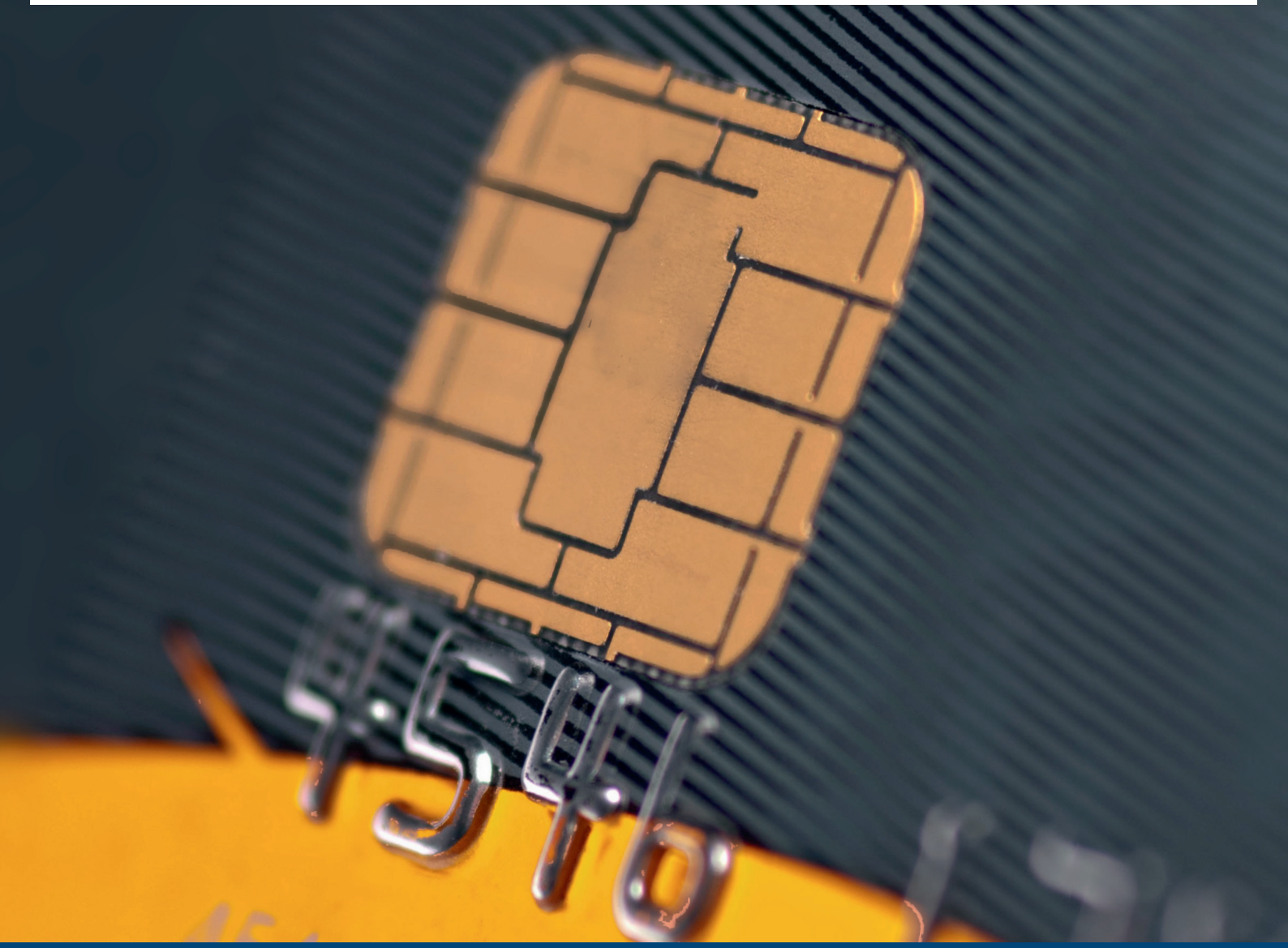
Bundeskriminalamt



Zahlungskarten-kriminalität

Bundeslagebild 2012

INHALT

1. Vorbemerkung 5

2. Darstellung und Bewertung der Kriminalitätslage 5

2.1 Manipulationen im Inland („Skimming“) 6

2.2 Manipulationen von Geldautomaten und POS-Terminals im Ausland 8

2.3 Einsatz gefälschter Debitkarten mit deutschen Kartendaten 8

2.4 Tatverdächtige 9

3. Gesamtbewertung 10

Impressum 11

1. VORBEMERKUNG

Das Bundeslagebild Zahlungskartenkriminalität enthält in gestraffter Form die aktuellen Erkenntnisse zur Lage und Entwicklung im Bereich der Zahlungskartenkriminalität. Es erstreckt sich ausschließlich auf Debit- und Kreditkarten (zusammenfassend als Zahlungskarten bezeichnet), da die übrigen Bereiche (z. B. Pre-Paid-Karten) für die Kriminalitätslage in Deutschland ohne Bedeutung sind. Das Phänomen des Diebstahls digitaler Daten von Zahlungskarten und deren anschließende Verwertung im Internet werden im Bundeslagebild Cybercrime 2012 dargestellt.

2. DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

Karten deutscher Emittenten weiterhin begehrt

Inhaber von Zahlungskarten deutscher Emittenten verfügen im internationalen Vergleich über eine hohe Bonität. Daher sind deren Karten bzw. Kartendaten begehrtes Ziel von Straftätergruppierungen. Das Bundeskriminalamt schätzt, dass in Deutschland über 130 Mio. Zahlungskarten ausgegeben wurden, davon rund drei Viertel Debitkarten[01] und ein Viertel Kreditkarten. Entsprechend diesem Verhältnis überwiegen bei den bekannt gewordenen Straftaten die Fälle aus dem Debitkartenbereich deutlich.
