SKIMMEN

Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012

«waakzaam en dienstbaar»

POLITIE

Skimmen

Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012

Martin Grapendaal

« waakzaam en dienstbaar »

POLITIE
Korps landelijke politiediensten

Uitgave

Dienst IPOL
Postbus 3016
2700 KX Zoetermeer

De Dienst IPOL
is een onderdeel van het Korps landelijke politiediensten

Colofon

Tekst Martin Grapendaal
Eindredactie Irene Spijker

Zoetermeer, februari 2012

Inhoud

Erratum

In het rapport "Skimmen" wordt de conclusie getrokken dat skimming in Nederland tot het verleden behoort.

Die conclusie is wat al te stellig. Skimmen is nog steeds mogelijk in gelduitgifte automaten die de bankpas in zijn geheel 'inslikken'. Skimmen is onmogelijk bij betaalterminals waar alleen het gedeelte van de pas met de chip in wordt gestoken.

Inleiding

Elke vier jaar wordt door de Dienst IPOL van het Korps landelijke politiediensten (KLPD), in samenwerking met de Dienst Nationale Recherche van hetzelfde korps, het Nationaal dreigingsbeeld (NDB) georganiseerde criminaliteit vervaardigd. Het eerste verscheen in 2004. In opdracht van het College van procureurs-generaal wordt telkens een zo breed mogelijk overzicht gepresenteerd van de stand van zaken rond de georganiseerde criminaliteit in Nederland. Centraal staan daarbij de criminele hoofdactiviteiten. Dat wil zeggen dat vooral de daarop betrekking hebbende strafrechtelijke delictcategorieën onderwerp van onderzoek zijn. Het gaat niet alleen om de meer traditionele vormen van georganiseerde criminaliteit zoals drugshandel, witwassen, mensenhandel en -smokkel, maar ook om minder bekende vormen zoals wapenhandel, *skimming*, kinderpornografie, vals geld en allerlei vormen van cybercrime.

Deze vormen van georganiseerde criminaliteit worden – aan de hand van uniforme onderzoeksvragen – in afzonderlijke projecten onderzocht. In het eindrapport NDB worden de resultaten van deze projecten samengevat en voorzien van wat wij "een kwalificatie van dreiging" noemen. Hiermee wordt aangegeven of de betrokken vorm van georganiseerde criminaliteit voor de komende vier jaar als een bedreiging van de Nederlandse samenleving moet worden gezien. Mede op grond van deze kwalificaties worden de landelijke beleidsprioriteiten voor de middellange termijn vastgesteld.

Dit rapport over skimming is een van de deelrapporten die de bouwstenen voor het NDB2012 vormen.

Eerst volgt nu een samenvatting. In hoofdstuk 1 wordt ingegaan op de afbakening van het onderwerp en de doelstelling van het onderzoek en worden de onderzoeksvragen op een rijtje gezet. Aan de beantwoording van die onderzoeksvragen zijn de hoofdstukken 2 tot en met 6 gewijd.

Samenvatting

Dit rapport over skimmen is tot stand gekomen als onderdeel van het Nationaal dreigingsbeeld 2012. Binnen dit project worden diverse deelprojecten uitgevoerd op het gebied van de georganiseerde criminaliteit. Het doel van de deelprojecten is een aantal onderzoeksvragen te beantwoorden die in grote lijnen voor al deze projecten hetzelfde luiden. Het gaat om de volgende zeven vragen:

1. Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de wijze waarop die criminaliteit wordt gepleegd?
2. Hoe heeft de omvang van het criminele verschijnsel zich ontwikkeld?
3. Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de kenmerken van personen respectievelijk criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?
4. Wat zijn de gevolgen van het criminele verschijnsel voor de Nederlandse samenleving?
5. Welke criminaliteitsrelevante factoren zijn, in welke mate en op wat voor wijze, van invloed op het criminele verschijnsel?
6. Wat zijn voor de komende jaren de verwachtingen over het criminele verschijnsel voor wat betreft omvang, werkwijzen, betrokkenen en maatschappelijke gevolgen?
7. Welke aanknopingspunten voor beleid dat gericht is op het tegenhouden of terugdringen van criminaliteit komen uit het onderzoek naar voren?

