verhoging van de pensioensleeftijd zijn we erg ver verwijderd van taferelen zoals die in Griekenland. Toch zullen er stappen moeten worden gezet om een trend in deze richting tegen te gaan. Het besef moet ontstaan dat het plegen van fraude – of dit nou tegen een werkgever, een multinationaal bedrijf of de overheid is – een serieuze misdaad is.

De bevolking is niet de enige groep waar dit besef moet groeien. Bedrijven en overheid hebben jarenlang verschillende soorten van fraude een relatief lage prioriteit gegeven ten opzichte van andere misdaden. Dit heeft ertoe geleid dat de pakkansen

2 Trouw. *Journalisten reizen gratis met gekraakte OV-chipkaart*, 25-01-2011.

3 De Tijd. *Griekse ongehoorzaamheid,* 29/04/2011.

in veel gevallen schrikbarend laag zijn. De pakkans bij verzekeringsfraude was in 2006 slechts 1%, terwijl er een schadepost was van een miljard euro[4]. Faillissementsfraudeurs worden slechts in 2,5% van de gevallen vervolgd en bij studiefinancieringfraude is veelal niet genoeg capaciteit om gericht onderzoek uit te voeren[5]. De lage pakkansen stimuleren de perceptie dat fraude geen ernstig probleem is. Het besef dat het serieus moet worden aangepakt zal in alle sectoren van de samenleving moeten groeien. Slechts wanneer dit fraudebewustzijn tot volwassenheid is gekomen, kan er effectief opgetreden worden om tot verbetering te komen.

4 http://www.allesoververzekeren.nl/documenten/CBV-folder.pdf
5 Binnenlands Bestuur. *Sociaal rechercheurs zien veel fraude studiefinanciering,* 8-7-2009.

DE ROL VAN ICT

Het is van groot belang dat de rol die ICT speelt in fraude duidelijk wordt gemaakt. Deze rol is tegenwoordig zo vitaal dat dit niet sterk genoeg benadrukt kan worden.

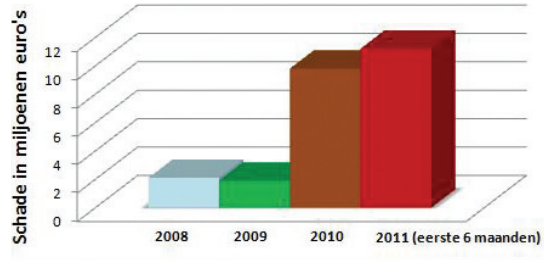
Fraude die online gepleegd wordt (ook wel: e-fraude) is een enorm lucratieve bezigheid. Het aantal potentiële slachtoffers is vrijwel grenzeloos. De anonimiteit is bijzonder hoog en mede hierdoor is de pakkans uitermate laag. Bovendien biedt de wereld van het internet voor individuen de mogelijkheid om een technologische voorsprong (hetzij door een grotere kennis, hetzij door betere software) op menige organisatie te nemen. Niet omdat deze organisaties geen toegang hebben tot geavanceerde software of expertise, maar omdat er helaas nog te vaak te weinig prioriteit wordt gegeven aan fraudebeheersing. Organisaties zijn niet de enige die hun beveiliging niet altijd op orde hebben. Particulieren houden veelal ook te weinig rekening met de mogelijkheid van fraude en maken zich hierdoor kwetsbaar.

Deze kwetsbaarheden worden genadeloos misbruikt door personen die het niet al te nauw nemen met de ethische normen en waarden. De rol die ICT daarin speelt is tweeledig. Allereerst zijn ICT-systemen van nature al zeer complex. Absolute veiligheid kan weliswaar nooit gegarandeerd worden, maar de hogere mate van complexiteit zorgt voor meer kwetsbaarheden. Dit feit en de enorme hoeveelheid data die omgaat in deze systemen leidt ontegenzeggelijk tot misbruik. Fraudegevallen ontstaan dus ook juist omdat processen en systemen via ICT lopen. De toepassing van ICT faciliteert fraude hier als het ware.

Daarnaast reikt ICT ook instrumenten aan die criminelen gebruiken om kwetsbaarheden uit te buiten. Het kan dan onder andere gaan om praktijken als 'phishing', 'malware', massamedia-fraude of een combinatie van meerdere instrumenten en technieken.

Deze moderne middelen zijn al jaren beschikbaar, maar het alsmaar toenemende aantal internetgebruikers zorgt voor een stijgende lijn in de frequentie van aanvallen en van het aantal potentiële slachtoffers. De bijzonder hoge penetratiegraad van internetgebruik in Nederland zorgt er helaas voor dat wij een aantrekkelijk doelwit voor online fraudeurs zijn. Mede hierdoor zien we een sterke verhoging van het aantal fraudepogingen.

De bankensector heeft de schade bijgehouden die de laatste jaren door phishing is toegebracht aan internetbankieren. In 2009 was dit nog 'slechts' 1,9 miljoen euro. Het jaar daarop was dit al meer dan vier keer vermenigvuldigd en in de eerste zes maanden van 2011 was deze schade al verder opgelopen tot 11,2 miljoen euro [De Nederlandse Bank; 2011]. De totale schade lijkt dus weer te verdubbelen ten opzichte van 2010. De stijgende lijn is overduidelijk (zie grafiek 1).



Grafiek 1: *Schade door phishing bij internetbankieren*

Andere vormen van e-fraude worden minder nauwkeurig bijgehouden, maar de algemene tendens is dat de frequentie waarmee deze aanvallen voorkomen steeds hoger komt te liggen.

Phishing is de verzamelnaam voor alle digitale activiteiten waarmee criminelen proberen persoonlijke informatie op te sporen. Met deze informatie kan fraude met internetbankieren, pinpassen, creditcards of zelfs met de identiteit worden gepleegd[6]. De meest voorkomende wijze waarop criminelen proberen gegevens te achterhalen is door een email te versturen die van een betrouwbare instantie,

6 www.veiligbankieren.nl

zoals een bank, lijkt te komen. Er wordt gevraagd aan de gebruiker om enkele persoonlijke gegevens in te voeren. Doet men dit niet, dan is er meestal een bepaalde dreiging, zoals de afsluiting van een bankrekening.

Om deze stijgende lijn tegen te gaan is de Nederlandse Vereniging van Banken in november 2011 begonnen met een campagne waarin men wijst op de gevaren van phishing en hoe gebruikers zich hiertegen kunnen wapenen.

Er zijn ook andere modus operandi die fraudeurs kunnen hanteren. Eén hiervan is het gebruik van malware (een samentrekking van 'malicious software'). Dit is kwaadaardige software die de computer infiltreert zonder dat de gebruiker zich hiervan bewust is. Deze malware kan grofweg twee algemene doelen hebben. Het kan waardevolle informatie (zoals gebruikersnamen en wachtwoorden) monitoren, opslaan en vervolgens doorsturen of het kan de processen van een computer daadwerkelijk beïnvloeden. Een gebruiker die naar de website van zijn eigen bank wil, kan dan bijvoorbeeld worden doorgestuurd naar de server van criminelen. Gegevens die worden ingevuld, kunnen worden bewerkt. Zo krijgen criminelen de gelegenheid om transacties te wijzigen of toe te voegen.

Fraudeurs hebben de mogelijkheid om specifieke individuen of grote groepen mensen tegelijkertijd aan te vallen. Momenteel ligt de nadruk op het maximaliseren van het aantal potentiële slachtoffers. Deze maximalisatie heeft geleid tot de term 'Mass Marketing Fraud' (MMF). De nadruk bij MMF ligt niet op de soort fraude die plaats vindt, maar meer op de wijze waarop slachtoffers benaderd worden. Dit kan onder meer per post, per telefoon en per internet gebeuren, maar de focus ligt op het gebruik van media om een zo groot mogelijk publiek te bereiken. Onder deze term is een veelvoud aan bekende fraudesoorten te scharen. Zonder er te diep op in te gaan valt hierbij te denken aan loterijfraude, 'Nigeriaanse 419' fraude, fraude op datingsites, 'advance fee' fraude en nog vele anderen. MMF is aantrekkelijk omdat het grensoverschrijdend is, er vrijwel geen investeringskosten aan verbonden zijn en omdat het moeilijk door overheidsinstanties te stoppen is.

Naast de vele mogelijkheden die ICT inherent biedt aan fraudeurs is er ook een toenemende trend dat organisaties hun ICT-infrastructuur uitbesteden aan externe partijen. Hun software, hardware en netwerken komen dan in de zogenaamde 'cloud' terecht. Dit betekent echter ook dat je de privacy, veiligheid, data-integriteit, het beheer van intellectueel eigendom en andere zaken in de handen van een derde partij legt. Wanneer blijkt dat deze derde partij zijn beveiliging niet op orde heeft, is het niet mogelijk directe aanpassingen te maken om die te verbeteren. Dat wil niet zeggen dat het gebruik van 'cloud computing' per definitie extra risico's met zich meebrengt. Integendeel, externe partijen die zich specialiseren in het beheren van ICT-infrastructuren hebben vaker de middelen in huis om voor betere beveiliging te zorgen dan menige afzonderlijke organisatie. Het probleem zit hem in de beperkte mogelijkheden om de externe beveiliging te controleren en zelfs wanneer deze mogelijkheden er wel zijn, is het nog de vraag in hoeverre controle naar behoren plaats vindt.

De mogelijkheden die ICT biedt zijn natuurlijk niet exclusief voorbehouden aan criminelen. Ook aan de kant van fraudebestrijding wordt gebruik gemaakt van de instrumenten die ICT biedt. Met name bij het detecteren van fraude wordt gespecialiseerde software ingezet. Deze software is erop gericht om afwijkingen van normaal gedrag te detecteren. Er is een hoop wiskundige kennis beschikbaar waarmee fraude kan worden opgespoord. Deze kennis wordt echter nog niet overal ten volle benut. Dit komt omdat organisaties meestal niet op dergelijke toepassingen zijn ingesteld. Ook het gebruik van centrale databases in sectoren is mogelijk. Zo kunnen gedetecteerde fraudegevallen gedeeld worden met collega's en concurrenten. Organisaties kunnen zich beter instellen op veelvoorkomende fraudemethoden en bekende fraudeurs kunnen geweerd worden.

De invloed van ICT op fraude en fraudebeheersing verschilt per fraudedomein en per bedrijfssector. Soms is het gebruik van ICT de fundamentele oorzaak van fraude en bij andere domeinen biedt het slechts instrumenten. Bij weer andere domeinen speelt het niet of nauwelijks een rol. Ook in de fraudebeheersing is het gebruik van ICT sterk sectorafhankelijk. Om deze verschillen te verduidelijken wordt hierna een overzicht gegeven van de huidige stand van zaken.

HUIDIGE BLIK OP HET VELD

Elke gerichte aanpak die betrekking heeft op fraudebeheersing zal moeten beginnen met een duidelijk overzicht van de huidige situatie. Een nulmeting. Informatie over de hoogte van de schade veroorzaakt door fraude is een eerste vereiste. Een gebrek hieraan betekent dat het niet mogelijk is om het effect van maatregelen te meten en dat elke conclusie slechts een schot in het donker is. Betrouwbare data is dus noodzakelijk, maar desondanks vaak niet aanwezig. Er zijn gelukkig positieve uitzonderingen – zoals de verzekeringsbranche die de laatste jaren veel aandacht aan fraudebeheersing heeft besteed – maar om tot een coherente strategie te komen, zal er een compleet beeld moeten komen waaraan gerefereerd kan worden. Ten tweede is er informatie nodig over de zwakke punten van systemen. In het algemeen kan men zeggen dat naarmate de complexiteit van een systeem toeneemt, het aantal zwakke punten ook toe zal nemen. ICT-systemen zijn in de regel zeer complex. Het logische gevolg is dat naarmate het gebruik van ICT-toepassingen toeneemt er meer zwakheden ontstaan. Wanneer slechts één medewerker door onveilig internetgedrag een schadelijk bestand binnen krijgt, kan een hele organisatie gecomprimeerd worden. Hoe meer systemen er in een keten zitten, hoe meer mogelijke zwakke plekken er zullen zijn. Om deze zwakke plekken te achterhalen moeten experts in het desbetreffende veld geraadpleegd worden.

Deze kwetsbaarheden zijn niet simpel te achterhalen en de doelstelling van deze Quick Scan is niet om een allesomvattende analyse aan te bieden. Energie, tijd en middelen zijn nodig om accurate uitspraken te doen. Er zal een bepaalde motivatie moeten zijn, voordat deze investeringen gedaan worden. In gesprekken met experts blijkt steeds weer dat investeringen gericht op signalering van fraude over het algemeen ruim terugverdiend worden in de vorm van gedetecteerde fraude. Het grootste probleem zit hem veelal in de prioriteit die een organisatie of bedrijvensector aan fraudepreventie en -beheersing toe kent. Veel bedrijven zien fraude niet als grote zorg, maar slechts als bijzaak of niet-vermijdbare kosten. Dit verschilt sterk per sector. De ontwikkelingen op het gebied van fraudebeheersing zijn momenteel dan ook gefragmenteerd. De meeste sectoren hebben hun eigen aanpak en ontwikkelen hun eigen, te vaak nog primitieve, methoden om fraude tegen te gaan zonder te overleggen met andere instanties die wellicht op dezelfde problemen zijn gestuit in het verleden. In sommige sectoren groeit langzaam het besef dat het probleem effectiever aangepakt kan worden als er wordt samengewerkt met bedrijven in dezelfde sector, met bedrijven in andere sectoren en met de overheid.