Belastbare Gesamtzahlen zur bundesweiten Fall- und Schadensentwicklung liegen der Polizei auch für das Jahr 2012 nicht vor[02]. Ein Großteil der Straftaten wird nicht angezeigt, da der Schaden des Betroffenen durch die Geldinstitute und Kreditkartenorganisationen in der Regel erstattet wird. Die Informationspolitik der Kartenorganisationen und Dachverbände hinsichtlich der erlittenen Verluste und Missbrauchsumsätze ist seit Jahren sehr restriktiv.

Chiptechnik erschwert Fälschungen

Das Fälschen von Debitkarten mit Echtdaten wird unter Aufwand-Nutzen-Gesichtspunkten durch die Täter weiterhin bevorzugt. Mit gefälschten Karten bieten sich den Tätern bessere Einsatzmöglichkeiten als mit gestohlenen Karten, da Letztere durch die Kartenorganisationen gesperrt werden, sobald der Diebstahl bemerkt wird. Dadurch werden sie für die Täter unbrauchbar. Der Einsatz gefälschter Debitkarten deutscher Emittenten kann allerdings aufgrund besonderer technischer Sicherheitsvorkehrungen nicht an inländischen, sondern ausschließlich an ausländischen Geldautomaten erfolgen. Seit 2011 ist es zudem den Tätern nicht mehr möglich, gefälschte Debitkarten im europäischen SEPA-Raum[03] einzusetzen, da innereuropäisch (mit Ausnahme Russlands) die Abrechnung ausschließlich über den Chip und nicht mehr über den Magnetstreifen erfolgt.
Zur Verhinderung missbräuchlicher Einsätze von Kartendaten, die durch Manipulationen von Geldautomaten, POS-Terminals etc. erlangt wurden, haben deutsche Banken und Sparkassen im Jahr 2012 die Daten von über 140.000 Zahlungskarten gesperrt.

