

Fraude en het Internet

Standpunt van de
Stichting Maatschappij, Veiligheid en Politie

Wat doet SMVP?

Een goed functionerende veiligheidszorg is van groot belang voor iedereen. Ontwikkelingen in de samenleving vereisen een voortdurende bezinning door alle betrokken partijen. Nieuwe ideeën op dit gebied verdienen steun en stimulans. Om tot optimale communicatie te komen tussen allen die het aangaat is een aanjager nodig.

De Stichting Maatschappij, Veiligheid en Politie wil die rol op zich nemen. De missie van de stichting is bij te dragen aan de maatschappelijke discussie over de verbetering van de veiligheid(szorg) in de breedste zin. Zij doet dit onder meer door meningen te formuleren over belangrijke thema's, door partijen bijeen te brengen, door vernieuwing te stimuleren, door conferenties, symposia en uitwisselingsprogramma's te organiseren en door achtergrondinformatie te verstrekken.

Fraude en het Internet

Standpunt van de Stichting Maatschappij, Veiligheid en Politie

Dordrecht, maart 1999

Inleiding

In haar rapport *Toekomst gezocht* stelt de Stichting Maatschappij, Veiligheid en Politie (SMVP) voor aandacht te besteden aan thema's waarvan kan worden verwacht dat zij in de toekomst een probleem kunnen gaan vormen voor de veiligheid. Een thema dat zich in dat verband leent voor een nadere bestudering is fraude bij het elektronische betalingsverkeer via het Internet. Het bestuur van de SMVP vroeg een projectgroep haar te adviseren over de verwachte ontwikkelingen op dat terrein en over de stappen die kunnen worden genomen om potentiële risico's terug te dringen. Deze projectgroep vervaardigde het rapport *Achtergronden van Internetfraude*. Dit rapport bevat een brede achtergrondbeschouwing van de problematiek. Het geeft een beeld van relevante ontwikkelingen en het benoemt terreinen waarop acties noodzakelijk zijn. Het rapport is bestemd voor een brede kring van geïnteresseerden, met name voor hen die niet zijn gespecialiseerd in deze problematiek maar daarvoor wel belangstelling hebben.

Op basis van het rapport van de projectgroep hebben verschillende malen discussies binnen het bestuur van de SMVP plaatsgevonden. Deze discussies hebben geleid tot het standpunt dat thans voor u ligt, getiteld *Fraude en het Internet*. In dit standpunt doet de SMVP een aantal aanbevelingen die naar haar mening van belang zijn om in de toekomst de risico's op financieel terrein zoveel mogelijk te beperken. In de visie van de stichting moet er, om de gesignaleerde problemen het hoofd te bieden, een aantal concrete stappen worden gezet. Daarnaast acht de stichting over een aantal vraagstukken een nadere maatschappelijke discussie noodzakelijk. Het rapport van de projectgroep is afzonderlijk gepubliceerd.*

Het Internet

Elektronische informatie-uitwisseling speelt een steeds grotere rol bij communicatie in onze samenleving. Het Internet is het belangrijkste elektronische open communicatienetwerk op dit moment. Los van de uitwisseling van informatie speelt het Internet ook een in belang toenemende rol bij zakelijke transacties en het daaraan verbonden betalingsverkeer. In het bedrijfsleven worden daarvoor de laatste jaren op grote schaal nieuwe toepassingen ontwikkeld. De verwachting is dat het betalingsverkeer via Internet in de nabije toekomst flink zal groeien.

Veel mensen maken zich zorgen over de mogelijke gevolgen van deze ontwikkeling. Wat zijn de maatschappelijke gevolgen ervan? Wat zijn de kansen en bedreigingen? Zijn er gevaren dat criminelen met behulp van het Internet hun slag slaan, bijvoorbeeld door het plegen van fraude? Kan het Internet worden gebruikt voor witwassen? En als dat het geval is, hoe kan de samenleving zich daartegen beschermen? Zonder enige twijfel brengt de groei van het betalingsverkeer via het Internet extra risico's met zich mee. Daaraan liggen drie redenen ten grondslag.