Deze vormen van samenwerking komen nog relatief weinig voor, maar hun aantal begint te groeien. Het concurrentiebelang wordt aan de kant geschoven om samen fraude tegen te gaan. De bankensector bijvoorbeeld beseft dat gevallen van fraude veel meer kosten dan alleen de directe schade die het veroorzaakt. De reputatie dat een bank 'veilig' is wordt aangetast en dat kan zorgen voor veel grotere problemen. Het zou de betrouwbaarheid van de gehele bankensector kunnen aantasten en ervoor zorgen dat het gebruik van internetbankieren een slechte naam krijgt. Een situatie waarin de banken terug gaan naar het handmatig verwerken van opdrachten is niet meer haalbaar [Hegt; 2008]. Mocht de integriteit van internetbankieren dus zodanig worden aangetast dat het vertrouwen volledig weg is, dan zou dit een ramp voor de hele bankensector betekenen. Dit kunnen zwaarwegende redenen zijn om het concurrentiebelang aan de kant te zetten als het gaat om fraudebeheersing.

De verschillende vormen van fraude hebben vaak invloed op meerdere bedrijfstakken. Dit zorgt ervoor dat er geen duidelijke eindverantwoordelijke is voor de fraudebestrijding in bepaalde domeinen. Zeker het gebruik van ICT heeft als gevolg dat fraude sectoroverkoepelend is. Wanneer er onduidelijkheid is over de eindverantwoordelijkheid, ontstaat er een ketenprobleem waarbij niemand het initiatief wil nemen om concrete stappen te zetten. Dit diffuse patroon dat ontstaat door een gebrek aan concrete actie zorgt voor een sluipende erosie van de rechtsstaat. Fraudeurs komen immers weg met hun wederrechtelijke acties, waardoor normvervaging steeds ernstiger wordt. De overheid

is op dat moment degene die de verantwoordelijkheid heeft om hiertegen op te treden. Zij heeft een leidende rol en moet een voorbeeldfunctie uitdragen. Een overheid die het belang van fraudebeheersing erkent zal in haar kielzog invloed uitoefenen op andere organisaties en kan zodoende de strijd aanvoeren tegen fraude. Incidenten zoals de recente DigiNotar-affaire tasten echter het noodzakelijke gezag van de overheid ernstig aan.

Het grote aantal afzonderlijke fraudedomeinen en de grote verschillen in het gebruik van ICT zorgen ervoor dat het wenselijk is om per domein een overzicht te geven van de huidige stand van zaken.

FRAUDEDOMEINEN

Het is van belang om per sector inzicht te hebben in de soort fraude, de schade die geleden wordt, de rol van ICT en de maatregelen die genomen zijn om fraude tegen te gaan. Daardoor alleen al ontstaat er een beeld dat voldoende is om de ernst van het fraudeprobleem te illustreren. Onderstaand wordt daarom voor een (klein) aantal domeinen een overzicht gegeven van de huidige situatie. Het gaat slechts om een greep uit de verschillende vormen van fraude en de lijst is verre van volledig. Vanwege de opzet van deze Quick Scan is het niet mogelijk om een compleet overzicht van alle fraudedomeinen te geven. Het is slechts bedoeld om een voorstelling te geven van de kosten die met fraude gemoeid zijn en om enkele initiatieven die dit tegengaan onder de aandacht te brengen. De rol van ICT in deze initiatieven krijgt bijzondere aandacht.

Acquisitiefraude

Definitie: *Het op geraffineerde wijze stelselmatig benaderen door malafide advertentiebureaus, uitgeverijen, adviesbureaus of personen, handelend in opdracht van dit soort bedrijven, van aan het economisch verkeer deelnemende organisaties (bedrijfsleven, overheid, gesubsidieerde sector), met als doel het onder valse voorwendselen verkrijgen van advertentieopdrachten door het oplichten en misleiden van werkzame personen binnen die organisaties, teneinde daar een financieel voordeel mee te behalen.*[7]

Schade: *400 miljoen [Steunpunt AcquisitieFraude; 2009]*

Acquisitiefraude komt in veel vormen voor, maar het basisidee is altijd hetzelfde. Fraudeurs gokken erop dat ondernemers geen tijd hebben om alles wat binnen komt grondig te bestuderen. Ze maken hier gebruik van door hen te laten tekenen voor bepaalde diensten die legitiem overkomen. Dit kan bijvoorbeeld gebeuren door spooknota's te versturen. Dit zijn facturen waarvoor geen onderliggende overeenkomst is. Wanneer deze ondertekend worden, wordt er betaald zonder dat er een dienst verleend wordt. Of blijkt uit de kleine lettertjes dat nu een dure dienst is afgesloten die naar alle vormen van redelijkheid en billijkheid niet overeen komt met het te betalen bedrag. De rol van ICT in acquisitiefraude blijft beperkt tot een faciliterende rol. Berichten kunnen makkelijker en sneller naar grote groepen ondernemers worden gestuurd, maar de achterliggende handelswijze wijzigt niet.

In 2003 hebben een aantal stakeholders besloten de handen ineen te slaan om deze vorm van fraude aan te pakken. Onder leiding van de Stichting Aanpak Financieel-Economische Criminaliteit in Nederland (SAFECIN) hebben onder andere het ministerie van Justitie, MKB-Nederland en de Stichting Reclame Code Commissie een meldpunt opgericht waar men terecht kan wanneer men slachtoffer is geworden. Dat meldpunt heet het Steunpunt AcquisitieFraude (SAF). Ondernemers krijgen advies over de te volgen procedures en wat zij kunnen doen om dit te voorkomen. Het doel van het SAF is om zowel preventief als repressief fraudeurs tegen te gaan en zodoende de omvang en schade van acquisitiefraude te verminderen.

De samenwerking is een duidelijk signaal dat het probleem wordt onderkend. Toch kan de aanpak nog verbeterd worden. Er is niet genoeg financiële armslag om ondernemers vooraf te waarschuwen en zodoende is preventie lastig te realiseren. Ook is er geen landelijk loket om digitaal aangifte te doen en blijkt het daadwerkelijk veroordelen van de daders een tijdrovende zaak, als een veroordeling

7 www.fraudemeldpunt.nl

überhaupt al plaats vindt[8]. Een bijkomend probleem is dat er steeds vaker grensoverschrijdend opgetreden wordt. Dit betekent dat er een internationale samenwerking nodig zal zijn om deze fraude effectief tegen te gaan.

Belastingfraude

Definitie: *Het bewust verzwijgen of onjuist doorgeven van genoten inkomsten of het onterecht opvoeren van aftrekposten om zodoende een financieel voordeel van de belasting te verkrijgen.*[9]

Schade: *onbekend*

Er zijn weinig openbare gegevens beschikbaar over de totale schade door belastingfraude. 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 bedrag per abuis in het belastinggat komt, twijfelachtig is. Desalniettemin gaat belastingfraude om gigantische bedragen. Wanneer we de 15 miljard pond extrapoleren aan de hand van het aantal volwassen inwoners in beide landen, dan komen we op een schatting van 4,36 miljard euro per jaar in Nederland[10], maar zoals gezegd gaat het om een uitermate voorzichtige schatting. De totale schade in Europa wordt geschat op maar liefst 200 tot 250 miljard euro per jaar[11]. Wanneer we kijken naar het inkomen dat omgaat in de verborgen economie in Nederland is dat 58 miljard euro per jaar [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 euro uit dat we elk jaar mislopen aan belastingen[12]. Dat dit een gigantisch bedrag is wordt extra duidelijk, wanneer we het vergelijken met het huidige begrotingstekort van 18 miljard euro.

De rol van ICT in belastingfraude is van oudsher niet groot. Het bestaat grotendeels uit het doorgeven van foutieve informatie of het verzwijgen van informatie. Met de digitale ondertekening van belastingaangiftes is hierin enigszins verandering gekomen. Het bleek mogelijk om belastingtoeslagen (weliswaar gaat het hier niet direct om inkomstenbelasting, maar het principe is belangrijk) op andermans naam met de eigen DigiD aan te vragen. Dit leidde tot massale fraude[13]. De keuze om het aanvragen van toeslagen op deze manier in te voeren was gebaseerd op wederzijds vertrouwen. Slechts één persoon hoefde misbruik te maken van deze aanname om hiervan te profiteren. Wanneer bij de ontwerpfase meer aandacht was besteed aan fraude, zou een dergelijk ontwerp nooit doorgevoerd kunnen zijn.

De belastingdienst en de fiscale opsporingsdienst (de FIOD-ECD) hebben een uitgebreid controleapparaat. Dit maakt het moeilijk om ongemerkt onjuiste informatie door te geven. De FIOD-ECD bestaat uit 1.100 medewerkers waaronder een aantal opsporingsteams, forensisch-technische recherche en juristen. Uit de eerdergenoemde bedragen blijkt duidelijk dat dit het domein is waar veel te bereiken is op het gebied van fraudebestrijding.

Het is de vraag in hoeverre detectiemethoden zoals wiskundige modellen toepasbaar zijn in dit domein. Deze modellen zijn gebaseerd op het vinden van statistische afwijkingen in data. Bij de verborgen economie gaat het echter om een gebrek aan data. Het zal een uitdaging zijn om innovatieve methoden te vinden die in dit veld toepasbaar zijn.

8 Het Parool. *Spooknota's teisteren bedrijfsleven*, 2-8-2011.
9 Bij gebrek aan een officiële definitie hanteren wij een eigen definitie.
10 15 / 3,9 (GB heeft 3,9 keer meer volwassen inwoners dan Nederland) * 1,1472 (pond t.o.v. euro).
11 http://www.europa-nu.nl/ - Beleid fraudebestrijding.
12 Reformatorisch Dagblad. *Staat loopt 24 miljard mis door zwart werk*, 20-12-2010.
13 NRC. *Massafraude met belastingtoeslagen*, 19-09-2011.

Beleggingsfraude

Definitie: *Geld dat verkregen wordt door middel van de belofte van hoge niet-haalbare rendementen. De illusie wordt gewekt dat deze rendementen behaald worden door personen vanuit de inleg van nieuwe klanten te betalen.*

Schade: > *750 miljoen* [Roest; 2007]

De grootste beleggingsfraudezaak ooit is de zaak van Bernard Madoff. Een joodse gerespecteerde handelaar op Wall Street die goede, maar onrealistisch hoge rendementen beloofde (van ongeveer 10%) en deze ook standaard uitbetaalde. Achteraf lijkt de constantheid van de uitbetalingen een reden voor verdenking te zijn (slechts drie maal een verlies in 87 maanden). Maar blijkbaar is het mens-eigen om niet achterdochtig te zijn, wanneer de praktijken in het eigen voordeel zijn. Op het moment dat het nieuw verkregen kapitaal niet meer voldoende was om de uitkeringen te betalen stortte deze 'piramide' in. De totale schade bleek $ 65 miljard te zijn! Van dit bedrag bleek $ 2 miljard schade uit Nederland te zijn.

Vanwege het kleinere inwonersaantal zullen beleggingsfraudezaken die in Nederland plaats vinden over het algemeen kleiner van omvang zijn. Toch gaat het ook hier over honderden miljoenen euro's. Naar alle waarschijnlijkheid gaat deze vorm van fraude de komende jaren vaker voorkomen of in ieder geval vaker aan het licht komen. Vanwege de historisch lage rentes zijn beleggers op zoek naar investeringen die hoge rendementen kunnen geven. In het verleden is steeds weer gebleken dat mensen verleid kunnen worden tot het investeren in producten met hoge rendementen. Het is nu de vraag of beleggers wakker zijn geschud door de grootschalige fraudepraktijken die aan het licht zijn gekomen. Of dat zij nog steeds het voordeel van de twijfel geven aan bedrijven die hoge rendementen beloven. Door het gebruik van ICT is de drempel om in een beleggingsmogelijkheid te stappen een stuk lager. Impulsieve beslissingen zonder gedegen vooronderzoek zullen daardoor vaker voorkomen. Dit is in het voordeel van fraudeurs. Om deze redenen is de verwachting dat er de komende jaren een groter aantal aangiftes van de zogenaamde 'Ponzi-schemes' en Boilerroom[14] zaken zal plaatsvinden.

Beginnende beleggers worden nog enigszins beschermd door de Autoriteit Financiële Markten (AFM). Het doel van het AFM is: "Het bevorderen van een ordelijk en transparant marktproces, een zuivere verhouding tussen marktpartijen en de bescherming van de consument op de financiële markten"[15]. In de praktijk stelt het AFM verplicht dat er bij beleggingen onder de € 50.000 een aantal voorwaarden zijn waaraan een product moet voldoen. Zo moet er een duidelijke prospectus zijn, en zijn er een aantal waarborgen nodig. Bij beleggingen boven de € 50.000 houdt het AMF geen toezicht meer. De achterliggende gedachte is dat beleggers die dergelijke bedragen investeren zelf voldoende kennis van zaken hebben, en zelf voldoende onderzoek naar het product moeten doen voordat zij investeren. Geen onterechte gedachtegang, maar in de praktijk blijkt het nog regelmatig mis te gaan. Een recent voorbeeld is 'Royal Dubai' en het daaropvolgende 'Golden Sun'[16]. Beide waren investeringsmogelijkheden die een rendement van 12,5% beloofden. Een professionele website, goede tv-reclame en een mooi kantoorpand bleken voldoende om mensen te laten geloven dat het om een solide, eerlijk en betrouwbaar product ging.