Skimmen is het kopiëren van gegevens die op de magneetstrip van een bankpas, creditcard of tankpas staan, naar een blanco pas. Met deze laatste pas en de juiste pincode wordt geld opgenomen van de betreffende rekening. De schade die hiermee in de afgelopen jaren werd veroorzaakt, laat voor de periode 2006-2009 een consequent stijgende lijn zien. Was er in 2006 nog sprake van 4,9 miljoen euro schade, in 2009 was dit bedrag opgelopen tot 39 miljoen euro. Als gevolg van intensievere bestrijding en voorlichtingscampagnes liep de schade in 2010 sterk terug, tot 24 miljoen euro. De verwachting is dat er over 2011 weer sprake zal zijn van aanzienlijke stijging. De voornaamste reden die hiervoor gegeven wordt, is het vervangen van de magneetstrip op de bankpas door de moeilijk te kraken EMV-chip. Naar verluidt zouden de voornamelijk Roemeense en Bulgaarse criminele samenwerkingsverbanden (csv's) nog een laatste slag willen slaan, voordat het skimmen via het kopiëren van de magneetstrip tot het verleden zal behoren.

In vergelijking met de eerdere NDB-rapportage over skimmen in 2008, is er met betrekking tot de daders en de modus operandi betrekkelijk weinig nieuws onder de zon aangetroffen. Het gaat nog steeds vooral om Roemeense criminele netwerken die op vaak ingenieuze wijze betaal- en geldautomaten manipuleren of tijdelijk vervangen. Op deze manier worden paslezers soms maandenlang misbruikt voordat overgegaan wordt tot *cashen.* Doordat banken en winkels hun apparaten steeds beter beveiligen, hebben we de afgelopen twee jaar gezien dat de skimmers hun aandacht verleggen naar onbemande betaal-automaten in parkeergarages en bij tankstations.

Sinds 1 januari 2012 wordt de magneetstrip in Nederland niet meer geaccepteerd. In plaats van de strip wordt nu de EMV-chip gebruikt. Daarmee behoort het skimmen tot het verleden. Hoewel csv's er blijk van hebben gegeven technologisch in de pas te kunnen lopen met innovaties, is er tot op heden nog geen melding geweest van het *shimmen* van de chip. Onderzoekers van de universiteit van Cambridge zijn erin geslaagd de beveiliging van de chip te omzeilen, maar de csv's beschikken blijkbaar nog niet over de kennis en apparatuur die daarvoor nodig zijn.

De verwachting is dat het skimmen zoals we dat tot nu toe kenden, in Nederland niet meer zal voorkomen. Er zijn landen (zoals de Verenigde Staten) die nog niet overgegaan zijn op de chip. Zij zullen waarschijnlijk in toenemende mate geconfronteerd worden met skimaanvallen.

Wel zal er in de eerste maanden van 2012 ook in Nederland waarschijnlijk nog sprake zijn van slachtofferschap. De *cashers* die zich in het buitenland bevinden, sparen de in 2011 geskimde passen. Pas op een later tijdstip zullen deze gefaseerd gebruikt worden voor geldopnamen in landen als Indonesië, de Dominicaanse Republiek en Argentinië.

De vraag of de EMV-chip in de nabije toekomst ook doelwit zal zijn van aanvallen, is nu niet te beantwoorden. De ervaring wijst uit dat csv's een groot adaptatievermogen hebben. We moeten er dus rekening mee houden dat de chip op enig moment door criminelen gekraakt zal worden. Dan is de bankensector weer aan zet.

De aanpak van skimmen en shimmen bevindt zich vooral op het technologische vlak. Voortdurende innovaties in beveiliging zorgen ervoor dat de csv's telkens achter de feiten aan lopen. Dit heeft wel een schaduwzijde. Wanneer de technologische beveiliging de perfectie nadert, zullen de csv's andere, meer intimiderende methoden gaan proberen. Dat maakt de kans op een rechtstreekse

confrontatie tussen slachtoffer en crimineel groter. In 2011 is het Landelijk Skimming Point Nederland ingericht. Hier wordt informatie verzameld en de aanpak gecoördineerd. Ook rechtshulpverzoeken worden hier in behandeling genomen. De knowhow is zo op één plaats geconcentreerd en niet meer versnipperd over Nederland.

1
Afbakening, doelstelling en onderzoeksvragen

1.1 Afbakening

Deze rapportage heeft betrekking op het fenomeen skimmen, en wel in georganiseerd verband.