In de eerste plaats betreft dit de omvang van het netwerk en de massaliteit van het gebruik. Die geven aan iedere gebruiker de mogelijkheid om anoniem te blijven, hetgeen

* Beide publicaties werden in conceptvorm besproken op een expertconferentie, waaraan werd deelgenomen door deskundigen uit diverse maatschappelijke geledingen (politie, openbaar ministerie, bestuur, departementen, banken, wetenschap).

betekent dat de authenticiteit van personen die via het Internet communiceren niet kan worden vastgesteld en men dus nooit weet met wie men 'zaken doet'.

In de tweede plaats speelt de open structuur van het netwerk een rol. Communicatie is onversluierd leesbaar en in principe ook door derden te wijzigen. Zo is onder meer de naam waaronder men aan het Internetverkeer deelneemt vatbaar voor manipulatie. Door het ontbreken van een controlerend of regulerend orgaan is het Internet een ongebonden communicatiemedium. Juist in verband hiermee hebben de Nederlandse financiële instellingen een eigen regulerend orgaan in het leven geroepen: Interpay. Naarmate een groter deel van de (financiële) handelingen verschuiven van bancaire instellingen naar klanten (thuisbankieren), zullen echter naar verwachting de controlemogelijkheden van financiële instellingen in de toekomst verminderen.

In de derde plaats kan worden gewezen op het wereldomspannende karakter van het Internet. Als gevolg daarvan wordt de uitoefening van de rechtsmacht van nationale overheden in toenemende mate problematisch. Een van de problemen van het Internet is, dat de locatie waar een handeling plaatsvindt en de locatie waar die handeling tot (rechts)-gevolgen leidt ver uiteen kunnen liggen. Zelfs als duidelijk is waar een bepaalde handeling juridisch wordt gepleegd, dan is het nog de vraag of de rechtsmacht van een bepaalde overheid zich tot die handeling uitstrekt. Dit probleem speelt vooral bij delicten die in het ene land verboden zijn en in het andere niet. De (vooral op nationale leest geschoeide) juridische werkelijkheid loopt achter bij de virtualisering van de samenleving. Zolang Nederlandse gebruikers via Nederlandse providers aan het Internetverkeer deelnemen is de juridische positie gewoonlijk helder en leveren controle- en handhavingsvraagstukken hooguit praktische problemen op. Maar niets verbiedt hen om gebruik te maken van de diensten van een provider op bijvoorbeeld Antigua met wie zij, eventueel zelfs via een open lijn, in verbinding staan. En dan is elke vorm van controle een illusie.

Risico's van het Internet

Een belangrijk deel van de potentiële gevaren van het Internet lijkt niet zozeer een gevolg te zijn van criminele handelingen maar van risicogedrag. Juist door de anonimiteit en de massaliteit trekt het Internet bepaalde typen gelukzoekers aan. Zo biedt het Internet veel mogelijkheden tot gokspelen, waaronder loterijen en piramidespelen. Waar de overheid van oudsher (publiekelijk) gokken heeft willen reguleren door middel van de Wet op de Kansspelen, zal dat bij gokspelen via het Internet moeilijk zijn. Men kan 'openbaar gokken' vanuit de leunstoel. Juist omdat deze gokspelen veelal internationaal plaatsvinden, is de mogelijkheid van controle voor nationale overheden beperkt. Een ander type risicogedrag is marktmanipulatie. Wat vroeger plaatsvond via telefoonverbindingen, gebeurt thans (naar het zich laat aanzien vooralsnog op beperkte schaal) via babbelboxen op het Internet, zoals bijvoorbeeld het agressief promoten van aandelentransacties. Soms gaat het daarbij om gewone handel (die niet strafbaar is, maar wel zeer risicovol), soms is ook sprake van oplichting of verduistering (zie hierover meer uitgebreid de SMVP-publicaties *Financiële Integriteit* uit 1995 en *Beursfraude en zelfregulering* uit 1996).