Om deze vorm van fraude tegen te gaan wil het AFM het toezichtbedrag verhogen tot € 100.000[17]. Toch zullen er altijd gevallen zijn waar de belofte van hoge rendementen een dusdanig sterke verleiding heeft dat beleggers onduidelijkheden voor lief nemen. Beleggers zullen er zelf voor moeten

14 Fraudeurs brengen slachtoffers het hoofd op hol met overtuigende verkooppraatjes over grote winsten. Omdat er veel achtergrondgeluiden te horen zijn, zoals rinkelende telefoons en schreeuwende verkopers, wekt de organisatie de indruk dat het om een echt en eerlijk bedrijf gaat dat belangrijke handel drijft, en dat je snel moet beslissen, want anders zijn de aandelen verkocht.
15 http://www.afm.nl/nl/over-afm.aspx
16 http://financieel.infonu.nl/. *Royal Dubai & Golden Sun: Miljoenen zwendel*, 2007.
17 http://www.fx.nl/. *AFM wil uitbreiding toezicht belegging*, 14-04-2010.

zorgen dat zij gedegen onderzoek uitvoeren en zich niet laten verblinden door mooie vooruitzichten. Complexe systemen voor fraudebeheersing hebben hier weinig nut. Van belang is wetgeving en voorlichting van de belegger. Deze kan dan vervolgens wel vooronderzoek doen op internet. Wanneer de minimale inleg van een product boven de toezichtdrempel van het AMF ligt, zouden bij potentiële beleggers alle alarmbellen moeten gaan rinkelen.

Faillissementsfraude

Definitie: *Als er sprake is van opzettelijk, wederrechtelijk handelen waardoor de faillissementsschuldeisers van de failliete rechtspersoon opzettelijk of culpoos worden benadeeld, is er sprake van faillissementsfraude* [Knegt et. Al.; 2005]

Schade: *1,7 miljard*[18]

In een kwart van alle faillissementen in Nederland vindt fraude plaats. Deze fraude is te verdelen over twee uitersten van een continuüm. Aan de ene kant zijn er ondernemers die ondanks hun beste inspanningen failliet gaan en die binnen hun faillissement wederrechtelijk handelen. Denk bijvoorbeeld aan het plotseling 'verdwijnen' van de resterende inboedel. Aan de andere kant van het continuüm zijn er ondernemers die een organisatie overnemen of opstarten met de voorbedachte intentie om deze failliet te laten gaan. Denk hierbij aan een overname van een onderneming die flink in de schulden zit voor een symbolisch bedrag, waarbij onderhands een geldbedrag betaald wordt door de ondernemer in schulden. De nieuwe eigenaar zorgt ervoor dat de boekhouding en alle bezittingen van waarde verdwijnen, waardoor uiteindelijk schuldeisers en werknemers hun vorderingen niet kunnen innen. Deze verschillende uitersten van fraude binnen faillissementsfraude leiden tot zeer uiteenlopende schattingen van de schade. Minister Opstelten noemt een bedrag van 1,7 miljard, andere onderzoeken gaan van een lager bedrag uit [Tromp et. Al.; 2010].

18 Aangegeven door minister Opstelten in een reactie op Kamervragen van het lid Gesthuizen. 28-01-2011.

Technologische ontwikkelingen spelen een marginale rol in deze vorm van fraude. Computers en ICT worden gebruikt om transacties af te handelen, maar de manier waarop de fraude tot stand komt verandert niet wezenlijk. De nadruk ligt op het misleiden van werknemers en handelspartners. Technologische ontwikkelen maken hooguit de interactie anoniemer.

Een pakkans van 2,5% bij deze vorm van fraude zorgt niet voor een preventieve werking. In combinatie met de hoge mogelijke baten houdt dit in dat faillissementsfraude een grote aantrekkingskracht heeft op kwaadwillenden. Er zijn wel mogelijkheden om de detectie van faillissementsfraude te verhogen. Vanuit onderzoek komt naar voren dat als voornaamste voorspeller er een groot aantal veranderingen in het bestuur in de zes maanden voorafgaand aan het faillissement is, en dat fraude vaker voorkomt wanneer bestuurders een strafblad hebben [Geldrop, van; 2011]. Door het gebruik van neurale netwerken kan de detectie verhoogd worden tot meer dan 30% [Veldkamp & de Vries; 2008] met een zeer laag percentage 'false positives'. Een grotere detectie leidt ook tot meer preventie. Wanneer duidelijk is welke bedrijven een groot risico op faillissementsfraude lopen, kan hier voordat het faillissement daadwerkelijk plaats vindt al meer aandacht aan worden besteed door middel van controles. Met behulp van mathematische technologie kan in principe ook worden bepaald welke bedrijven of bestuurders 'at risk' zijn.

Detectie is een belangrijk onderdeel van fraudebeheersing. Het is echter slechts een eerste stap. Het veroordelen van fraudeurs blijkt een tijdrovend en inefficiënt proces te zijn. Experts geven aan dat een verbeterde samenwerking tussen de betrokken instanties hierin een belangrijke rol kan spelen [Tromp et. Al.; 2010], omdat de aanpak van faillissementsfraude een ketenprobleem is. Er is niet één orgaan dat eindverantwoordelijk is. Juist dit maakt een effectieve aanpak moeilijk. Recidivisme is relatief eenvoudig voor fraudeurs die eerder tegen de lamp gelopen zijn. Het gebruik van katvangers of het oprichten van een buitenlandse BV zorgt er meestal voor dat de wederrechtelijke praktijken

voortgezet kunnen worden. Curatoren doen vaak geen aangifte, omdat dit een tijdrovend proces is dat regelmatig weinig resultaat oplevert. De medewerkers van Justitie geven op hun beurt aan dat vanwege het lage aantal aangiftes het probleem niet hoog op de beleidsagenda komt te staan. Deze cirkel zal doorbroken moeten worden om verdere ontwikkelingen mogelijk te maken.

Hypotheekfraude

Definitie: *Het op basis van valse informatie verkrijgen van een hypothecaire geldlening, met dien verstande dat bij juiste informatie de lening niet, of niet onder dezelfde condities verstrekt zou worden*[19].

Schade: *Onbekend*

Hypotheekfraude kent veel vormen[20]. Een hypotheekaanvraag kan gedaan worden op valse gegevens zoals vaag gekopieerde werkgeversverklaringen of kopieën van paspoorten. Er zijn zogenaamde 'ABC'-constructies waarbij een woning wordt gekocht en direct voor een hoger bedrag aan een derde wordt doorverkocht. Het kopen van een of meerdere woningen als hoofdwoning en deze dan doorverhuren, terwijl dit niet mag zonder toestemming van de hypotheekverstrekker, huisjesmelken, of de woning gebruiken voor illegale handelingen zoals hennepteelt of prostitutie. Het aantal personen dat bij deze fraude betrokken is, is groot: kopers, (door)verkopers, makelaars, taxateurs, notarissen, vastgoedtussenpersonen, hypothecaire tussenpersonen en hypothecaire financiers[21]. ICT biedt instrumenten om deze vorm van fraude te vergemakkelijken. Vervalsingen van documenten en dergelijke zijn bijvoorbeeld mogelijk. De rol van ICT is echter niet fundamenteel voor dit domein.

Vanwege de complexiteit van het probleem is er een breed kader aan tegenmaatregelen nodig. De instantie die deze vorm van fraude aanpakt is de Stichting Fraudebestrijding Hypotheken (SFH).

Vrijwel de gehele Nederlandse hypothekenmarkt is hierbij aangesloten en het fraudeloket zetelt bij de Nederlandse Vereniging van Banken. Er zijn echter veel andere belanghebbenden.

De gemeenten Den Haag en Rotterdam hebben convenanten opgesteld met het SFH, omdat huisjesmelken in deze gemeenten een serieus probleem is. In Rotterdam is een pilot opgestart om hypotheekfraude aan te pakken. Kernpunten van deze pilot zijn ook hier de samenwerking tussen de verschillende partijen en fraudebewustwording. Wanneer bijvoorbeeld een notaris een woning tegenkomt die binnen een half jaar twee maal wordt verkocht, moet dit een reden zijn om te gaan kijken wat daarvan de reden is. Blijkt later dat dit inderdaad door malafide praktijken komt, dan moet er contact worden opgenomen met de financier.

De pilot in Rotterdam richt zich echter niet op het gehele gebied van hypotheekfraude. Wanneer iemand met een valse werkgeversverklaring bij een financier komt, ziet een notaris hier niets van. Om deze praktijken tegen te gaan is een incidentenwaarschuwingssysteem opgezet, het SFH-systeem. Bekende fraudeurs worden in dit systeem geregistreerd en alle leden van het SFH hebben inzicht hierin. Op deze wijze worden financiers gewaarschuwd voor risicovolle klanten. Ook hier kunnen risicovolle situaties worden geïdentificeerd met behulp van mathematische technologieën. Het gebruik van ICT voor fraudebeheersing levert al resultaten op[22].

Identiteitsdiefstal

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 [Vries, de; 2007].*

Schade: *onbekend*

19 http://www.stichtingfraudebestrijdinghypotheken.nl
20 De Volkskrant. *Goochelen met geld en papieren,* 8-4-2005.
21 www.rotterdamveilig.nl. *De fraude voorbij,* 27-11-2007.
22 http://www.stichtingfraudebestrijdinghypotheken.nl/index.php?p=501900

Identiteitsfraude is een overkoepelende fraudeactiviteit. In het verlengde hiervan worden met de achterhaalde gegevens een reeks aan verschillende fraudesoorten gepleegd. Voorbeelden zijn fraude met internetbankieren, uitkeringen aanvragen op naam van een ander of zelfs de gehele identiteit van een persoon overnemen compleet met een gezin, sociale contacten en baan. Deze laatste vorm is het meest 'spectaculair', maar gelukkig erg zeldzaam.

Identiteitsdiefstal is het fraudedomein waar ICT de meest cruciale rol speelt. De complexiteit van ICT-systemen geeft een dermate groot aantal kwetsbaarheden dat identiteitsfraude vrijwel uitsluitend hier plaats vindt. Toch bestond dit domein van fraude ook al voor de hoogtijdagen van het internet. Praktijken als 'dumpster diving', waarbij persoonlijke gegevens uit het afval worden gepikt en daarna voor illegale praktijken worden gebruikt, bestaan al langere tijd. Sinds de opkomst van ICT is de manier waarop identiteitsdiefstal wordt gepleegd echter in een korte periode fundamenteel veranderd. Deze revolutie komt voort uit het feit dat vrijwel alle data die voor zakelijke transacties nodig is online wordt opgeslagen. De gemiddelde Nederlander komt tegenwoordig voor in maar liefst 500 databases [Schermer & Wagemans; 2009]. Dit betekent dat maar een van deze 500 databases een kwetsbaarheid in de beveiliging hoeft te hebben om criminelen de gelegenheid te geven iemands persoonlijke data te stelen. ICT speelt bij identiteitsdiefstal dus een wezenlijke rol.

Fraudeurs verzamelen de gegevens die hiervoor nodig zijn steeds vaker online. Aan de ene kant komt dit door de innovatie van fraudeurs en de steeds geavanceerdere methoden die zij gebruiken. Phishing, skimmen, trojans, het zijn allemaal manieren om persoonlijke gegevens te verkrijgen en de technieken die hiervoor gebruikt worden, worden steeds complexer. Op het moment dat er stappen worden gezet om één methode tegen te gaan, wordt er al snel een nieuwe aanpak bedacht om dit te omzeilen. Aan de andere kant komt de toename van identiteitsfraude ook omdat mensen steeds meer bereid zijn om gevoelige persoonlijke informatie openbaar te maken door deze op het wereldwijde web te zetten. Dat maakt de kans op potentiële fraudeurs groter.

Er zijn geen Nederlandse cijfers over het aantal gevallen van identiteitsdiefstal of de schade die hierdoor wordt veroorzaakt. In andere landen zijn ze hier verder mee. In de Verenigde Staten wordt het aantal slachtoffers van identiteitsdiefstal bijvoorbeeld geschat op 11,1 miljoen. De totale schade is maar liefst 37 miljard dollar in 2010 [Javelin Strategy and Research; 2011]. Identiteitsdiefstal is dus een zeer serieus probleem met potentieel enorme schade.