Kort gezegd bestaat het skimmen van bankpassen, creditcards en/of tankpassen erin dat de gegevens van de magneetstrip op de pas gekopieerd worden naar een blanco pas. Met deze pas en de juiste pincode kan geld opgenomen worden van de betreffende rekening. Om de benodigde gegevens te bemachtigen prepareren de daders pinautomaten. Betaalautomaten in winkels voorzien zij 's nachts van hard- en software om de gegevens te kopiëren, een paar dagen later verwijderen ze deze voorziening weer, de gegevens van de klanten worden per sms of e-mail naar een buitenland verzonden en op blanco passen gezet, en korte tijd later wordt elders in Europa een grote som gelds illegaal gepind. Gelduitgifteautomaten krijgen een vals voorzetpaneel met dezelfde hard- en software. Meestal wordt ook nog een klein cameraatje gemonteerd om de pincode 'af te kijken'.

Zoals gezegd, gaat het in deze rapportage om skimming met een georganiseerd karakter. Dit wil zeggen dat de skimmingactiviteiten a) hun beslag krijgen in de structurele samenwerking tussen personen en b) worden gepleegd met het oog op het gezamenlijk behalen van financieel of materieel gewin.

Het eerste kenmerk, structurele samenwerking tussen personen, betekent niet alleen dat er sprake is van (de intentie tot) herhaald plegen[1] maar ook van enige consistentie in de samenstelling van het samenwerkingsverband[2]. In sommige gevallen kan *de intentie* van herhaald plegen volstaan.

---

1 Het herhaald plegen hoeft niet noodzakelijkerwijs betrekking te hebben op hetzelfde delict.

2 De consistentie kan er bijvoorbeeld ook in bestaan dat het criminele ondernemen georganiseerd is volgens het 'kwal-model' (Grapendaal, Nieuwenhuis, Van der Leest & Soudijn, 2004) of dat binnen een netwerk wisselende coalities worden gesmeed.

1.2 Doelstelling

Het primaire doel van het NDB is het verschaffen van inzicht in de (toekomstige) ontwikkeling van criminele verschijnselen op het terrein van de georganiseerde criminaliteit, waarmee onderbouwing mogelijk wordt voor politie en justitie bij het vaststellen van prioriteiten in de aanpak van de georganiseerde criminaliteit op nationaal besturingsniveau.

Het doel van dit deelproject is het verkrijgen van inzicht in:
- de ontwikkeling van aard en omvang van skimming;
- de (samenwerkingsverbanden van) personen die zich met skimming bezighouden of daarbij op een andere manier betrokken zijn;
- de maatschappelijke gevolgen;
- de toekomstige ontwikkelingen van de aard, omvang en gevolgen.

Het verkregen inzicht kan dienen ter ondersteuning van de aanpak van skimming door publieke en private partijen. Het rapport vormt een bouwsteen voor het Nationaal dreigingsbeeld 2012.

De genoemde doelstelling wordt bereikt door het beantwoorden van een zevental onderzoeksvragen die in de volgende paragraaf gepresenteerd worden.