Het Internet speelt wel degelijk ook een rol bij criminaliteit. In de pers wordt de laatste tijd veel aandacht besteed aan verschillende vormen van criminaliteit. Zo leest men met enige regelmaat over onderwerpen als (kinder-)pornografie, het ontduiken van auteursrecht, belastingfraude, smaad, belediging, het saboteren van computersystemen door virussen of door zogenaamde elektronische bombardementen (het zenden van zoveel berichten dat het systeem uitvalt). Zeker als deze delicten internationaal worden gepleegd zijn zij moeilijk te bestrijden, laat staan te voorkomen. Wel blijken opsporingsinstanties in toenemende mate vaardigheid te verwerven om met gebruikmaking van de gegevens van potentiële verdachten die op het net zelf te vinden zijn tot strafrechtelijke resultaten te komen.

Financiële criminaliteit

In dit standpunt van de SMVP staat de financiële criminaliteit centraal. Er is weinig informatie beschikbaar over de aard en omvang van financiële criminaliteit op het Internet. Bovendien is de bestaande kennis sterk gefragmenteerd. Desondanks lijkt de uitspraak gerechtvaardigd dat er op dit moment weliswaar sprake is van financiële criminaliteit, soms zelfs met aanzienlijke schade, zonder dat er, op dit moment althans, moet worden gesproken van een onbeheersbare groei van deze misdaad. Voor zover de informatie thans strekt, is het vooral fraude dat een substantieel probleem vormt. Het gaat vooral om vormen van fraude met creditcards door middel van het gebruik van valse nummers, dan wel het onrechtmatige gebruik van bestaande nummers. Juist het open karakter van het net heeft tot gevolg dat misbruik van nummers die in aangesloten systemen zijn opgeslagen mogelijk is. De schade als gevolg van fraude belooft jaarlijks vele miljoenen guldens. Fraude doet zich ook voor in de sfeer van de belastingontduiking, met name de BTW. Door illegaal kopiëren en door het rechtstreeks aanschaffen van goederen in het buitenland loopt de staat ook over een breed front belastinginkomsten mis. Een tweede vorm van misdaad is het doen van niet gelegitimeerde overschrijvingen door middel van inbreken in computers. Van beide vormen van misdrijven zijn tal van voorbeelden uit de literatuur bekend. Met de groei van het internationale betalingsverkeer via het Internet zullen deze vormen van criminaliteit naar verwachting toenemen.

Over eventueel gebruik van het Internet voor witwasactiviteiten zijn geen gegevens voorhanden. Toch lijkt hier geen reden tot bovenmatige bezorgdheid, tenminste voorzover het gaat om de geldstromen die via de Nederlandse financiële instellingen lopen. De risico's bij Internettransacties zijn vergelijkbaar met transacties via het girale betalingsverkeer. Op dit moment lopen in Nederland alle financiële transacties nog via de banken. De banken zijn verplicht, net zoals in het gewone betalingsverkeer, De Nederlandsche Bank over buitenlandse betalingen te informeren en eventuele ongebruikelijke transacties door te geven aan het Meldpunt Ongebruikelijke Transacties. Echt nieuw is het betalen met elektronisch geld (e-cash). Tot dusverre wordt daarvan relatief weinig gebruik gemaakt en onder zeer strikte controle van de banken. Er zijn geen gevallen van misbruik bekend.

Juist de centrale rol die de reguliere bankwereld (thans nog) speelt, maakt dat de risico's van verschillende vormen van financiële criminaliteit beperkt zijn. Voor in principe alle financiële delicten geldt dat deze naar verwachting substantieel zullen toenemen zodra rechtstreekse betalingen tussen particulieren mogelijk worden. Men dient zich overigens wel te realiseren dat de meeste vormen van financiële criminaliteit niet specifiek zijn voor het Internet. Het is geen nieuw type misdaad. Het gaat vooral om traditionele vermogenscriminaliteit in een nieuw jasje. Internet maakt nieuwe modaliteiten van oude misdaad mogelijk. Duidelijk is wel dat er steeds weer nieuwe, en vaak zeer inventieve, mogelijkheden worden ontdekt om te eigen bate informatie te 'manipuleren' waarmee op oneerlijke manier geld wordt verkregen. Er bestaat nog lang geen zicht op alle mogelijkheden en er zullen naar verwachting de komende jaren steeds weer nieuwe mogelijkheden bijkomen. Dat betekent dat het onderwerp permanente aandacht vereist.