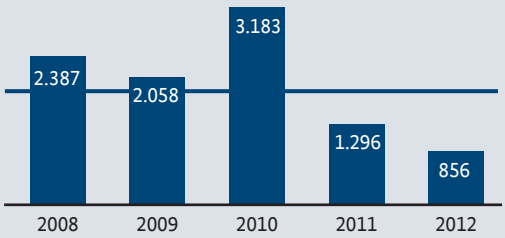
01 Debitkarten: (von englisch (to) debit = belasten) räumen keinen Kredit ein; bei Zahlungen mit Debitkarten wird das Konto sofort belastet. Die bekannteste Debitkarte in Deutschland ist die von Banken und Sparkassen ausgegebene ec-Karte.
02 Die im Bundeslagebild angeführten Falldaten basieren auf Erkenntnissen aus dem nationalen und internationalen Informationsaustausch.
03 SEPA: Single Euro Payments Area.

2.1 MANIPULATIONEN IM INLAND („SKIMMING“)[04]

Rückläufige Entwicklung bei Angriffen auf Geldautomaten

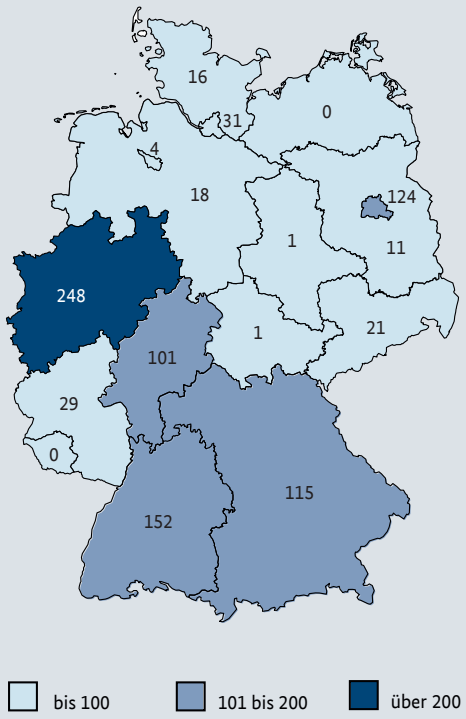
Im Jahr 2012 wurde in Deutschland mit insgesamt 856 Angriffen auf Geldautomaten zur Erlangung von Kartendaten und PIN erneut ein Rückgang der Skimming-Straftaten um rund 34 % registriert. Im Verhältnis zur durchschnittlichen Zahl der Angriffe auf Geldautomaten in den letzten fünf Jahren (1.956 Fälle) liegt die aktuelle Fallzahl um 56 % deutlich unter dem Mittelwert.

Anzahl der Angriffe auf Geldautomaten in Deutschland 2008 - 2012



Bedingt durch Mehrfachangriffe einzelner Geldautomaten waren 2012 bundesweit 505 Automaten (2011: 784) betroffen, ein Rückgang von 35 %. Die Manipulationszeiträume sind oftmals sehr kurz. Sie betragen teilweise nur wenige Stunden. Insbesondere Geldautomaten in stark frequentierten Bereichen wie in Fußgängerzonen und Bahnhöfen werden oft mehrfach manipuliert. Durch den Abbau bzw. die sicherheitstechnische Aufrüstung von Türöffnern zu Bankfoyers sind Kartendatenabgriffe in diesem Bereich nahezu bedeutungslos geworden. Im Jahr 2012 ist der Datenabgriff lediglich in 15 Fällen durch Türöffnermanipulationen erfolgt.

Angriffe auf Geldautomaten nach Bundesländern 2012



Keine neuen Tatbegehungsweisen beim „Skimming“ an Geldautomaten

Die Modi Operandi zur Erlangung der PIN/Geheimzahl sind im Wesentlichen unverändert. Nach wie vor installieren die Täter Vorbaugeräte zum Auslesen der Kartendaten (so genannte „Skimmer“) sowie versteckte Mini-Kameras oberhalb der Tastatur oder im Deckenbereich (z. B. Rauchmelderattrappen) zur Aufzeichnung der PIN-Eingaben. Alternativ werden unmittelbar auf der Originaltastatur Tastaturattrappen angebracht, die die eingegebenen PIN-Daten speichern. Die zunehmende Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen (mechanisch und elektronisch) erschwert der Täterseite den erfolgreichen Einsatz ihrer Skimming-Technik.