1.3 Onderzoeksvragen

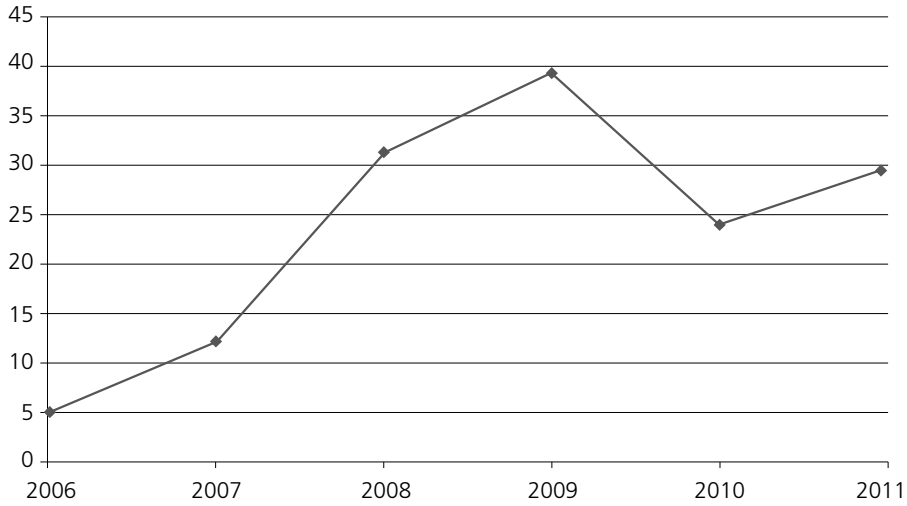
De volgende onderzoeksvragen worden in dit rapport beantwoord:
1. Hoe heeft de aard van skimming zich ontwikkeld voor wat betreft de wijze waarop deze vorm van criminaliteit wordt gepleegd?
2. Hoe heeft de omvang van skimming zich ontwikkeld?
3. Hoe heeft de aard van skimming zich ontwikkeld voor wat betreft de kenmerken van personen respectievelijk criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?
4. Wat zijn de gevolgen van skimming voor de Nederlandse samenleving?
5. Welke criminaliteitsrelevante factoren zijn, in welke mate en op wat voor wijze, van invloed op skimming?
6. Wat zijn voor de komende jaren de verwachtingen over skimming voor wat betreft omvang, werkwijzen, betrokkenen en maatschappelijke gevolgen?
7. Welke aanknopingspunten voor beleid dat gericht is op het tegenhouden of terugdringen van skimming komen uit het onderzoek naar voren?

2
Omvang en schade

In het NDB2008 (Boerman, Grapendaal & Mooij, 2008) worden de bedragen genoemd die in de jaren 2005 tot en met 2007 met skimmen gemoeid waren: respectievelijk 1,8 miljoen, 4,9 miljoen en 12,1 miljoen euro. Uit een persbericht van De Nederlandsche Bank blijkt dat dit laatste bedrag in 2008 bijna verdrievoudigde tot 31 miljoen, om in 2009 nogmaals te stijgen tot 39 miljoen. Pas in 2010 daalt het schadebedrag naar 24 miljoen euro, om – blijkens halfjaarcijfers – in 2011 weer te stijgen naar 29 miljoen euro (zie figuur 1). Naar verluidt wilden skimmers in 2011 nog een laatste slag slaan, omdat vanaf 1 januari 2012 het 'oude' skimmen niet meer mogelijk zou zijn: de magneetstrip op de bankpas werd per die datum gedeactiveerd en de aanwezige EMV-chip geactiveerd.

Figuur 1

Jaarlijkse schade door skimming (x1.000.000)



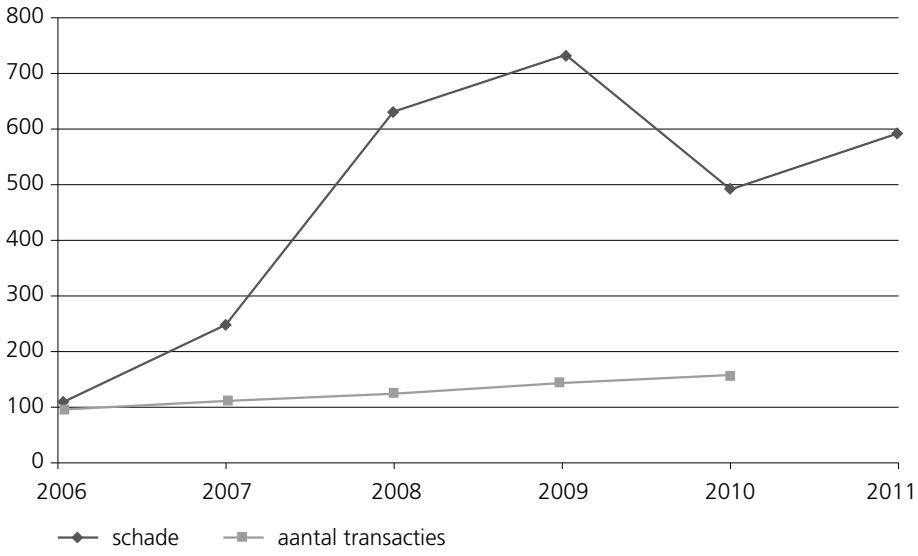
In procenten van de omzet die met het betalen met de betaalpas is gerealiseerd, kwam de totale fraude in Nederland uit op ruim 0,03 procent. Inclusief de fraude met creditcards op bijna 0,05 procent (Currence, 2010).