Bij een dergelijke schets van potentiële gevaren is men licht geneigd te vergeten dat er tegenwoordig al heel veel wordt gekocht en gehandeld via het Internet (boeken, CD's), en dat dit vrijwel zonder uitzondering probleemloos verloopt voor de betrokken partijen. Het feit dat er een aparte organisatie bestaat die als regulerend orgaan optreedt bij het financiële verkeer speelt daarbij, althans voor transacties die in Nederland plaatsvinden, een grote rol.

Risico's voor de toekomst

De belangrijkste risico's voor de nabije toekomst lijken vooral te worden gevormd door:

1. De mogelijkheid van rechtstreekse betaling van (chip)kaart naar (chip)kaart, zeker als de bedragen die kunnen worden overgeschreven substantieel toenemen. Het gevolg hiervan is immers dat de regulering die thans door de financiële instellingen wordt verricht niet meer mogelijk is.
2. Een toename van het Internetverkeer vanuit Nederland via in het buitenland gevestigde providers, zeker als deze gevestigd zijn in landen waar het met de regelgeving niet zo nauw wordt genomen. Dergelijk elektronisch verkeer onttrekt zich aan elke waarneming en elke vorm van controle.
3. De groei van het gebruik van de encryptie (sleutels die berichten onleesbaar maken voor derden). Hoe belangrijk encryptie op zichzelf ook is, het zal betekenen dat een toenemend deel van het berichtenverkeer door de overheid niet meer kan worden onderschept. De huidige afspraken die zijn gemaakt om het gebruik van encryptie te beperken, zal een slimme crimineel er niet van weerhouden ruimschoots gebruik te maken van de mogelijkheden die deze technische mogelijkheden hem bieden om berichten voor de overheid verborgen te houden. Het kernprobleem van de encryptie is, dat het voor alles dilemmatisch van karakter is. Voor de beveiliging van het reguliere betalingsverkeer is het onontkoombaar en geldt: hoe zwaarder de toegepaste encryptie hoe beter. Voor onderzoek en opsporing door de overheid vormt het een ernstige belemmering en zou de encryptie vooral niet te zwaar mogen zijn. Dat er al vele jaren discussie is over encryptie, zal gelet op het hier gestelde, geen verwondering wekken. Hoe dan ook, als de voortekenen niet bedriegen moet de overheid er zich op voorbereiden dat het afluisteren van berichten op het Internet op termijn problematisch, zo niet onmogelijk gaat worden. Het is van groot belang aandacht te besteden aan de vraag of politie en justitie voldoende zijn geëquipeerd om, ook in de toekomst, hun verantwoordelijkheid waar te maken inzake opsporing en vervolging.

Naast deze drie mogelijke gevolgen voor de nabije toekomst doet zich de meer fundamentele vraag voor hoe de huidige tendensen van virtualisering op de langere termijn onze samenleving zullen beïnvloeden. Informalisering ('ontstoffelijking') van de economie, de groei naar nieuwe vormen van ruilhandel, belastingontduiking, de vraag welke gevolgen de afname van de beïnvloedingsmogelijkheden van de overheid in de praktijk zal hebben, de ontwikkeling van nieuwe mogelijkheden van overheidsoptreden en de maatschappelijke haalbaarheid daarvan, het zijn allemaal voorbeelden die erop wijzen dat wij nog aan het begin staan van een ontwikkeling waarvan de langetermijneffecten niet zijn te voorspellen.

Aanbevelingen

Er zijn al heel veel maatregelen genomen om het (financiële) internetverkeer in goede banen te leiden. Toch moet er rekening mee worden gehouden dat er in de toekomst sprake zal blijven van aanzienlijke risico's. Daarom lijkt een aantal nieuwe stappen van belang. Het gaat daarbij vooral om preventie in de sfeer van de structurele maatregelen.