De ernst van het probleem wordt ook door de overheid onderkend. Als reactie hierop is per 1 maart 2010 een centraal meldpunt ingesteld voor identiteitsdiefstal (CMI)[23]. Enkele van de instanties die hieraan meewerken zijn het ministerie van Defensie, het ministerie van Veiligheid en Justitie, de Koninklijke Marechaussee, het Expertisecentrum Identiteitsfraude, de Belastingdienst, het UWV en de politie. Het doel van het CMI is om: "burgers, bedrijven en overheden die te maken hebben met identiteitsfraude of met een fout in de registratie van persoonsgegevens, te ondersteunen en te adviseren." Deze doelstelling duidt op een repressieve aanpak. Onder het motto 'voorkomen is beter dan genezen' is te beargumenteren dat een preventieve strategie nog ontbreekt en nog opgesteld moet worden. Preventieve maatregelen kunnen getroffen worden door ervoor te zorgen dat software beter beveiligd wordt, maar welke oplossingen er ook ontwikkeld worden, of dit nou encryptie, biometrie of mobiele authenticatie is, de kwetsbaarheid blijft uiteindelijk bij de persoon zelf liggen. Denken dat software deze kwetsbaarheid volledig zal uitsluiten, is een illusie [Dobbelaere; 2010]. Bewust bezig zijn met veilig internetgedrag is de allerbelangrijkste maatregel die gebruikers zelf kunnen nemen om misbruik te voorkomen.

Sociale uitkeringsfraude

Definitie: *Het opzettelijk verkeerde informatie*

23 http://www.overheid.nl/identiteitsfraude

geven of dingen verzwijgen om onterecht aanspraak te maken op een sociale uitkering of om deze te behouden[24].

Schade: *onbekend*

De gedetecteerde fraude in 2010 was 53 miljoen aan bijstandsfraude en 66 miljoen aan fraude met andere uitkeringen[25]. Ook hier geldt dat het waarschijnlijk om het topje van de ijsberg gaat. Vooral bij deze kostenpost is het ethisch aspect zeer belangrijk. Het draagvlak voor uitkeringen is erg kwetsbaar. Op het moment dat berichten over een grootschalig misbruik openbaar worden gemaakt komen er al snel allerlei onderbuikgevoelens naar boven over de onrechtvaardigheid van het uitkeren van belastinggeld aan personen die hierop geen recht hebben.

Fraude met uitkeringen kan in twee categorieën worden ingedeeld. Er is een groep mensen die geen recht heeft op een uitkering en die bewust valse (of juist helemaal geen) informatie door geeft om door middel van misleiding een uitkering aan te vragen. Hierin speelt ICT een marginale rol. Daarnaast is er een groep mensen die gegevens steelt en op andermans naam uitkeringen aan vraagt die worden uitbetaald op een rekeningnummer waar de fraudeur bij kan. De rol van ICT is hier fundamenteler, maar dit wordt besproken onder het domein 'identiteitsdiefstal'.

Fraudebeheersing op dit gebied gebeurt door verschillende instanties waaronder het UWV en de SIOD. Detectie gebeurt door risicoanalyses, bestandskoppelingen en risicoselectie. Ook de informatie-uitwisseling tussen betrokken instanties wordt steeds verbeterd. Deze toegenomen samenwerking leidt tot een verbeterde fraudebestrijding.

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].*

Schade: *900 miljoen – 1 miljard*

Verzekeringsfraude is een veelvoorkomend probleem met hoge kosten en een erg lage pakkans (in 2006 slechts 1%). De tendens om declaraties online te laten invullen zorgt voor een gevoel van anonimiteit bij de gebruiker, waardoor de perceptie van het risico om gepakt te worden daalt. Het gebruik van ICT stimuleert zo de mogelijkheid tot fraude en maakt het gemakkelijker voor verzekerden om de stap naar het plegen van delicten te zetten.

Naar aanleiding van de hoge kosten en de lage pakkans is besloten om een overkoepelend orgaan op te richten, namelijk het Verbond van Verzekeraars. Het besef dat fraude een serieus probleem was dat veel effectiever aangepakt diende te worden bleek in veel organisaties niet of nauwelijks aanwezig. Om deze redenen is in 2006 een Deltaplan opgezet. In dit plan werd gesteld dat elke aangesloten verzekeraar een bepaald minimumniveau van fraudebeheersing dient te hebben. De uiteindelijke ambitie was om de pakkans met een factor tien te verhogen (naar 10%). Hoewel het er naar uitziet dat dit te hoog gegrepen is, zijn er zeker verbeteringen opgetreden.

Deze inspanningen hebben ertoe geleid dat vrijwel elke verzekeraar een aparte afdeling voor fraude heeft opgericht. De grootte en mogelijkheden van deze afdelingen verschillen wel sterk per verzekeraar. Waar anti-fraudebeleid bij de één een hoge prioriteit heeft, is het bij de ander slechts een bijkomstigheid. Nu de winsten over het algemeen onder druk staan vanwege de roerige economische tijden, is

24 http://www.utrecht.nl/smartsite.dws?id=327233#Algemeen%20belang. Definitie aangepast om deze niet alleen voor bijstandsfraude, maar ook voor uitkeringsfraude in het algemeen te laten gelden.
25 VNG Magazine. G*rote schade door uitkeringsfraude*, 9-9-2011.

te zien dat bij een aantal verzekeraars middelen weggehaald worden bij fraudebeheersing, omdat ze elders 'beter' ingezet kunnen worden. Een spijtige ontwikkeling die op korte termijn wellicht uitkomst biedt, maar de toenemende fraude zal op de lange termijn voor een grotere kostenpost zorgen.

Het Verbond van Verzekeraars heeft er wel voor gezorgd dat fraudebestrijding eenvoudiger is geworden. Er is speciale software waarmee fraudeurs kunnen worden aangemerkt op een zwarte lijst. Wanneer deze persoon zich bij een andere verzekeraar aanmeldt, krijgt deze verzekeraar een melding. Op deze wijze kan er rekening gehouden worden met de potentiële risico's die elke klant representeert.

Zorgfraude

Definitie: *Onder zorgfraude verstaan we 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*[26].

Schade: 2-3 miljard

Zorgfraude vindt meestal plaats doordat er onjuiste declaraties ingediend worden. Dit fraudedomein is mogelijk vanwege de rol die ICT hier speelt. De grote hoeveelheid declaraties en inefficiënte fraudedetectiesystemen bieden gelegenheid tot misbruik. De complexiteit van het systeem is dusdanig hoog dat er kwetsbaarheden in optreden die geëxploiteerd worden.

Wel is de zorgsector al georganiseerd in de strijd tegen fraude. 'Zorgverzekeraars Nederland' behartigt de belangen van alle organisaties in Nederland die zorgverzekeringen aanbieden[27].

Jaarlijks wordt bijgehouden voor welke bedragen fraude is verhinderd. In 2010 gaat dat om een bedrag van 6,2 miljoen [Zorgverzekeraars Nederland; 2010]. Daarnaast is er een bedrag van 106,3 miljoen euro aan onjuiste nota's afgewezen. Omdat bij deze tweede post niet kan worden bewezen dat er sprake is van opzet, wordt dit bedrag niet onder de noemer fraude geschaard. Schattingen over het bedrag aan ongedetecteerde fraude ontbreken helaas, maar volgens onderzoek van SAS[28] kan de totale schade aan zorgfraude in Europa worden geschat op 56 miljard euro per jaar [SAS; 2011]. Dit is ongeveer 5% van het totale bedrag dat aan zorg besteed wordt. In Nederland is er een totaal bedrag van 74,5 miljard[29] voor de zorg. Wanneer we een schade van 5% extrapoleren, zou dit neerkomen op 3-4 miljard euro aan fraude per jaar. Andere schattingen gaan uit van 3%-5%, zodat 2-3 miljard euro per jaar mogelijk realistischer is. Dit is natuurlijk een erg ruwe manier van schatten en meer verfijnde meetmethoden zijn nodig voor een betrouwbare schatting.

In de zorgindustrie wordt al veel aandacht besteed aan fraudebeheersing. Preventie gebeurt door het actief informeren van verzekeraars en zorgaanbieders. Verder maakt de industrie gebruik van risicoanalyses en voorlichting [Zorgverzekeraars Nederland; 2010. p. 3]. Daarbovenop past ruim 70% van de zorgverzekeraars geautomatiseerde detectiemethoden toe. Op basis van de informatie verkregen op een seminar van Zorgverzekeraars Nederland (6 april 2011) moet echter worden geconcludeerd dat het hier om relatief primitieve detectiemethoden gaat. Meer geavanceerde modellen zijn in staat om deze detectiegraad flink op te hogen.

Er is in deze sector ook sprake van een groeiende samenwerking. Dit heeft geleid tot de oprichting van een nieuw 'Kenniscentrum Fraudebeheersing in de Zorg' dat als doel zal hebben de samenwerking en informatie-uitwisseling te bevorderen en te coördineren. Dit moet, gegeven de enorme belangen in deze sector, worden toegejuicht.

26 https://www.zn.nl/consumenteninfo/fraude-in-de-zorg/
27 Zorgverzekeraars Nederland. www.zn.nl
28 www.sas.com
29 https://www.zn.nl/branche/feiten-en-cijfers/

OVERHEID

De overheid heeft direct en indirect met fraude te maken. Er is sprake van directe betrokkenheid wanneer bedrijven of burgers frauderen ten koste van de overheid, ook wel verticale fraude genoemd. Hier is bijvoorbeeld sprake van wanneer er misbruik wordt gemaakt van sociale voorzieningen. Indirect heeft de overheid te maken met fraude tussen burgers en/of bedrijven onderling, ook wel horizontale fraude genoemd. Deze vorm van fraude levert geen directe schade op voor de overheid, maar is wel een maatschappelijk probleem. Het creëert een milieu van wantrouwen en heeft invloed op de economie.

Het kabinet heeft zich als doel gesteld om mensen perspectief te geven op fatsoenlijk werk en inkomen en om het draagvlak te behouden voor sociale voorzieningen. Hierbij geldt het principe om iedereen zoveel mogelijk naar vermogen te laten participeren in de samenleving. Burgers zijn bereid om elkaar deze solidariteit te bieden, mede omdat dit ook zorgt voor een vangnet voor henzelf. Wanneer personen onrechtmatig voordeel behalen door middel van fraude, ondergraven zij deze maatschappelijke solidariteit en zal de bereidwilligheid snel afnemen. De maatschappelijke norm dat fraude een ernstige zaak is en als zodanig behandeld moet worden moet dan ook tot uitdrukking worden gebracht in handhaving van uitkeringsregels, arbeidswetgeving en strenge straffen. In het handhavingprogramma 2011-2014 [Rijksoverheid; 2011] staan de belangrijkste aandachtspunten voor een betere informatie-uitwisseling om zodoende de pakkans te verhogen, voor een goede voorlichting en voor een aanscherping van het sanctiebeleid. Fraude zou niet mogen lonen. Dat betekent dat wanneer iemand veroordeeld wordt hij of zij het genoten economisch voordeel in zijn geheel moet terugbetalen en hierbovenop een geldboete krijgt. Deze boete moet in proportie zijn met de misdaad. De bedoeling is dat per 1 juli 2012 de boete 100% van het fraudebedrag is. Op dit moment is dat nog veel minder. Daarnaast krijgen recidivisten oplopende straffen en worden zij uitgesloten van bepaalde rechten of voorzieningen die gebruikt zijn voor het fraudedelict. Dit wordt gedaan met de achterliggende gedachte dat het straffen geen doel op zich is. Er wordt een poging gedaan gedrag te veranderen en fraude te voorkomen.

Naast deze activiteiten in de verticale fraude speelt de overheid ook een belangrijke rol in horizontale fraude. Domeinen zoals faillissementsfraude hebben geen instantie die eindverantwoordelijke is. Bij deze zogenaamde ketenproblemen ontstaat daardoor de perceptie dat er weinig doortastend wordt opgetreden, omdat niemand zich geroepen voelt het voortouw te nemen. In dit soort situaties is de overheid uitermate geschikt als aanjager. De overheid kan bij voldoende signalen vanuit de samenleving – bijvoorbeeld wanneer er een groot aantal aangiftes gedaan wordt – besluiten samenwerkingsbestanden te sluiten met betrokken partijen. Zodoende kan de overheid de toon zetten voor bedrijven in een sector en deze met zich meetrekken.

Zo'n domein is e-fraude. Met het alsmaar toenemende gebruik van internet worden steeds vaker gegevens gestolen via online ingangen. Deze gegevens kunnen dan gebruikt worden om (online of offline) financieel gewin te verkrijgen. De complexe omgeving en de vele schakels die in ICT-systemen zitten zorgen voor veel kwetsbare punten. Als slechts een van deze plekken aangevallen wordt, kan het hele systeem een risico lopen. Een gerucht-makend voorbeeld hiervan heeft zich medio 2011 voorgedaan bij het inlogsysteem van de overheid, DigiD. De software zelf lijkt vooralsnog betrouwbaar te zijn, maar er hoeft maar één onderdeel van de keten kwetsbaar te zijn om het gehele systeem te ondermijnen. Dit kwam goed naar voren toen bleek dat het certificaat dat voor DigiD gebruikt werd was aangetast bij Diginotar. Hierdoor kon worden meegekeken op het moment van inloggen. Met de kennis die nu bekend is en het motief van de dader in ogenschouw genomen lijkt de kans dat er daadwerkelijk schade aangericht is miniem, maar het geeft duidelijk aan hoe een kwetsbare plek een verder betrouwbaar systeem overhoop kan halen. Als de overheid op dergelijke vitale systemen steken

laat vallen, dan is de vraag gerechtvaardigd of dat niet vaker voorkomt.