Hoewel het totale schadebedrag ten gevolge van skimming de afgelopen jaren dus is gestegen, is de schade per pas gedaald: in 2008 bedroeg deze nog 1500 euro, in 2011 ging het om 1100 euro.

Het aantal pintransacties is een maat voor de gelegenheid tot skimmen. De afgelopen jaren geeft dit aantal transacties een onafgebroken stijging te zien: van 1,45 miljard in 2006 tot 2,15 miljard in 2010 (Currence, 2010). Niet alleen het schadebedrag stijgt dus voortdurend, met een enkele onderbreking van die trend, ook de gelegenheid tot skimmen is toegenomen. In figuur 2 zijn die twee ontwikkelingen geïndexeerd weergegeven, waarbij 2006 op 100 is gesteld.

Figuur 2

Geïndexeerd aantal pintransacties en schadeomvang



We zien dat met name in de beginjaren het schadebedrag veel sneller steeg dan de gelegenheid tot skimmen uitgedrukt in aantal pintransacties. In 2010 was het schadebedrag 400 procent hoger dan in 2006, terwijl het aantal transacties met 50 procent was gestegen.

Op het totaalbedrag dat jaarlijks in Nederland gepind wordt (tussen 2006 en 2011 is dat gestegen van 64,2 miljard euro naar 80,9 miljard) is een schadebedrag van 29 miljoen euro (in 2011) 'te verwaarlozen'. Ook in internationaal perspectief bezien is de schade bescheiden. Een vergelijking van Nederlandse fraudegegevens met die van andere landen wordt weliswaar bemoeilijkt door het ontbreken van statistieken, maar gegevens van landen die wel fraudestatistieken publiceren, laten zien dat er, met name in Frankrijk en in het Verenigd Koninkrijk, sprake is van een hoger niveau van fraude dan in ons land. Ook hier laat zich een opwaartse beweging zien, waarbij zich in 2009 in het Verenigd Koninkrijk een onderbreking van deze trend voordeed. Voor het overgrote deel wordt de fraude in deze landen overigens veroorzaakt door misbruik van gegevens van betaalkaarten en creditcards die voor het betalen van aankopen via het internet worden gebruikt. Zoals bekend worden Nederlandse bankpassen, in tegenstelling tot creditcards, hiervoor niet gebruikt en is voor dit doel iDEAL ontwikkeld. In Spanje bleef de fraude de afgelopen jaren stabiel en kwam daardoor lager uit dan in Nederland.

3
Daders

In vergelijking met 2008, toen voor het laatst over skimming gerapporteerd werd (NDB2008), is er wat de daders betreft weinig nieuws onder de zon aangetroffen. Het grootste deel van de daders is afkomstig uit Roemenië. Bacau in Roemenië wordt in dat verband ook wel Skimcity genoemd. Recentelijk blijkt uit opsporingsonderzoeken dat ook Marokkanen en Bulgaren inmiddels actief zijn op deze markt.

In het rapport *Georganiseerde criminaliteit in politieregio's. Een analyse van 25 regionale cba's* (Boerman, Mesu, Nieuwenhuis & Grapendaal, 2010) wordt over de daders van skimming het volgende opgemerkt:

> In veel cba's wordt melding gemaakt van skimmende Roemenen. Uit gegevens van het Openbaar Ministerie blijkt dat niet alleen Roemenen zich bezighouden met het vervalsen van betaalpassen maar ook Nederlanders, Bulgaren, Maleisiërs, Surinamers en Britten, aldus de cba van Amsterdam-Amstelland. Zuid-Holland-Zuid beschrijft de voorkeur van Turken voor het skimmen van tankpassen. Somaliërs en Hindoestanen zouden echter een voorkeur hebben voor het skimmen van creditcards. Deze skimmende groepen zijn etnisch homogeen. Ook wordt in deze regio een Sri Lankaans netwerk in verband gebracht met skimmen. De opbrengsten worden mogelijk gebruikt voor de financiering van de Tamil Tijgers. Volgens de cba van Midden en West Brabant gebruiken Bulgaren vaak geavanceerdere technieken voor het skimmen dan Roemenen.
> Bij skimming zijn niet alleen buitenstaanders betrokken: soms probeert men personeel bereid te vinden betaalautomaten (BEA's) tegen betaling tijdelijk af te staan, zodat de apparaten na manipulatie kunnen worden teruggeplaatst. Zowel Rotterdam-Rijnmond als Noord-Holland-Noord als Amsterdam-Amstelland maakt melding van een neppostbode die gekleed in een TNT-uniform klanten laat pinnen voor pakjes om hun gegevens te bemachtigen.