Hierna volgen zeven aanbevelingen van de SMVP. De twee eerste aanbevelingen zijn het meest concreet en behelzen de instelling van een samenwerkingsverband en een platform. De overige aanbevelingen zijn meer indicatief van aard en geven de terreinen aan waarop actie belangrijk is.

1. Instelling samenwerkingsverband

Het is van groot belang dat iedere (zakelijke) gebruiker zich realiseert dat de risico's van het gebruik van Internet moeilijk voorspelbaar zijn. Er zijn altijd mensen die er genoeg in scheppen te zoeken naar de zwakke punten van nieuwe technologische ontwikkelingen. Veelal gebeurt dat zonder een crimineel motief, zoals bij veel hackers. Maar als er wel sprake is van kwade bedoelingen, kan dat tot grote schade leiden. En het probleem is dat nimmer bekend is op welke manier dat gaat gebeuren. Uitwisseling van kennis en samenwerking op dit terrein is daarom van groot belang. In die zin is het belangrijk dat eind vorig jaar door de Internationale Kamer van Koophandel (ICC) een nieuwe divisie is opgericht die wereldwijd bedrijven moet helpen zich te beschermen tegen *cybercrime*. Deze divisie, die in London is gevestigd, zal nauw samenwerken met Interpol te Lyon en met de FBI. Ook in Nederland dient een dergelijke vorm van samenwerking te worden overwogen. Dit kan eventueel vorm krijgen door de instelling van een instituut of een samenwerkingsverband, dat tot taak heeft om kennis te vergaren en voorlichting te verzorgen over actuele vormen van misbruik van het Internet voor criminele doeleinden. Het samenwerkingsverband dient zeer beperkt van omvang te zijn en kan een gezamenlijk initiatief zijn van overheid en bedrijfsleven.

2. Instelling platform

De technologische ontwikkelingen gaan snel. De SMVP acht het van groot belang dat deze ontwikkelingen nauwlettend in de gaten worden gehouden en getoetst op de gevolgen voor de samenleving. Dit vereist een voortdurende samenspraak van vertegenwoordigers van de diverse maatschappelijke terreinen die worden geconfronteerd met de ontwikkelingen op het terrein van de virtualisering. De Stichting Maatschappij, Veiligheid en Politie is van plan om een breed samengesteld platform op te richten, om daarover periodiek van gedachten te wisselen. Naar behoefte kan het platform daarover publiceren, of het bestuur van de SMVP vragen een standpunt te formuleren.

3. Voorlichting

Er dient aandacht te worden besteed aan bewustwording van niet-professionele gebruikers ten aanzien van potentiële gevaren. Dit lijkt een goedkope doodoener, maar dat is het niet. Te vaak wordt nog onderschat dat veel nieuwe gebruikers zich op hun speeltje storten, zonder zich bewust te zijn van de risico's. Voorlichting daarover vindt in het geheel niet plaats, noch door providers, noch door anderen, terwijl voorlichting de bewustwording sterk kan bevorderen en daarmee van groot belang is.

4. Preventie

Het belang van preventieve maatregelen kan niet genoeg worden benadrukt. Voor een deel dienen deze van maatschappelijke, organisatorische aard te zijn, zoals de vraag hoe te voorkomen dat door gebruik te maken van een valse identiteit frauduleuze handelingen kunnen worden gepleegd. Voor een ander deel zijn zij van technische aard, zoals de hiervoor reeds genoemde encryptie en de ontwikkeling van betere fire-walls (beschermingsmuren binnen computers waardoor men slechts een beperkte toegang heeft tot bestanden).