04 Skimming: Kartendatenerlangung durch Auslesen der gesamten Magnetstreifen (-daten) einer Zahlungskarte und das Kopieren/Übertragen auf eine Kartenfälschung.

Wieder zunehmende Bedeutung der Manipulation von POS-Terminals[05]

Nachdem im Jahr 2011 - erstmals seit 2008 - wieder Manipulationen von POS-Terminals in Deutschland festgestellt wurden, sind im Jahr 2012 in mindestens 77 Fällen ein oder mehrere POS-Terminals manipuliert worden. Hiervon haben die Täter in 50 Fällen die Kartendaten und PIN erfolgreich ausgespäht (2011: 14 Fälle, + 257 %) und diese anschließend im außereuropäischen Ausland eingesetzt. In den anderen 27 Fällen konnte die Manipulation aufgrund unterschiedlicher Sicherungssysteme und Präventionsmaßnahmen frühzeitig erkannt werden, bevor es zu missbräuchlichen Umsätzen kommen konnte.
In weiteren etwa 500 Fällen wurden POS-Terminals in Geschäften aufgrund von Verdachtsmeldungen vorsorglich durch die Netzbetreiber ausgetauscht, da Manipulationen nicht ausgeschlossen werden konnten.
Im Jahr 2012 stand die Sperrung von rund 20.000 Zahlungskarten (etwa 14 % aller Sperrungen) durch deutsche Banken und Sparkassen im Zusammenhang mit der Manipulation von POS-Terminals.

POS-Terminal mit „Haube“

POS-Terminal mit „Haube“

POS-Terminal mit Aufsatztastatur

Zwei gängige Manipulationsvarianten

Bei der Manipulation von POS-Terminals wurden unterschiedliche Vorgehensweisen der Täter festgestellt. Bei einer Variante erlangen die Täter durch Einbruch oder durch unbemerktes Verbleiben im Objekt nach Geschäftsschluss Zugriff auf die POS-Terminals. Die Geräte werden nach der Entwendung zeitnah außerhalb des Geschäftes manipuliert und noch in der gleichen Nacht wieder im Kassenbereich deponiert.
Bei einem anderen Modus Operandi ersetzen die Täter die POS-Terminals durch Ablenkung des Personals während des laufenden Geschäftsbetriebes gegen einen Dummy. Nach erfolgter Manipulation werden die Geräte wieder am ursprünglichen Kassenbereich platziert.

Terminal-Manipulationen für den Kunden nicht erkennbar

Die elektronischen Bauteile zum Auslesen und Abspeichern von Kartendaten (Magnetstreifendaten) und PIN werden entweder im POS-Terminal selbst installiert oder befinden sich in einer „Haube“, die auf das Originalgerät aufgesetzt wird. Die Veränderungen am oder im Gerät sind jedoch bei allen Varianten äußerlich nicht oder nur äußerst schwer erkennbar. Nach der Manipulation sind die Täter in der Lage, an sämtliche Kartendaten (Magnetstreifendaten) und die dazugehörigen PIN der an diesem Terminal eingesetzten Zahlungskarten zu gelangen. Der Datenabgriff erfolgt zum Teil über mehrere Wochen mit mehreren Hundert oder in Einzelfällen sogar mehreren Tausend betroffenen Kunden.

Fahrkarten- und Tankautomatenmanipulationen ohne Bedeutung

Nachdem in den Jahren 2010 und 2011 erstmals - wenn auch nur in geringem Maße - Manipulationen von Fahrkartenautomaten der Deutschen Bahn AG und unbeaufsichtigten Tankautomaten festgestellt wurden, waren diese Phänomene im Jahr 2012 mit insgesamt nur drei gemeldeten Fällen bedeutungslos.