Het lijkt erop dat de skimmers hun aandacht in 2010 verlegd hebben (Currence, 2010). Waren aanvankelijk gelduitgifteautomaten van banken en betaalautomaten in winkels het doelwit, de laatste jaren zijn onbemande betaalautomaten in toenemende mate slachtoffer. Voorbeelden zijn automaten van tankstations en parkeergarages. De kaartjesautomaten van de Nederlandse Spoorwegen die in 2009 en begin 2010 frequent bezocht werden, zijn met groot succes extra beveiligd tegen skimmen. In 2010 behoorden de zogenoemde

chipknipladers met vijftig geslaagde aanvallen voor het eerst tot de automaten die aan skimming ten prooi vielen.

In 2010 zorgden de geskimde 'e.dentifiers' van de ABN-AMRO voor enige ophef.[3] In de zogenoemde bankshops van deze bank kunnen rekeninghouders internetbankieren. Na enige tijd bleken de identificatie-apparaatjes gemanipuleerd te zijn. De skimmers hadden in het hol van de leeuw toegeslagen en voor zo'n 1,5 miljoen euro buitgemaakt. De apparaatjes zijn inmiddels vervangen door tweedegeneratie-e.dentifiers.

[3] Zie onder andere http://925.nl/archief/2010/10/18/miljoenenschade-criminelen-kraken-abn-amros-edentifier

4
Criminaliteitsrelevante factoren

Criminaliteitsrelevante factoren zijn algemeen maatschappelijke factoren die van invloed zijn op de toekomstige ontwikkeling van de georganiseerde criminaliteit. Deze factoren worden in het algemeen langs een zestal dimensies gerangschikt. Doorgaans wordt voor deze dimensies het acroniem SEPTED gebruikt. De letters staan voor sociaal-cultureel, economisch, politiek, technologisch, ecologisch en demografisch. In de context van het NDB worden ze gebruikt om verwachtingen te kunnen formuleren over de richting van de ontwikkeling in de behandelde vormen van georganiseerde criminaliteit. Lang niet alle van de denkbare factoren zijn van even grote betekenis. Het is mogelijk dat bepaalde factoren van geen enkel belang zijn bij het formuleren van de verwachtingen. In dit hoofdstuk wordt aandacht besteed aan de factor die de grootste invloed heeft op het verschijnsel skimming: technologie.

Skimmen betreft in feite de magneetstrip op de diverse bankkaarten. De technologische ontwikkeling van de EMV-chip zal het skimmen beduidend moeilijker maken. Inmiddels zijn vrijwel alle betaalautomaten uitgerust met de mogelijkheid de EMV-chip te lezen en wordt de strip door deze automaten niet meer geaccepteerd. Begin 2011 verschenen berichten dat de "EMV-chip ook gevoelig is voor skimmen". Wetenschappers van de universiteit van Cambridge waren erin geslaagd de beveiliging van de chip te kraken.[4] Het voert te ver hier de precieze technologie die daarvoor vereist is uit de doeken te doen. In de kern gaat het erom dat met een manipulatie van de chiplezer de pincode achterhaald kon worden. Vervolgens moest nog wel de bijbehorende bankkaart ontvreemd worden om met die combinatie geld op te nemen. Strikt genomen is dit geen skimming, omdat de gegevens van de kaart niet gekopieerd worden naar een andere kaart: de aanval richt zich op de communicatie tussen de chip en de lezer. Inmiddels wordt deze relatief nieuwe vorm *shimming* genoemd. Afgewacht moet worden welke vlucht deze vorm van kaartfraude neemt, maar het verschijnsel is in zekere zin wel verontrustend. In verband met de noodzakelijke diefstal van de kaart neemt de kans op een confrontatie tussen de eigenaar van de kaart en de dief immers toe. In januari 2012 waren er nog geen gevallen bekend geworden van succesvolle pogingen de EMV-chip te shimmen.