De overheid heeft wat de online veiligheid betreft twee functies die zij kan uitoefenen. Een preventieve functie waarin zij maatregelen treft die schade voorkomt, en een functie waarin zij gedane schade detecteert en bestraft.

Voorkomen is, ook in dit veld, altijd beter dan genezen. De kosten van het detecteren, corrigeren, compenseren en bestraffen buiten beschouwing gelaten kan ook een vertrouwenscrisis ontstaan als mogelijk gevolg van fraude. Als burgers geen vertrouwen meer hebben in de online beveiliging van de overheid of van particuliere bedrijven, dan zou dit een bureaucratische chaos teweeg brengen. Een overstap van een persoonlijke benadering naar een digitale benadering is efficiënt, maar als door wantrouwen dezelfde stap teruggezet moeten worden, zou dat zorgen voor grote chaos en wanorde. De overheid doet er dus goed aan maatregelen te nemen om fraude te voorkomen. Zij doet dit reeds door haar producten uitvoerig te laten testen voordat ze publiekelijk in gebruik worden genomen, maar sporadisch komen hierin toch missers voor. DigiD is al genoemd. De fout lag hier bij de afgever van het certificaat, Diginotar. Het enige wat de overheid hier verweten kan worden is dat er niet grondig genoeg onderzoek is gedaan naar het bedrijf. Een ander voorbeeld is de OV-chipkaart. Deze bleek snel na de ingebruikname gemakkelijk te kraken. Fraude bleek simpel terwijl de kans op detectie vrijwel nihil is. Wil men ervoor zorgen dat de burgers het vertrouwen houden in nieuwe technologische ontwikkelingen, dan zal ervoor gezorgd moeten worden dat nieuwe producten dusdanig getest en ontwikkeld worden dat dit niet, of in ieder geval niet met het huidige gemak, mogelijk is.

De andere manier waarop de overheid fraude kan voorkomen is door het maatschappelijk besef hiervan aan burgers en bedrijven over te brengen. Een groot gedeelte van de huidige fraudedomeinen is gericht op het verkrijgen van persoonlijke informatie. Deze informatie wordt over het algemeen niet verkregen door ingewikkelde aanvallen op databases, maar door in essentie simpele pogingen tot misleiding in te zetten. Dit kan weliswaar gebeuren met geavanceerde technieken en steeds slimmere software op de achtergrond, maar het principe is erop gericht om personen zelf door middel van misleiding gevoelige informatie door te laten geven. De beste verdediging hiertegen ligt bij de mens zelf. De basis is dat mensen verstandig en veilig internetgedrag moeten vertonen en ook op andere manieren behoedzaam zijn, wanneer zij met potentieel gevoelige informatie omgaan. De overheid is zich hier terdege van bewust, zoals blijkt uit de campagne 'veilig internetten'[30]. In Groot-Brittannië is bestudeerd wat de meest kwetsbare groepen in de samenleving zijn. Met deze informatie en de kennis over met welke praktijken deze groep het meeste risico lopen, kan gerichter worden ingespeeld op risico's.

De andere taak van de overheid bestaat uit detectie en repressie. Hiervoor is het 'Programma Aanpak Cybercriminaliteit' gestart. In dit programma ligt de nadruk op innovatie. Er wordt gezocht naar nieuwe manieren om cybercrime tegen te gaan. Hierbij moet vermeld worden dat cybercrime natuurlijk meer behelst dan alleen e-fraude. Zaken als kinderporno of online heling worden ook door dit programma opgepikt. Een van de drie proeftuinen die in het kader van dit programma zijn opgezet is echter wel specifiek gericht op fraude, namelijk de proeftuin 'internetgerelateerde fraude'. Er zijn op het moment van schrijven nog geen resultaten bekend, maar het zal interessant zijn om de bevindingen in de gaten te houden.

HUIDIGE TECHNIEKEN BIJ FRAUDE EN FRAUDEBEHEERSING

Samenvattend kunnen we concluderen dat er bij de meeste fraudedomeinen een noodzaak aan informatie is die daarna misbruikt wordt. De rol van ICT is hier cruciaal. Het gebruik ervan en de complexiteit die dit met zich meebrengt zorgt voor kwetsbaarheden. De hoeveelheid data op internet

30 www.veiliginternetten.nl

is gigantisch. Deze schat aan informatie heeft aantrekkingskracht op cybercriminelen. Bij vrijwel alle domeinen speelt ICT een rol. Soms slechts als instrument, soms als fundamentele factor.

Persoonlijke gegevens worden online opgespoord en doorverkocht aan geïnteresseerden. Er bestaan speciale markten waar men zich hiermee bezighoudt en de prijs van informatie is niet hoog. De persoonlijke gegevens kunnen gebruikt worden om onschuldige gebruikers te misleiden. Betrouwbaar ogende berichten lokken slachtoffers naar websites met malafide software of naar websites die vrijwel identiek zijn aan die van een officieel bedrijf. De gebruiker staat hier gevoelige informatie af in de veronderstelling dat het om een legitieme website gaat en zo worden gebruikersnamen, wachtwoorden en andere informatie ontfutseld en misbruikt. Er hoeft maar één persoon in een bedrijf te zijn die door deze praktijken wordt misleid. Vervolgens is er een risico dat het gehele systeem risico loopt.

Met de huidige technologieën wordt de mogelijkheid om een vals beeld van de situatie te schetsen steeds groter. Er bestaat software die het beeldscherm dat gebruikers te zien krijgen kan aanpassen. Hierdoor kan bijvoorbeeld een gebruiker die een opdracht via internetbankieren aan de bank geeft, ongemerkt een tweede opdracht hebben verzonden, die de malafide software erin heeft gezet, zonder dat dit terug te zien is in de webbrowser. De klant geeft zijn fiat aan de in zijn ogen correcte betaling en ziet pas later op het papieren afschrift wat er is gebeurd.

In reactie op het toenemend gebruik van ICT bij fraude hebben organisaties die zich bezighouden met fraudebeheersing hun eigen systemen ontwikkeld om dit tegen te gaan.

In een aantal sectoren zien we dat er interne systemen zijn ontwikkeld waarin informatie wordt opgeslagen over fraudeurs. Deze variëren van zeer eenvoudige maatregelen tot uiterst geavanceerde detectiealgoritmen. Er worden zwarte lijsten gecreëerd zodat een persoon die bij één organisatie fraude heeft gepleegd voortaan niet met een blanco strafblad bij een andere organisatie kan binnenkomen. Bedrijven hebben zelf de verantwoordelijkheid om hun klanten te screenen. Deze systemen helpen daarbij. Het is aan organisaties om deze informatie te gebruiken om het risico dat zij ten prooi vallen aan fraude te verkleinen. Bij het creëren van systemen waarin persoonlijke informatie wordt opgeslagen is er altijd een spanningsveld tussen deze systemen en de privacy-wetgeving. Er moet onderzoek gedaan worden naar wat is toegestaan, en wat niet. Wanneer verschillende organisaties binnen een sector samenwerken, kunnen de kosten en de kennis die het oplevert gedeeld worden.

We zien de ontwikkeling van dit soort informatiesystemen nu in meerdere sectoren plaatsvinden. Een samenwerking tussen de verschillende sectoren waarin de sectoren die al meer onderzoek hebben verricht hun ervaringen doorspelen zou kostenbesparend werken, een groter effect sorteren en een vlottere afhandeling bewerkstelligen. Wanneer elke sector voor zich de mogelijkheden en onmogelijkheden onderzoekt – zoals nu gebeurt – is dat verspilling van tijd en middelen.

Wat fraudebeheersing betreft speelt ICT de grootste rol in de fraudedetectie. Er worden programma's gebruikt om risicofactoren op te sporen. Sommige zijn relatief simpel, waarin een A4'tje met een tabel wordt gebruikt om aan te geven of iets in de categorie 'hoge kans op fraude' of in de categorie 'lage kans op fraude' valt. Andere programma's zijn uitgebreider en werken met complexe wiskundige modellen. Speciale teams worden ingezet om deze modellen te ontwikkelen en te implementeren. De programma's detecteren afwijkingen in patronen. Vooral in de private sector zijn deze programma's zeer geavanceerd. Grootste obstakel voor deze programma's blijkt vaak de ruwe data te zijn. Deze is vaak niet direct te gebruiken voor metingen. Wanneer een organisatie of een sector zich vanaf het begin van het proces bewust is van het risico op fraude en nadenkt over manieren om dit te detecteren, zou dit probleem voorkomen kunnen worden. Op dit moment is de volgorde vaak nog

andersom. Pas wanneer er het vermoeden van fraude is, wordt gekeken naar manieren om dat te detecteren. Er is dus een omslag in het denken nodig. Het fraudebewustzijn moet een hogere prioriteit krijgen. Bij nieuwe producten, nieuwe services of de ontwikkeling van nieuwe ICT-systemen moet bij elke stap de mogelijkheid van fraude in het achterhoofd gehouden worden. Wanneer de nadruk op fraudebeheersing ligt, wordt er ook voor gezorgd dat alle data dusdanig opgeslagen wordt dat het direct bruikbaar is, wanneer het vermoeden van fraude bestaat. Onderzoek kan dan snel en kundig plaatsvinden. Communicatie is van essentieel belang hierbij. Uiteindelijk zullen er altijd fraude-experts op het gebied van fraude in een organisatie moeten zijn. Programma's kunnen afwijkende patronen herkennen die met het blote oog niet te vinden zijn, maar het uiteindelijke oordeel over deze afwijkingen moet aan deskundigen worden overgelaten.

Wat bij de analyse van de fraudedomeinen opvalt, is het feit dat er vaak geen betrouwbare cijfers zijn over de totale omvang van de schade door fraude. In sommige gevallen wordt alleen gedetecteerde en voorkomen fraude bijgehouden, in andere gevallen zijn er zelfs helemaal geen schattingen over de totale schade. Dit is een groot tekort. In vrijwel elk domein zijn maatregelen getroffen om fraude tegen te gaan, maar zonder een goede nulmeting kunnen de effecten van deze maatregelen niet worden gemeten. De mate waarin een anti-fraudemaatregel geslaagd is moet dan worden getoetst op basis van anekdotische ervaringen en gevoelsmatige meningen. Bij elke sector waar de totale schade nog niet bekend is moet de prioriteit liggen bij deze metingen. Zonder een nulmeting kan er niet tot een professionele fraudebeheersingsstrategie gekomen worden en zal elke 'triomf' ter discussie staan.

Wanneer we de wijze waarop ICT en andere technieken op dit moment worden ingezet samenvatten kunnen we concluderen dat de frauderende groep zich moeiteloos heeft aangepast aan de opkomst van ICT. De mogelijkheden die dit voor fraudeurs biedt worden volop benut om allerlei gegevens te stelen en vervolgens te misbruiken.

Aan de kant van de fraudebeheersing is dit proces wat later in gang gezet, maar zien we duidelijk dat de verschillende sectoren hiermee bezig zijn. Waar fraudeurs zich echter onbeperkt kunnen richten op innovaties moeten legale organisaties rekening houden met de beperkingen die door de wetgeving worden opgelegd. Om ervoor te zorgen dat deze 'handicap' een zo min mogelijk negatief effect heeft moeten organisaties, bedrijfssectoren en de overheid ervoor kiezen om hun kennis te bundelen. Elke sector is op dit moment bezig met zijn eigen hoekje van fraudebestrijding en vindt daar waardevolle mogelijkheden. Een samenwerking waarin bestaande kennis wordt gedeeld kan leiden tot een win-winsituatie waar alle partijen kunnen profiteren van de ervaringen van de ander. Zulke samenwerkingsverbanden zullen er automatisch toe leiden dat ook het fraudebewustzijn stijgt. Daardoor daalt het risico op fraude. Om dit voor elkaar te krijgen zullen er initiatieven nodig zijn om de stakeholders met elkaar in contact te laten komen. Het besef zal moeten ontstaan dat fraude een delict is dat ons allemaal raakt, en dat we ook samen moeten oplossen.

TOEKOMSTIGE BLIK OP HET VELD

De opkomst van ICT blijft onverminderd doorgaan, maar ook de hoeveelheid opgeslagen data stijgt nog steeds exponentieel. Het aantal uren dat mensen op de een of andere manier met data bezig zijn, via een computer, smartphone of anderszins, neemt nog steeds hand over hand toe. Dit betekent tevens dat de complexiteit van de dataverzamelingen nog steeds exponentieel toeneemt. Daardoor neemt ook de kwetsbaarheid ervan evenredig toe. Bij een ongewijzigd beleid zullen er steeds grotere ontsporingen gaan plaatsvinden. Ontwikkelingen gaan zo snel dat ze bijna niet te volgen zijn. Voorspellingen van enige precisie zijn in dit veld dan ook ondoenlijk. Hoewel het onmogelijk is te zeggen welke invloeden technologische ontwikkelingen zullen hebben, kunnen we de trends van het heden doortrekken naar de toekomst en op basis daarvan verwachtingen formuleren. Daarbij moet wel de kanttekening gemaakt worden dat het altijd mogelijk is dat innovatieve technieken of ontdekkingen kunnen worden gedaan die het hele veld veranderen. Zo zouden bijvoorbeeld de coderingen van het berichtenverkeer van en tussen banken kunnen worden gekraakt, waardoor het hele financiële systeem op zijn grondvesten zou schudden. Er wordt weliswaar gebruik gemaakt van niet kraakbaar geachte 'public cypher'-technologie, maar het is niet ondenkbaar dat ook hiervoor algoritmen kunnen worden ontworpen om deze te ontcijferen. Wiskundig is dit probleem nog niet opgelost, maar er is ook nog niet bewezen dat het een onoplosbaar probleem is.