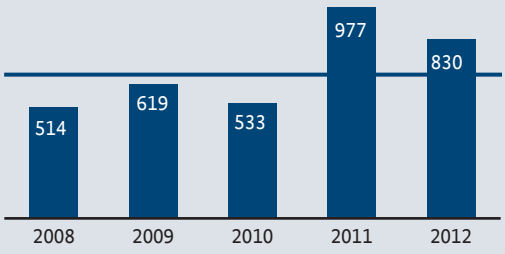
05 Point of Sale-Terminals = Kassenterminals.

2.2 MANIPULATIONEN VON GELDAUTOMATEN UND POS-TERMINALS IM AUSLAND

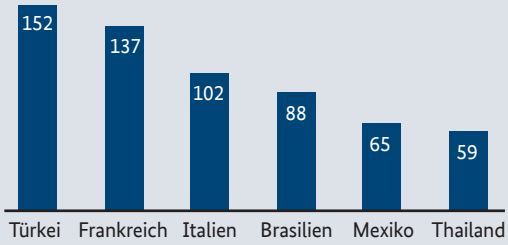
Weiterhin Abgriffe deutscher Kartendaten im Ausland

Im Jahr 2012 wurden im Ausland bei Manipulationen von insgesamt 830 Geldautomaten und POS-Terminals deutsche Kartendaten abgegriffen. Das entspricht zwar einem Rückgang von rund 15 % gegenüber 2011, jedoch liegt die Fallzahl mit 19 % deutlich über dem durchschnittlichen Wert der letzten fünf Jahre. Zu berücksichtigen ist in diesem Zusammenhang, dass die Zahl der registrierten Fälle unter dem Vorbehalt steht, dass in vielen Auslandsfällen der „Point of Compromise“ (PoC)[06] nicht eindeutig identifiziert werden kann und somit eine Vielzahl von Fällen nicht in die Statistik einfließt.

Manipulierte Geldautomaten und POS-Terminals im Ausland mit Abgriffen deutscher Kartendaten 2008 - 2012