---

4 Onder andere http://tweakers.net/nieuws/73295/pincode-emv-chip-blijkt-vatbaar-voor-skimmen.html

De invoering van de EMV-chip betekent overigens niet dat er in 2012 geen aangiften van skimming meer worden gedaan. Informatie van het Landelijk Skimming Point[5] laat zien dat de criminele samenwerkingsverbanden (csv's) de kaarten die in 2011 geskimd zijn, 'opgespaard' hebben. In januari 2012 werden in landen als Indonesië, Argentinië en de Dominicaanse Republiek nog bedragen geïnd met in 2011 geskimde passen. De 'cashers' wachten tot de datum waarop het salaris overgemaakt wordt, om er zeker van te zijn dat de bankrekeningen een positief saldo te zien geven.

[5] Zie hierover hoofdstuk 5.

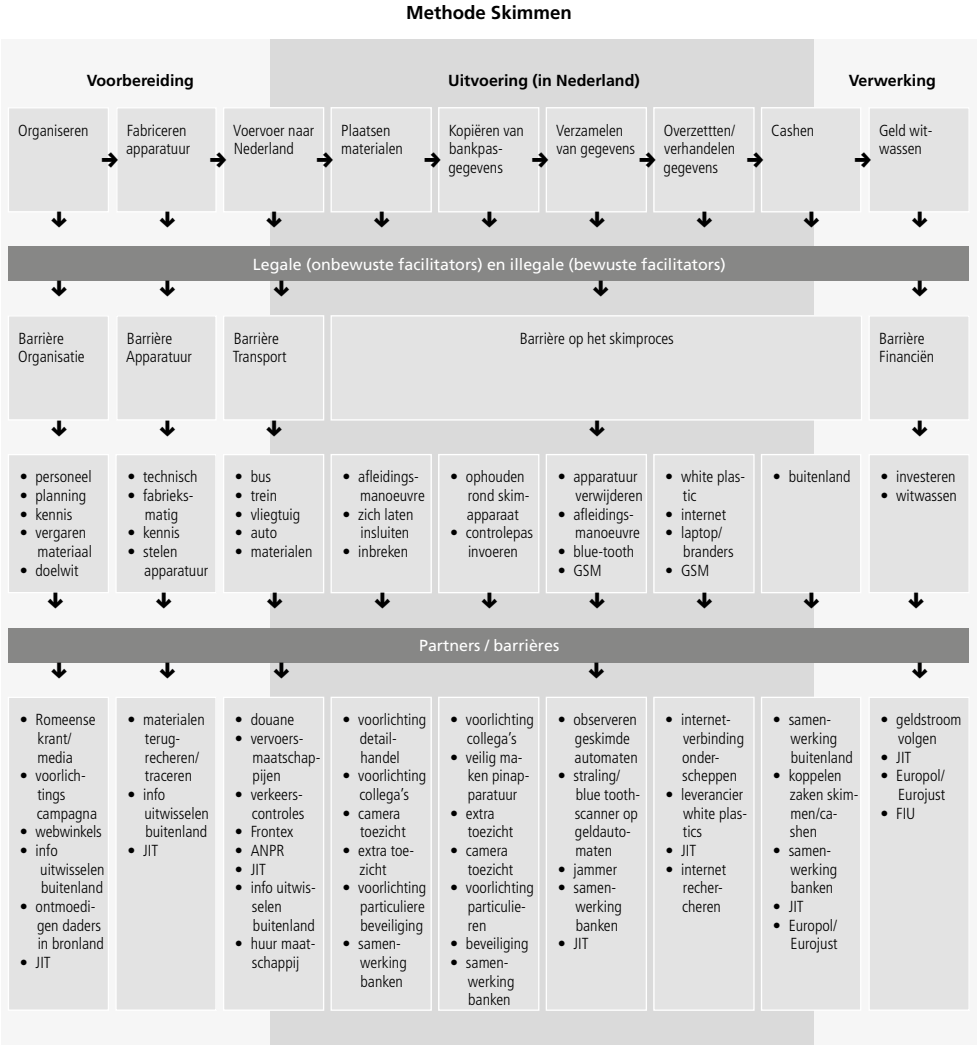
5
Aanpak

Volgens Currence is er sprake van positieve ontwikkelingen op het gebied van skimmen. Die zijn te danken aan een drietal maatregelen. In de eerste plaats moet het toenemende gebruik van de EMV-chip op de bankpassen, in plaats van de magneetstrip, genoemd worden. Hoewel blijkbaar niet waterdicht, is de beveiliging van zo'n chip geavanceerder dan die van de magneetstrip. Ten tweede is Currence een voorlichtingscampagne voor het MKB gestart waardoor veel gemanipuleerde apparaten tijdig ontdekt werden. Tot slot hebben de banken hun detectiesystemen in 2010 verder aangescherpt, waardoor geskimde bankpassen eerder geblokkeerd kunnen worden. Dit blokkeren van de strip wordt door banken ook preventief en op aanvraag van de rekeninghouder gedaan. Wanneer iemand bijvoorbeeld naar een buitenland gaat waar de magneetstrip nog gebruikt wordt, kan hij bij zijn bank vragen de magneetstrip te blokkeren.

Ook de politie heeft niet stilgezeten. In de loop van 2011 is het Landelijk Skimming Point Nederland ingericht, een samenwerkingsverband van de politie, het Openbaar Ministerie en Equens. Dit verzamelt onder andere alle gerapporteerde skimmingincidenten in Nederland. Door onderlinge vergelijking van de modi operandi kan gemakkelijker dan voorheen vastgesteld worden of de incidenten aan een en hetzelfde samenwerkingsverband toegeschreven kunnen worden. Daarnaast worden buitenlandse rechtshulpverzoeken centraal bij het Skimming Point in behandeling genomen. Op deze manier worden die verzoeken beter gecoördineerd. Ook is bij het Skimming Point het onderstaande barrièremodel ontwikkeld, dat laat zien op welke plekken in het criminele bedrijfsproces de aanpak het beste gericht kan worden. In twee workshops met experts is het model verder verkend en aangescherpt. Op basis van deze workshops is ervoor gekozen de primaire focus te leggen op het opwerpen van barrières in de bronlanden (Roemenië en Bulgarije), van barrières op de technologie/magneetstrip van de bankpas en van barrières op cashing.