FRAUDE IN DE TOEKOMST

Het basisprincipe van fraude verandert niet wezenlijk. Het is voor fraudeurs nog steeds zaak informatie te verkrijgen en deze vervolgens zodanig te misbruiken dat er een (financieel) voordeel wordt behaald. Wat wel fundamenteel verandert, is de wijze waarop informatie wordt verkregen. De rol die ICT-systemen hierin spelen is leidend voor verdere ontwikkelingen. Aan de ene kant zorgt de toenemende complexiteit op zichzelf al voor verdere veiligheidsrisico's, aan de andere kant zorgt zij ervoor dat er telkens nieuwe en verbeterde instrumenten voor criminelen ontstaan en nieuwe platformen waarop zij deze kunnen toepassen.

E-fraude heeft de afgelopen jaren een professionaliseringsslag gemaakt. In de vroege jaren van het internet werden pogingen om misbruik van een systeem te maken uitgevoerd door individuen die elk aspect van hun operatie moesten kunnen uitvoeren. Tegenwoordig is er echter sprake van specialisatie. Voor elke stap in het proces kunnen mensen worden ingehuurd. Potentieel waardevolle gegevens zijn simpel en voor weinig geld te koop en er kunnen derden worden ingehuurd om een bepaald stuk code te schrijven, wanneer dat nodig is. Deze verdeling van taken zorgt ervoor dat een fraudeur zich kan specialiseren op één bepaald gebied en hierin zodoende een bepaalde mate van expertise kan ontwikkelen. Deze expertise helpt hem om nieuwe kwetsbaarheden te vinden. Een eerste vereiste voor innovatie is immers het beschikken over voldoende kennis. De innovatiedrang van fraudeurs is indrukwekkend te noemen. Voor elke zwakke plek die gesloten wordt, worden in recordtempo nieuwe kwetsbaarheden ontdekt. In de tijd die het organisaties kost om deze nieuwe kwetsbaarheden weer te repareren hebben kwaadwillenden vrij spel. Het is dweilen met de kraan open.

Er kan vanuit worden gegaan dat deze professionalisering nog verder zal toenemen. Daarmee zullen ook de innovatiemogelijkheden en de geavanceerdheid van de gebruikte methoden toenemen. Zo blijft de 'fraudesector' momenteel steeds een stap voor op de fraudebeheersing.

De wijze waarop systemen worden gekozen als doelwit is vergelijkbaar met de wijze waarop legitieme bedrijven hun strategieën kiezen. Fraudeurs zoeken punten waar de mogelijke winst het grootst en de kans op mislukking het kleinst is. Op deze punten vallen zij de systemen aan. Organisaties die achterlopen ten opzichte van hun concurrenten op het gebied van fraudebeheersing zullen een groter risico lopen. Doordat er een rationele strategie schuilgaat achter het kiezen van doelen, is het mogelijk een analyse van sterke en

zwakke systemen te maken die een indicatie geeft over toekomstige doelwitten. De systemen die erg kwetsbaar zijn en waar de potentiële winst zeer groot is zijn in de toekomst een waarschijnlijke prooi voor fraudeurs.

Grofweg kunnen ontwikkelingen in fraude in twee categorieën worden ingedeeld, namelijk verbreding en verdieping. Verbreding vindt plaats wanneer bestaande fraudetechnieken op een nieuw gebied worden toegepast. Er is sprake van verdieping wanneer fraudetechnieken verder ontwikkeld, geavanceerder en complexer worden.

Verbreding doet zich onder andere voor wanneer een nieuwe technologische ontwikkeling in de maatschappij doordringt. Een recent voorbeeld hiervan is het gebruik van de nieuwe generatie mobiele telefoons, de smartphone. Het is de verwachting dat met ingang van 2013 het aantal mobiele telefoons met internettoegang het aantal computers met internettoegang zal overstijgen. Het gebruik van de mobiele telefoon voor zakelijke transacties zal hierdoor alleen maar toenemen. Gartner[31] voorspelt dat eind 2013 van alle online zakelijke transacties 12,5% via de smartphone zal gaan. Op het moment van schrijven zijn er nog geen massale succesvolle fraudeaanvallen bekend op smartphones, maar er is een toenemend aantal kleine inbreuken die gemeld worden op de verschillende security blogs. Wanneer er toegang wordt verkregen tot andermans smartphone, dan krijgt de inbreker de beschikking over waardevolle gegevens. Opgeslagen wachtwoorden, bankinformatie, sociale media accounts, telefoonnummers en andere waardevolle data liggen dan voor het oprapen. Informatie, geld of zelfs iemand zijn identiteit kunnen gestolen worden! Smartphones hebben de potentie om een zeer waardevol doelwit te worden.

Ondanks de opkomst van het zakelijke gebruik van smartphones is er buiten de gespecialiseerde media maar weinig aandacht voor de risico's die dit met zich meebrengt. De beveiliging van smartphones is over het algemeen nog minimaal. Firewalls en andere anti-virussoftware bestaan, maar worden (te) weinig gebruikt[32]. Waar het bij de persoonlijke computer al jarenlang gemeengoed is om allereerst te zorgen voor een goede firewall en anti-virusscanner lijkt dit besef bij de mobiele telefonie nog niet door te dringen. Zoals Stan Hegt, IT-adviseur van KPMG, zegt: "Het blijft toch mensenwerk en de put wordt vaak pas gedempt als het kalf verdronken is." Generaliserend gesproken lijken mensen nog niet te beseffen dat een smartphone in essentie hetzelfde is als hun persoonlijke computer en dus dezelfde kwetsbaarheden heeft. Gebruikers moeten zich er bewust van zijn dat hun gegevens niet alleen door goede software beschermd kunnen worden. Zij hebben zelf ook de verplichting om zich van het risico op fraude bewust te zijn.

Producenten van software zorgen er soms wel voor dat er extra veiligheidsmaatregelen genomen worden, zoals verscherpte monitoring en een lagere transactielimiet bij de mobiele applicaties van banken, maar beveiliging is een gedeelde verantwoordelijkheid van zowel producenten als gebruikers. Producenten moeten zorgen voor de veilige software, maar gebruikers moeten deze downloaden, up to date houden en malafide websites proberen te vermijden.

Met het groeiende aantal zakelijke transacties die mobiel worden uitgevoerd is de smartphone een nieuwe schakel in de keten van bedrijfsprocessen. Met de geringe beveiliging die er op dit moment is, zal er wanneer het gebruik van smartphones een kritiek punt bereikt, hoogstwaarschijnlijk een piek te zien zijn in het aantal pogingen om gegevens te stelen.

Hebben we dan niets geleerd van het verleden? Dat is te zwaar gesteld. Bedrijven zijn zeer serieus met de beveiliging bezig. Beveiligingssoftware voor de telefoon is al beschikbaar en wordt alleen maar beter. De anti-virussoftware die voor de persoonlijke computer is ontstaan is echter niet bruikbaar voor

31 www.gartner.com. *Gartner Says the Use of Mobile Fraud Detection in Mobile Commerce Environments is Imperative*, 20-9-2010.

32 www.technewsworld.com. *10 Best IT Practices for Smartphone Security*, 15-9-2010.

smartphones, omdat deze een te zware belasting op de batterij pleegt. Ook kunnen deze anti-virusprogramma's nog geen andere applicaties testen[33]. Dit testen gebeurt door de verkopers zelf, maar met het toenemende aantal applicaties en het aantal updates en 'patches' wat daarbij komt is het de vraag in hoeverre dit volledig en nauwkeurig gebeurt. Concluderend betekent dit dat de smartphones van tegenwoordig een waardevol doelwit zijn (en alleen maar meer waard worden) waar de beveiliging nog geen staat van volwassenheid heeft bereikt. Het ligt in de lijn der verwachting dat de fraudesector in de nabije toekomst hiervoor veel aandacht zal hebben.

Willen leveranciers van smartphones ervoor zorgen dat het marktaandeel van hun product blijft groeien, dan zullen zij hieraan extra aandacht moeten besteden. Als er inderdaad een piek komt in het aantal fraudegevallen in deze sector, dan kan dit een vertrouwensbreuk opleveren. Met name het zakelijk gebruik van smartphones zal hier dan onder leiden. Op dit moment is er nog een duidelijke scheiding tussen leveranciers en onafhankelijke partijen die eigen anti-virussoftware en firewalls verkopen. Een samenwerking tussen deze partijen kan een winst opleveren, doordat ze de verantwoordelijkheden kunnen delen. Het is belangrijk om maatregelen te treffen voordat echt serieuze fraudezaken de kop opsteken. Er moet geanticipeerd in plaats van gereageerd worden.

Recentelijk is er naast de smartphone ook een opmars van de zogenaamde 'tablets' gekomen. Het is te vroeg om conclusies te trekken over de beveiliging van de tablet. Vast staat wel dat er meer mogelijkheden zijn qua capaciteit en batterij. De vraag is in hoeverre de gebruiker zelf zorgt voor veilig gedrag. Een tablet heeft op het eerste oog meer gelijkenissen met een persoonlijke computer dan een smartphone. Het is dus voor te stellen dat gebruikers de link tussen de computer en de tablet sneller zullen leggen en daardoor meer geneigd zullen zijn om op de beveiliging te letten, zoals ze al hebben geleerd om dat bij de computer te doen.

De relatief nieuwe ontwikkelingen van smartphones en tablets zijn een interessant fenomeen waar mogelijkheden liggen voor potentiële fraudeurs, maar ook bij andere vormen van e-fraude lijken de fraudeurs in de nabije toekomst het nog voor het zeggen te hebben. Niet al te lang geleden bleken de gegevens van het netwerk van een spelconsolesysteem niet voldoende beveiligd, waardoor creditcardgegevens van 75 miljoen(!)[34] gebruikers kwetsbaar waren. Een ander actueel onderwerp is het Elektronisch Patiëntendossier (EPD). De informatie die hierin moet worden opgeslagen is hoogst gevoelig en kan uitermate waardevol zijn voor fraudeurs. Het is de vraag of de voordelen opwegen tegen de risico's. Het verleden heeft ons steeds weer geleerd dat elektronische systemen inherent niet veilig zijn en dat absolute veiligheid niet gegarandeerd kan worden.

Een belangrijke factor in deze onveiligheid is het gegeven dat de ICT-omgeving uit meerdere structuren bestaat die allemaal onafhankelijk van elkaar ontwikkeld zijn en pas later worden samengevoegd. Met elke toevoeging wordt de ICT-omgeving complexer en komen er meer vlakken die door cybercriminelen kunnen worden aangevallen. Idealiter zou het, vanuit het kader van fraudebeheersing, gewenst zijn om eens in de zoveel tijd het geheel in zijn totaliteit te herschrijven om zodoende een solide systeem te creëren. In de regel kunnen we zeggen dat hoe minder complex een systeem is opgebouwd, hoe minder mogelijkheden een cybercrimineel heeft om aan te vallen.

Tussen de plegers en de bestrijders van fraude bestaat altijd een spanningsveld. Waar de één zoekt naar openingen, probeert de ander constant gaten te dichten. Dit zorgt ervoor dat fraudeurs gedwongen worden steeds geavanceerdere technieken te gebruiken om in bepaalde domeinen te kunnen blijven opereren. Er vindt verdieping plaats. Door de hoge mate van organisatie in criminele organisaties zijn zij in staat fondsen vrij te maken voor onderzoek naar deze geavanceerde digitale aanvalstechnieken. De wijze waarop gegevens worden geaccumuleerd

33 www.bankinfosecurity.com. *Mobile: Combating Malicious Apps*, 23-09-2011.

34 NRC. *Geen financiële schade Sony-gamers*, 27-4-2011.

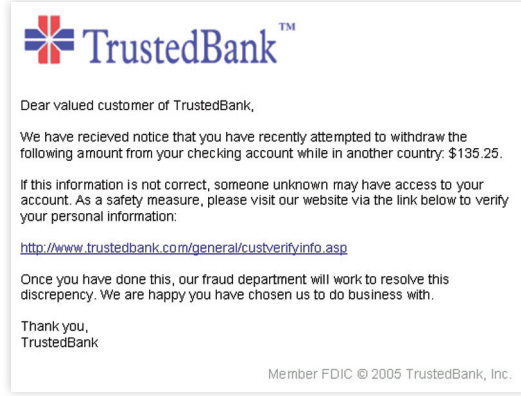
wordt geoptimaliseerd en met toenemende efficiëntie toegepast. Deze nieuwe vindingen zijn door middel van het internet snel te verspreiden (of te verkopen) en zolang een bepaalde exploit nog niet is gerepareerd, hebben cybercriminelen vrij spel om deze te misbruiken voor hun doeleinden.