5. Rol van providers

In de vierde plaats is er de afgelopen tijd sprake van een groeiende discussie over de rol en de verantwoordelijkheden van betrokkenen, zoals met name de providers. Wat mag er van providers worden verwacht aangaande het toezicht op de inhoud van het berichtenverkeer dat via zijn computer de wijde wereld in gaat? Als zij onverhoopt op iets strafbaars stuiten (kinderpornografie, maar ook criminele transacties - hoewel die laatste natuurlijk nauwelijks te traceren zijn), moeten zij dat aan de politie melden? En moeten providers op verzoek van opsporingsinstanties informatie verstrekken en zo ja, wanneer en aan wie? Belangrijke discussies zijn reeds gaande, maar er moet in de praktijk nog veel werk worden verricht. Aan providers zullen wat dat betreft hogere eisen moeten worden gesteld dan aan de leveranciers van traditionele telecommunicatiediensten.

6. Wetgeving

Het achterlopen van wetgeving is een groot en moeilijk oplosbaar probleem. Handel, betalingen, mensen, misdaad, alles gaat over grenzen heen, maar de wetgeving blijft nationaal en loopt alleen al daarom structureel achter. Hoewel thans op bijvoorbeeld Europees niveau maatregelen worden genomen om dit euvel terug te dringen, zal duidelijk zijn dat dit, gelet op het mondiale karakter van het probleem, slechts een bescheiden effect zal hebben. De voorgaande aanbevelingen laten zien dat de controle op de informatiestromen via het Internet een nieuw type maatregelen vereist, die voor een deel slechts effect zullen hebben als zij op mondiaal niveau worden getroffen. De rol van de nationale wetgeving verdient verdere doordenking.

7. Controle en opsporing

Controle en opsporing zijn aan herijking toe. Gelukkig gebeurt er al veel op dit gebied. 'Surveilleren op het Internet' begint een belangrijke term te worden. En de opsporingsinstanties realiseren zich dat opsporen via het Internet andere vaardigheden en andere strategieën vereist. Omdat 'afluisteren' steeds moeilijker wordt, zullen daarvoor andere opsporingsmethoden in de plaats moeten komen. Bij opsporingsonderzoeken is van belang dat er van alle betalingen een zogenaamde audit-trail bestaat, een vastgelegd en daardoor te traceren spoor van de weg die het geld heeft afgelegd en de daarop betrekking hebbende (elektronische) stukken. Maatregelen die ertoe leiden dat de audit-trail niet meer kan worden gevolgd, dienen in principe zoveel mogelijk te worden vermeden.

Tot slot

De SMVP meent dat er geen reden is voor mythevorming rond de gevaren van het Internet in zijn algemeenheid en het betalingsverkeer in het bijzonder. De neiging bestaat om het Internet risico's toe te dichtten alsof die uniek zijn voor dit medium, terwijl dergelijke risico's zich op soortgelijke wijzen voordoen bij andere betaalvormen of andere telecommunicatiemiddelen. Toch is alertheid geboden; immers er bestaan wel degelijk problemen en in de toekomst kan een groei daarvan niet worden uitgesloten. De hiervoor beschreven maatregelen dienen ertoe de risico's zoveel mogelijk te beperken.

Het bestuur van de Stichting Maatschappij, Veiligheid en Politie is de projectgroep die het achtergrondrapport heeft vervaardigd bijzonder erkentelijk voor haar arbeid en dankt de medewerkers van de groep, in het bijzonder de secretaris J.L. Copray, voor hun bereidheid aan dit project mee te werken.

Met dit standpunt is een belangwekkend en omvangrijk project van de SMVP afgesloten: het project Financiële Instellingen en Onveiligheid. Dit project startte in 1994 onder leiding van de Stuurgroep Financiële Instellingen en heeft geleid tot tal van onderzoeken en publicaties, zoals het boek *Financiële Integriteit*, het evaluatieonderzoek naar de meldingen van ongebruikelijke transacties, het onderzoek naar integriteit op de beurs en diverse beleidsaanbevelingen. Het bestuur dankt ook de stuurgroep voor het vele werk dat zij in dit project heeft willen steken, en spreekt de hoop uit dat de aanbevelingen van de Stichting Maatschappij, Veiligheid en Politie een bijdrage zullen leveren aan een veilige ontwikkeling van het betalingsverkeer via het Internet.

Mr Pieter van Vollenhoven,
Voorzitter Stichting Maatschappij, Veiligheid en Politie