Figuur 3

Een barrièremodel voor skimming (Bron: Landelijk Skimming Point)



6
Verwachtingen

Inmiddels zijn vrijwel alle Nederlandse bankpassen voorzien van de EMV-chip. De betaalautomaten blijven hierbij achter, maar in toenemende mate worden de consumenten in de gelegenheid gesteld te betalen door middel van identificatie met de EMV-chip.

Op 1 januari 2012 was het pinnen met de EMV-chip in Nederland voor 100 procent ingevoerd. Daarmee zijn de skimgelegenheden tot een minimum beperkt. Het blijft echter afwachten welke technologische truc de skimmers in petto hebben om ook de EMV-chip te 'kraken'. Het verleden heeft uitgewezen dat csv's er telkens weer in slagen een technologische achterstand in te lopen. Mocht dat ook nu het geval zijn, dan impliceert dat niet dat we weer 'terug bij af' zijn: de al eerder genomen preventieve maatregelen, die zonder EMV-chip al tot een behoorlijke reductie hebben geleid, blijven vanzelfsprekend van kracht.

In Europa is vrijwel overal de EMV-chip ingevoerd. Elders zijn er nog veel landen die de magneetstrip voorlopig blijven hanteren. Het is waarschijnlijk dat de csv's hun aandacht gaan verleggen naar deze landen. De Verenigde Staten zullen voor hen het belangrijkst zijn, maar ook Indonesië en landen in Midden- en Zuid-Amerika kunnen in toenemende mate slachtoffer worden van skimpraktijken.

Al met al ligt voor de middellange termijn (1 tot 4 jaar) in Nederland een verdere daling van de skimschade in het verschiet. Voor de langere termijn zijn de technologische ontwikkelingen bepalend.

Gebruikte literatuur

Boerman, F., M. Grapendaal & A. Mooij (2008). *Nationaal dreigingsbeeld 2008. Georganiseerde criminaliteit*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

Boerman, F., S. Mesu, F. Nieuwenhuis & M. Grapendaal (2010). *Georganiseerde criminaliteit in politieregio's. Een analyse van 25 regionale cba's.* Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

Currence (2010). *Jaarverslag 2010.*

Grapendaal, M., F. Nieuwenhuis, W. van der Leest & M. Soudijn (2004). *Criminele samenwerking. Verslag van een onderzoek voor het Nationaal dreigingsbeeld zware of georganiseerde criminaliteit*. Zoetermeer: Korps landelijke politiediensten, Dienst Nationale Recherche Informatie.