Wanneer we het stelen van persoonlijke gegevens, waarbij de term 'phishing' het bekendst is, ontleden kunnen drie stappen worden onderscheiden [Hegt; 2008], het aas (1), de haak (2) en de vangst (3).

Het aas is het gedeelte waar deceptie plaats vindt. Een nietsvermoedend persoon of een groep personen krijgt een bericht (vaak in de vorm van een e-mail) waarin de indruk wordt gewekt dat het bericht afkomstig is van een betrouwbare bron. De 'haak' is het punt waar de informatie daadwerkelijk wordt verkregen. Dit gebeurt veelal doordat een gebruiker te goede trouw zijn persoonlijke gegevens, zoals gebruikersnaam en wachtwoord, invult op een website die niet veilig is. Bij punt drie, de vangst, wordt de verkregen informatie ingezet om er (financieel) voordeel mee te behalen. De manier waarop dit gebeurt is afhankelijk van de informatie die is verkregen.

Punt één bestond er oorspronkelijk uit dat het internet werd afgespeurd naar e-mailadressen. Wanneer voldoende van deze adressen verzameld waren, werd een bericht naar een zo groot mogelijk aantal mensen gestuurd om zodoende het aantal potentiële slachtoffers te maximaliseren. De berichten die mensen ontvingen waren vaak amateuristisch opgezet, vol met spelfouten, gemakkelijk te herkennen valse links, niet persoonsgericht en de websites waren duidelijk opgezet met de intentie tot misleiden.

Met het professionaliseren van de fraudesector zal dit tot het verleden behoren. Berichten zullen niet meer te onderscheiden zijn van echte berichten. De kopieën van websites worden steeds beter en na het 'inloggen' word je doorgestuurd naar de betrouwbare echte website, waardoor slachtoffers vaak niet eens weten dat er net iets is gebeurd waardoor hun


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Figuur 1: *Voorbeeld van een poging tot Phishing*

gegevens zijn gestolen. In de toekomst zal het voor zowel beginnende als ervaren computergebruikers alleen maar lastiger worden om het onderscheid te maken tussen echte berichten en pogingen om informatie te verkrijgen. De specialisatie van fraudeurs zorgt ervoor dat phishing-berichten steeds moeilijker te herkennen zijn tot op het punt waarop ze qua uiterlijk niet van echte berichten te onderscheiden zijn.

Een verdere ontwikkeling die fraudeurs hierbij helpt is dat mensen steeds meer persoonlijke informatie online zetten. Voornaamste reden is het massale gebruik van sociale media als Facebook[35], Linkedin[36] en – meer lokaal – Hyves[37]. Op deze sociale media is allerlei waardevolle informatie te vinden over individuen en groepen. Interesses en hobby's worden regelmatig openbaar gemaakt. Hierdoor wordt het gemakkelijker om berichten te personaliseren en wordt het voor gebruikers nog moeilijker om phishing-pogingen te onderscheiden van legitieme berichten. In plaats van de grootschalige pogingen die tot doel hebben om de binnengehaalde hoeveelheid informatie te maximaliseren is er een tendens aan de gang waarbij specifieke doelen

35 *>800 miljoen leden per 11-10-2011* http://www.facebook.com/press/info.php?statistics
36 *>120 miljoen leden per 11-10-2011* http://press.linkedin.com/about
37 *10,3 miljoen leden per 11-10-2011* http://www.hyves.nl/over/facts/

worden uitgezocht die de mogelijkheid bieden van waardevolle informatie. Deze tendens is al enige tijd aan de gang en zal in de toekomst blijven groeien. Dit heeft tot gevolg dat het steeds moeilijker wordt om pogingen tot gegevensdiefstal te doorzien.

Op het tweede punt, de haak, zullen de ontwikkelingen ook verder gaan. Ontwikkelingen van de laatste jaren zijn bijvoorbeeld de 'Man-in-the-Middle'[38], 'Man-in-the-Browser'[39] en 'Boy-in-the-Browser'[40]. Voorgaande voorbeelden zijn manieren waarop informatie wordt gekopieerd of toegevoegd, terwijl de gebruiker hier niet van op de hoogte is. Voor hem lijkt er niets aan de hand te zijn. Op het moment dat de computer of verbinding gecompromitteerd is, is het aan de anti-virussoftware om de malafide software te detecteren. Doordat deze malafide software niet continu opereert, gebeurt dat niet altijd. Aan de voorkant is het aan de gebruikers om ervoor te zorgen dat zij geen gevaarlijk internetgedrag vertonen en niet besmet raken. Aan de andere kant moeten organisaties ervoor zorgen dat zij voor hun producten beveiligingsmaatregelen treffen, waardoor deze methoden niet toepasbaar zijn.

Bij het gebruiken van gestolen gegevens om daadwerkelijk voordeel te verkrijgen is er het minste sprake van verdieping. De toegenomen digitalisering van de samenleving zorgt wel voor een afname van persoonlijk contact bij zakelijke transacties waardoor identificatie veelal plaatsvindt door controlevragen als het BSN (of in de V.S. het 'social security number') in combinatie met andere persoonlijke gegevens. Wanneer deze gegevens in het bezit zijn, kan er een veelvoud aan fraudesoorten gepleegd worden. Creditcards, toeslagen, belasting. Het kan allemaal aangepast worden. De DigiD-code zorgt in Nederland nog voor een extra controle op het digitale vlak (met de mogelijkheid van een tweede authentificatiemethode). Maar omdat meestal ook de mogelijkheid bestaat om ook op papier gegevens door te geven is een vervalste handtekening, die in eerste instantie zelden gecontroleerd wordt tot iemand aan de bel trekt, vaak voldoende om valse aanvragen te doen.

FRAUDEBEHEERSING IN DE TOEKOMST

De wijze van fraudebeheersing hangt in grote mate af van het type fraude. Wanneer het gaat om fraude van buitenaf proberen de belanghebbenden dit meestal zelf op te lossen. Het is in een aantal sectoren maar al te duidelijk dat het onderwerp fraude niet de hoogste prioriteit heeft. Oplossingen worden veelal gezocht in intensivering van de opsporing, maar echt innovatieve toepassingen om fraude te voorkomen ontbreken veelal.

Wanneer er sprake is van (de verdenking van) interne fraude wordt meestal een onafhankelijk audit bureau ingehuurd om de zaak te onderzoeken. Deze bureaus hebben een erg hoog niveau in fraudedetectie. Vooral in deze private sector wordt veel geïnvesteerd in geavanceerde methoden om afwijkingen van normale patronen te identificeren. Deze bedrijven hebben experts in huis die innovatieve manieren ontwikkelen om fraude te detecteren. Een nadeel hiervan is dat de bureaus veelal pas ingehuurd worden, nadat de fraude heeft plaatsgevonden. Er is dus geen sprake van preventie. Deze private bedrijven werken op projectbasis en ontwikkelen hun methode al naargelang de situatie. De expertise die deze bedrijven in huis hebben wordt vaak gemist bij bedrijfssectoren of bij de overheid waar fraude niet het hoofdproduct is, maar slechts een nare bijkomstigheid.

De aanpak van fraude kan echter niet uitsluitend met nieuwe technologieën worden bestreden. Het detecteren van afwijkingen in data is niet voldoende. Gerben Schreurs, partner bij de Forensic-afdeling van KPMG, geeft aan dat fraudebeheersing tegenwoordig vanuit meerdere disciplines plaatsvindt. Gespecialiseerde teams bestaan uit mensen met een achtergrond in een veelvoud van disciplines waaronder kunstmatige intelligentie, technische informatica, bedrijfskunde, wiskunde. De aanpak van fraude bestaat tegenwoordig uit

38 https://www.owasp.org/index.php/*Man-in-the-middle_attack*
39 https://www.owasp.org/index.php/*Man-in-the-browser_attack*
40 http://resources.infosecinstitute.org/imperva%E2%80%99s-*amichai-shulman-discusses-the-boy-in-the-browser-attack/*

meer dan slechts data-analyse en kan met recht multidisciplinair worden genoemd.

Het professionalisme van de private sector is in veel sectoren die een poging doen om fraude tegen te gaan, nog niet aanwezig. Wat fraudedetectie betreft zou het een goede stap zijn voor de verschillende samenwerkingsbestanden die al ontstaan zijn om met deze private bedrijven samen te werken en kennis te delen. De teams die hier werken hebben veel ervaring en kunnen waar nodig innoveren. De methoden die nu gebruikt worden bij interne controles zijn wellicht niet direct toepasbaar op bijvoorbeeld acquisitiefraude, maar de manier waarop wordt gezocht naar oplossingen is een proces dat overal toepasbaar is.

Het detecteren van fraude alleen is echter niet voldoende. Het uiteindelijke doel is het streven naar preventie. Fraudedetectie speelt hier natuurlijk wel een belangrijke rol in aangezien een hoge graad van detectie een afschrikwekkend effect heeft, maar er zijn ook andere ontwikkelingen die moeten plaatsvinden. Op dit moment zijn er al interne databases ontwikkeld (en in ontwikkeling) waar meldingen over fraudeurs opgeslagen kunnen worden en waaruit organisaties relevante data kunnen halen, waardoor zij het principe 'Customer Due Diligence[41]' kunnen toepassen. Deze databases zullen in de toekomst meer gaan voorkomen en maken het voor fraudeurs moeilijker om hun delicten te herhalen. Er zitten echter wel een aantal uitdagingen aan het ontwikkelen van deze databases.

Ze moeten ten eerste zodanig worden ontworpen dat zij niet toegankelijk zijn voor buitenstaanders. Zoals we al eerder hebben gezien, is dit een obstakel omdat absolute veiligheid niet gegarandeerd kan worden. Ten tweede moeten zij dusdanig ingedeeld zijn dat ieder alleen maar toegang heeft tot de gegevens die hij mag inzien en dat leidt tot het derde punt. Wat betreft het delen van informatie is er altijd het 'gevaar' dat men de regels overtreedt zoals die worden opgesteld door het 'College Bescherming Persoonsgegevens' (CBP). Het ontwikkelen van dergelijke software, maar ook het verkrijgen van kennis over wat wel en niet is toegestaan bij het delen van persoonlijke informatie is een tijdrovend proces. Wanneer dit gecoördineerd zou worden vanuit meer samenwerking, zal dit een concreet resultaat opleveren voor een grote groep belanghebbenden, waar er anders niets zou gebeuren vanwege de te hoge kosten.

Zoals al eerder vermeld, zorgt een hogere mate van complexiteit voor een groter risico op fraude. Immers, elke toegevoegde keten is een nieuwe potentiële zwakke plek die aangevallen kan worden. Vanwege constante toevoegingen en uitbreidingen worden systemen met de jaren steeds complexer en dus kwetsbaarder. Dit geldt vooral voor ICT-systemen. Een voor de hand liggende oplossing is om een systeem na een aantal jaar vanaf het begin te herprogrammeren, intussen rekening houdend met alle nieuwe functies om zodoende een minder complexe versie van het systeem te krijgen. Veiligheidsstandaarden moeten dan wel op alle niveaus worden geïmplementeerd. Zowel hardware als software, waar ook 'compilers' en operating systems onder vallen, moeten op elkaar worden afgestemd. Gebeurt dit niet, dan zorgt de interactie die tussen al deze verschillende systemen ontstaat voor nieuwe kwetsbaarheden. Er is behoefte aan standaarden waarop men zich kan richten.

Een andere optie is om de zwakste ketens te versterken. Technologisch gezien gebeurt dit al. Regelmatig komen patches en updates uit die de nieuwste veiligheidslekken dichten. Dit lijkt een eeuwigdurende cirkel te worden tussen fraudeurs en fraudebestrijders. Zolang de opgelopen schade en de kosten van het telkens repareren van beveiligingslekken kleiner zijn dan de kosten van een grootschalige herstructurering, zal dit niet veranderen maar het deconstrueren van complexe systemen lijkt op de lange termijn een reële mogelijkheid om systemen veiliger te maken.

Een factor waaraan nog veel extra aandacht moet worden besteed is de menselijke factor. Werknemers

41 Het principe dat organisaties zorgvuldig zijn in de klanten die zij aannemen.

of gebruikers zijn zich vaak niet bewust van het feit dat informatie voor schadelijke doeleinden kan worden gebruikt. Een van de beroemdste 'hackers'[42] van het afgelopen decennium, Kevin Mitnick, geeft in zijn boek [Mitnick & Simon; 2003] aan hoe hij door sociaal contact aan veelal onschuldige stukjes informatie kwam en deze gebruikte om medewerkers steeds meer waardevolle en gevoelige informatie af te troggelen, een methode die hij 'social engineering' noemt. Om deze praktijken te voorkomen moet het fraudebewustzijn van burgers en werknemers omhoog. Met name voor werknemers zijn er mogelijkheden om dit met behulp van technologische hulpmiddelen te bereiken. Een techniek die in opkomst is, is 'serious gaming'[43]. Dit zijn games waarbij wordt getracht op een speelse manier bepaalde serieuze doelstellingen te behalen. Het is voor te stellen dat er een game wordt ontworpen waarbij werknemers voorschriften krijgen te verwerken over het uitgeven van informatie, uitleg krijgen over malafide websites en e-mails en in het algemeen leren veilig gedrag te vertonen. Wanneer de menselijke factor wordt versterkt, zal dit een drempel opwerpen voor potentiële fraudeurs voor het verkrijgen van gevoelige informatie. Serious gaming kan een uitermate geschikt middel zijn om hieraan bij te dragen.