Staaten, in denen deutsche Kartendaten 2012 am häufigsten ausgespäht wurden



2.3 EINSATZ GEFÄLSCHTER DEBITKARTEN MIT DEUTSCHEN KARTENDATEN

Haupteinsatzgebiete vorwiegend in Amerika

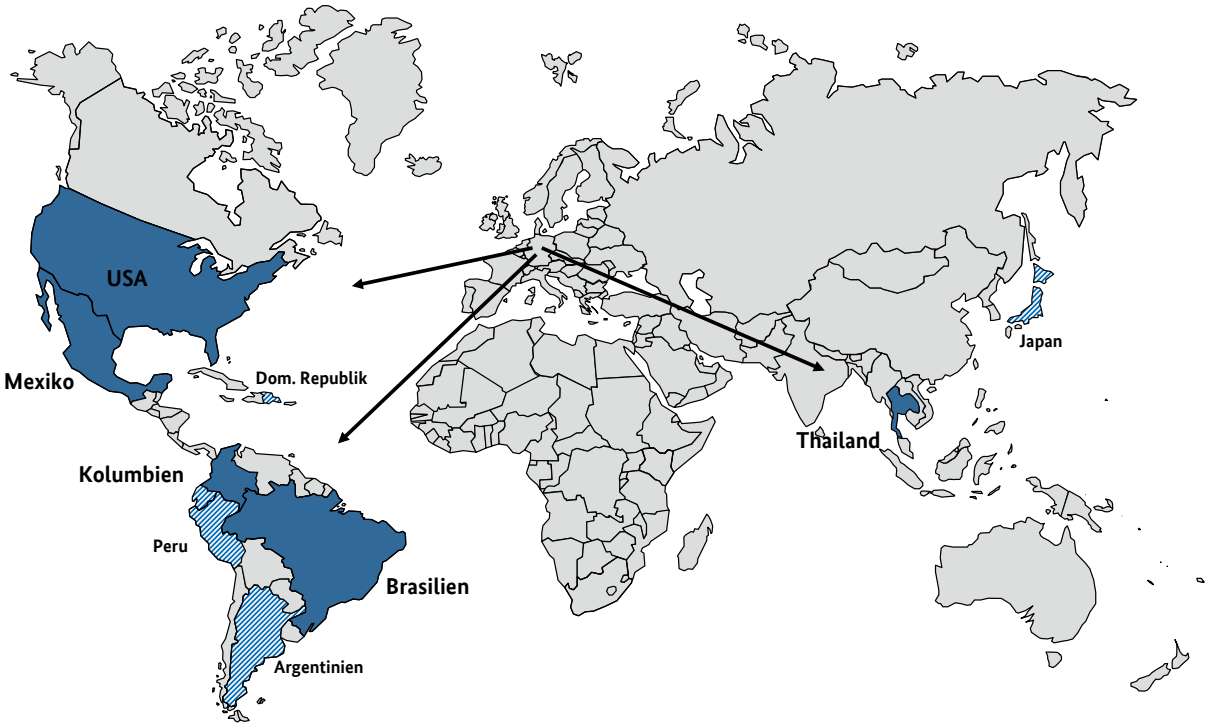
Seit dem 01.01.2011 werden Transaktionen mit Debitkarten im SEPA-Raum nicht mehr über den Magnetstreifen, sondern über den Chip autorisiert. Dies zwingt die Täter dazu, den Einsatz ihrer noch auf Magnetstreifenbasis funktionierenden „White Plastics“ ins außereuropäische Ausland in sogenannte „Nicht-Chip-Länder“ zu verlagern. Diese Entwicklung einer Verlagerung der missbräuchlichen Karteneinsätze in den außereuropäischen Raum zeichnete sich bereits in der zweiten Jahreshälfte 2010 ab.
Neben den in der nachfolgenden Grafik dargestellten Haupteinsatzgebieten gefälschter deutscher Debitkarten im Jahr 2012 wurden in Einzelfällen weitere Verwertungsstaaten in Mittel- und Südamerika, Asien und Afrika registriert.

Hohe Schäden durch POS-Manipulationen

Nach Einschätzung des Bundeskriminalamts[07] liegt der durch den Einsatz gefälschter Debitkarten mit deutschen Kartendaten entstandene Schaden im Jahr 2012 – trotz gesunkener Fallzahlen im Bereich der Manipulation von Geldautomaten – in etwa auf dem Vorjahresniveau von rund 35 Mio. Euro.
Grund hierfür dürfte die gestiegene Zahl von POS-Terminal-Manipulationen sein, da diese als weitaus schadensträchtiger einzustufen sind als Manipulationsfälle von Geldautomaten. Die Schadenssumme allein aus POS-Terminal-Manipulationen beläuft sich 2012 auf etwa 10 Mio. Euro.

06 Point of Compromise (PoC): Geldautomat oder Vertragsunternehmen, an/in dem die rechtmäßigen Karteninhaber ihre Zahlungskarte eingesetzt haben bzw. Ort, an dem die Kartendaten anschließend in „Täterhände“ gelangt sind (Zahlungskartendatenquelle).
07 Dem Bundeskriminalamt liegen keine konkreten Daten der Deutschen Kreditwirtschaft zur Schadensentwicklung vor.

Haupteinsatzstaaten gefälschter Debitkarten mit deutschen Kartendaten 2012



2.4 TATVERDÄCHTIGE

Dominanz rumänischer und bulgarischer Tatverdächtiger

Die Tatverdächtigen bei der Manipulation von inländischen Geldautomaten stammen wie in den Vorjahren fast ausschließlich aus Südosteuropa. Hier dominieren rumänische, gefolgt von bulgarischen Staatsangehörigen. Deutsche Staatsangehörige spielen in diesem Kriminalitätsbereich nahezu keine Rolle.
Die Tätergruppierungen zeichnen sich durch eine flexible und arbeitsteilige Vorgehensweise aus. Sie organisieren den gesamten Tatablauf von der Beschaffung der Kartendaten über die Produktion bis hin zum betrügerischen Einsatz der Kartendubletten im Ausland.