Naast het fraudebewustzijn van werknemers moeten de eindgebruikers ook rekening houden met hun eigen veiligheid. Mensen gebruiken voor belangrijke zaken al regelmatig dubbele identificatiemethoden. Tegenwoordig bestaan deze meestal nog uit het beantwoorden van een aantal persoonlijke vragen of door het invoeren van een gebruikersnaam en wachtwoord, waarbij een tweede middel zoals een code via sms wordt gebruikt voor extra controle. Een techniek die daarnaast in opmars is, is het identificeren van mensen via 'biometrics'. Dit gebeurt onder andere door middel van irisscans, vingerafdrukken of spraakherkenning. Hoewel deze extra controle een extra drempel is, ontstaat wel het risico dat misdadigers over gaan tot kidnapping of andere serieuzere misdrijven om toegang te verkrijgen. Zo zijn er verhalen bekend over auto's die een slot hebben dat reageert op de vingerafdruk van de eigenaar en waar misdadigers de vinger van de eigenaar hebben afgesneden om toegang tot de wagen te krijgen[44].

42 'Hacker' is in feite niet de juiste term, aangezien een hacker oorspronkelijk niet tot doel heeft om schade te veroorzaken of financieel voordeel te vergaren, maar in populair taalgebruik is dit de meest herkenbare term. Vandaar dat we deze term hier gebruiken.
43 Zie ook de verkenning van STT over serious gaming. http://www.stt.nl/uploads/documents/219.pdf. Of www.seriousgames.tv

44 BBC News. *Malaysia Car Thieves Steal Finger*, 31-05-2005.

HET BUITENLAND

In de voorafgaande hoofdstukken is voornamelijk uitgegaan van het Nederlandse perspectief. In het buitenland hebben overheden last van hetzelfde probleem en vanwege de wereldwijde economische recessie is fraude een kwestie waaraan overal serieus aandacht wordt besteed. Met de grotere rol van cybercrime in fraude is ook de internationalisering van fraude een groter probleem geworden.

Waar fraude vroeger voornamelijk regionaal optrad, is dit niet langer het geval. Een cybercrimineel uit land A kan gegevens stelen in land B, ze vervolgens verkopen aan een ander in land C en vervolgens wordt er misbruik van gemaakt in land D. Vanwege deze internationalisatie is er ook een internationale aanpak van fraude nodig. Langzamerhand zien we dat verschillende landen gaan samenwerken bij het oppakken van sommige van de grootste zaken, maar wat de kleinere fraudevergrijpen betreft is hier nog geen sprake van. Europol vervult hier een belangrijke functie, maar ook daar zijn te weinig fondsen beschikbaar voor efficiënte procedures, laat staan dat landen zich door die organisatie de wet laten voorschrijven.

Naast deze internationale samenwerking zien we ook dat sommige landen speciale strategieën ontwikkelen om fraude tegen te gaan.

In Groot-Brittannië is in 2006 een onderzoek gedaan naar fraude waaruit een aantal problemen naar voren kwamen[45].

- Er was geen eenduidige manier waarop fraude gemeten werd.
- Het rapporteren van fraude gebeurde niet naar behoren.
- De aanpak door justitie van fraudezaken duurde te lang en was inefficiënt.

Deze drie punten zijn problemen die niet alleen in Groot-Brittannië voorkomen, maar waar we zelf ook mee te maken hebben en die ook in andere landen terug te zien zijn.

Als reactie op dit rapport werd de National Fraud Authority opgericht. Het allereerste punt waar zij zich mee bezighield was om betrouwbare meetmethoden te implementeren. Om dit voor elkaar te krijgen werd in alle sectoren onderzoek gedaan naar hun methoden en deze kennis werd daarna gedeeld. De totale schade werd vóór de NFA opgericht werd, geschat op 12 miljard euro. Met de implementatie van nieuwe meetmethoden wordt deze tegenwoordig geschat op 38 miljard euro per jaar. De verwachting is nog steeds dat dit een grove onderschatting van de werkelijkheid is.

Door de methoden van fraudemeting met elkaar te delen werd al een begin gemaakt met het verhogen van het fraudebewustzijn bij de overheid en bij andere sectoren. Een volgende punt waaraan gewerkt werd was dat elke afdeling een groep had die verantwoordelijk was voor de eigen fraudebeheersing. Zo werd door een continue samenwerking, het delen van kennis en 'best practices' het fraudebewustzijn steeds hoger. De factor communicatie staat hoog op de prioriteitenlijst van de NFA.

De taak van de NFA is dan ook niet om zelf fraude te bestrijden, maar om de verschillende sectoren te coördineren. Een belangrijk citaat uit het onderzoek van 2006 is het uitgangspunt van de organisatie.

"A lot of organizations have anti-fraud roles but there is no overall coordination of effort, which leads to overlap and gaps. A national strategy would be directed at ensuring the whole was greater, rather than less than the sum of parts." [Attorney General Office; 2006]

Een andere aanpak is te vinden in België. Daar is in 2008 Carl Devlies aangesteld als staatssecretaris voor de coördinatie van fraudebestrijding[46]. Onder zijn leiding zijn actieplannen opgesteld om fraude tegen te gaan. De nadruk ligt ook hierbij op de samenwerking tussen de verschillende sectoren. Uit een onderzoek dat is uitgevoerd door Devlies blijkt dat ook in België de nadruk allereerst ligt op het verkrijgen van eenduidige meetmethoden

45 http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/

46 http://www.carldevlies.be/nl/

en schadebedragen die beargumenteerd kunnen worden [Schoorens; 2010]. Wanneer deze nulmetingen bekend zijn, moet er een centraal punt komen waar deze informatie opgeslagen en gedeeld kan worden met andere belangstellenden.

Wat opvalt wanneer verscheidene landen worden vergeleken, is de nadruk op betrouwbare meet-methoden en samenwerking tussen de sectoren. Deze landen vinden het van essentieel belang dat er sprake is van coördinatie tussen alle partijen en dat er een cultuur van informatie-uitwisseling ontstaat.

AFSLUITEND

Dit document is bedoeld om een blik op het huidige veld en inzicht in een mogelijke toekomst te geven. Conclusies over het pad dat moet worden bewandeld, worden hier niet getrokken. Dit kan alleen worden gedaan door de belanghebbende partijen in het veld zelf.

Op dit moment is er een groeiende aandacht voor fraudebeheersing en dit geeft hoop voor de toekomst. De manier waarop deze groei plaatsvindt is echter gefragmenteerd en niet erg efficiënt. De rol die ICT speelt in zowel fraude als fraudebeheersing is van vitaal belang. Er is veel kennis beschikbaar, maar deze wordt nog te weinig gedeeld. Organisaties moeten zich realiseren dat fraude geen punt is waar de concurrentie met elkaar moet worden aangegaan, maar juist het punt waarop men moet samenwerken. In andere landen zien we al een stap in de richting van een gecoördineerde samenwerking waarbij de unieke aanpak van iedere individuele sector in zijn waarde wordt gelaten, maar waar kennis, informatie en middelen worden gedeeld om tot een som te komen die groter is dan alle delen afzonderlijk. Of deze situatie ook wenselijk is in Nederland zal moeten worden bepaald in overleg met de verschillende industrieën, politici, wetenschappers en de overheid, maar is het overdenken waard. Fraude is immers een probleem dat alle sectoren van de samenleving treft en daarom zullen alle sectoren mee moeten werken om tot een oplossing te komen. Hoe dan ook, samenbundeling van kennis en inzichten en beleidsuitvoering is een eerste prioriteit.

STICHTING TOEKOMSTBEELD DER TECHNIEK

De Stichting Toekomstbeeld der Techniek (STT) organiseert al ruim 40 jaar brede, participatieve lange termijn toekomstverkenningen op het snijvlak van technologie en samenleving. De stichting biedt daartoe een vrije ruimte waarin enthousiaste belanghebbenden elkaar ontmoeten en op creatieve wijze toekomstbeelden bouwen. Daaruit komen inspirerende visies op de toekomst van techniek en maatschappij. De producten van de STT-verkenningen worden breed gewaardeerd door de gebruikers die ook bij de verkenningen betrokken worden. Dat zijn bijvoorbeeld de overheid en het bedrijfsleven, maar ook de onderzoekswereld en maatschappelijke groeperingen. Het gaat bij de resultaten niet alleen om bijdragen aan visievorming of beleidsontwikkeling en agenda's voor de toekomst. Uit de toekomstverkenningen komen bijvoorbeeld ook onderzoeksprogramma's, netwerken of instituten voort, waarvoor de basis al tijdens de verkenningen wordt gelegd.

Naast toekomstverkenningen en Horizonscans ontplooit de stichting vanuit de STT-Academy een aantal complementaire activiteiten:

- De co-financiering van een aantal bijzondere leerstoelen en het faciliteren van de inzet van studenten bij toekomstverkenningen.
- Het beheer van een nationale verkenningendatabase (TV-online) waarin naast verkenningen van STT ook studies van andere verkennende instanties (ook bedrijfsleven) worden geplaatst.
- De organisatie van masterclasses en seminars voor de disseminatie van uitkomsten van verkenningen en methodiekstudies en voor netwerkvorming.
- Het beheer van het Netwerk Toekomstverkenningen dat sinds 1974 een platform vormt voor kennisuitwisseling over toekomstverkenningen en over thema's van STT-verkenningen. Het NTV heeft ruim 60 leden uit het bedrijfsleven, universiteiten, overheid en maatschappelijke instellingen.

Het Algemeen Bestuur van STT bestaat uit ruim 35 personen uit de top van de overheid, het bedrijfsleven, de onderzoekswereld en maatschappelijke organisaties.

STT is een non-profitorganisatie. De activiteiten worden gefinancierd met bijdragen van de overheid en het bedrijfsleven.

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

Bezoekadres: Prinsessegracht 23, 2514 AP Den Haag
Postadres: Postbus 30424, 2500 GK Den Haag
Tel. 070-302 98 30

info@stt.nl

Stichting Toekomstbeeld der Techniek

STT Academy

UNIVERSITEIT TWENTE

Universiteit Twente. De plek waar talent zich het best ontplooit. Studenten en medewerkers staan centraal. 3.300 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 700 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 50

Universiteit Twente, de ondernemende universiteit.

BRONNEN

- Attorney General Office (2006). *Fraud Review.* Final Report
- De Nederlandse Bank. *Q&A Veilig bankieren.* pc 14-11-2011
- Dobbelaere, M. (2010). *Identity Theft in de ICT. Onderzoek naar de wenselijkheid van een Belgische en/of Europese regelgeving.* Mylex, p. 72
- Javelin Strategy and Research (2011). *2011, Identity Fraud Survey Report*
- Geldrop, A.J. van (2011). *Indicators of Bankrupcy Fraud*. Universiteit Twente
- Hegt, S. (2008). *Analysis of Current and Future Phishing Attacks on Internet Banking Services*. Technische Universiteit Eindhoven
- HM Revenue & Customs (2011). *Measuring the Tax Gap*, 2011
- Knegt, R., Beukelman, A.M., Popma, J.R., Willigenburg, P., Zaal, I. van (2005). *Fraude en misbruik bij faillissement: een onderzoek naar hun aard en omvang en de mogelijkheden van bestrijding.* Hugo Sinzheimer Instituut, Amsterdam
- Mitnick, K., Simon, W. (2003). *The Art of Deception: Controlling the Human Element of Security*
- Rijksoverheid (2011). *Handhavingprogramma* 2011-2014
- Roest, F. (2007). *Beleggen in gebakken lucht.* Functioneel Parket Openbaar Ministerie
- SAS (2011). *Future Bright: Fighting Fraud*
- Schermer, B.W., Wagemans, T. (2009). *Onze digitale schaduw*
- Schimmel, P. (2004). *Fraudebeheersing: hoe doe je dat?*
- Schneider, F. (2010). *The Shadow Economy in Europe*
- Schoorens. G. (2010). *Naar een nationale strategische aanpak van de strijd tegen fraude.* Openbaar Ministerie (België)
- Steunpunt AcquisitieFraude (2009). *Protocol*
- Tromp, N., Snippe, J., Bieleman, B., Bie, E. de (2010). *Preventieve maatregelen horizontale fraude.* WODC
- Veldkamp, B.P., Vries, T. de (2008). *Identification of Bankruptcy Fraud in Dutch Organizations.* Universiteit Twente
- Verbond van Verzekeraars (1998). *Fraudeprotocol*
- Vries, E.A. de (2007). *Identiteitsfraude: een afbakening*. Boom Juridische uitgevers, Den Haag
- Zorgverzekeraars Nederland (2010). *Fraudebestrijding in de zorg – Resultaten 2010*