Die Tatverdächtigen agieren in kleinen Gruppen und halten sich zum Abgriff der Kartendaten meist nur relativ kurze Zeit, in einzelnen Fällen aber auch bis zu mehrere Wochen, an unterschiedlichen Orten in Deutschland auf. Die mittels technischer Manipulation gewonnenen Daten werden in der Regel sehr schnell verwertet. Nach bisherigen Erfahrungswerten liegen zwischen dem Datenabgriff und dem betrügerischen Einsatz der gefälschten Karten im Ausland meist nur ein oder zwei Tage.

3. GESAMTBEWERTUNG

Die mit Beginn des Umstellungsprozesses auf Chipkarten festzustellende positive Entwicklung bei der Bekämpfung der „Skimming-Kriminalität“ in Deutschland hat sich auch 2012 mit einem deutlichen Rückgang der Fallzahlen im Bereich der Manipulation von Geldautomaten fortgesetzt.
Zu dem starken Rückgang der Fallzahlen haben verschiedene Faktoren beigetragen. So haben u. a. der Austausch von Geldautomaten „älterer Bauart“ und der Einsatz wirksamer Anti-Skimming-Module eine Abnahme der Skimming-Fälle in Deutschland bewirkt. Darüber hinaus haben insbesondere die Umstellung auf die Chiptechnologie sowie die mittlerweile von vielen Geldinstituten zusätzlich ergriffenen Maßnahmen, die zusammenfassend mit dem Begriff „Magstripe-Controlling“ bezeichnet werden, die Einsatzmöglichkeiten gefälschter Karten zunehmend erschwert. Die „Magstripe-Controlling“-Strategie umfasst u. a. die grundsätzliche Deaktivierung der Magnetstreifen (modifizierte „Zwei-Karten-Strategie“), bei der die Aktivierung des Magnetstreifens für den Einsatz in „Nicht-Chip-Ländern“ nur auf Initiative des Kunden erfolgen kann, sowie die Reduzierung der Einsatzmöglichkeiten nach Risikoländern und die Festlegung von Limits für Auslandsabhebungen.

Die Bedeutung der derzeit festzustellenden negativen Entwicklung der Fallzahlen bei POS-Terminal-Manipulationen beruht insbesondere auf der Vielzahl möglicher Datenabgriffe und der damit einhergehenden hohen Schadenssummen.
Seit dem erneuten vermehrten Auftreten von POS-Terminal-Manipulationen betreibt das Bundeskriminalamt einen intensiven Informationsaustausch mit den Netzbetreibern, den Terminalherstellern, der EURO-Kartensysteme GmbH als Zentralstelle der deutschen Kreditwirtschaft für die Bearbeitung von Skimmingfällen, den großen Handelsunternehmen und den Dachorganisationen des Einzelhandels. Durch die Übermittlung von Warnhinweisen und Präventionsempfehlungen sowie durch die Umsetzung spezifischer Maßnahmen sollen die potenziell betroffenen Unternehmen in die Lage versetzt werden, POS-Terminal-Manipulationen in ihren Unternehmen zu erschweren bzw. bereits erfolgte Manipulationen leichter erkennen zu können.
Daher ist zu erwarten, dass aufgrund der eingeschränkten Verwertungsmöglichkeiten der auf Magnetstreifenbasis funktionierenden „White Plastics“ mittelfristig auch die Manipulationen von POS-Terminals an Bedeutung verlieren werden.

IMPRESSUM

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2012

Druck
BKA

Bildnachweis
Fotos Polizeiliche Quellen

www.bka.de