Bundeskriminalamt

ZAHLUNGSKARTEN-KRIMINALITÄT

Bundeslagebild 2011

BKA

ZAHLUNGSKARTENKRIMINALITÄT

Bundeslagebild 2011

Bundeskriminalamt

65173 Wiesbaden
info@bka.de
www.bka.de

INHALTSVERZEICHNIS

1. VORBEMERKUNG

Das Bundeslagebild Zahlungskartenkriminalität enthält in gestraffter Form die aktuellen Erkenntnisse zur Lage und Entwicklung im Bereich der Zahlungskartenkriminalität.

Das Bundeslagebild Zahlungskartenkriminalität 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 2011 dargestellt.

2. DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

2.1 Gesamtentwicklung

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[1], dass in Deutschland über 125 Mio. Zahlungskarten ausgegeben wurden, davon rund drei Viertel Debitkarten[2] 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 2011 nicht vor. 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.

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[3] einzusetzen, da innereuropäisch (mit Ausnahme Russlands) die Abrechnung ausschließlich über den Chip und nicht mehr über den Magnetstreifen erfolgt.

Das Bundeskriminalamt schätzt den durch den Einsatz gefälschter Debitkarten mit deutschen Kartendaten entstandenen Schaden im Jahr 2011 auf rund 35 Mio. Euro (2010: 60 Mio. Euro).

---

1 Dem Bundeskriminalamt stehen keine konkreten Zahlen zur Verfügung.

2 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.

3 SEPA: Single Euro Payments Area.

2.2 Manipulationen im Inland

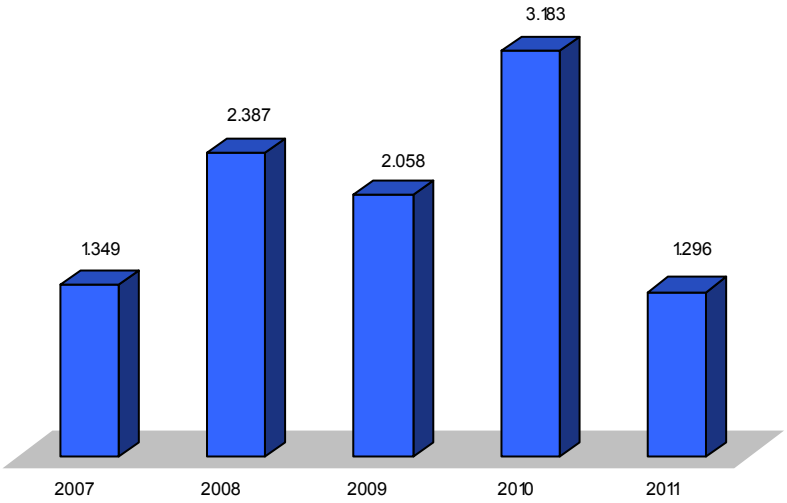
2.2.1 Angriffe auf Geldautomaten („Skimming“[4])

Im Jahr 2011 kam es in Deutschland insgesamt zu 1.296 (2010: 3.183) Angriffen auf Geldautomaten zur Erlangung von Kartendaten und PIN. Dies entspricht einem Rückgang von rund 59 %. Bedingt durch Mehrfachangriffe einzelner Geldautomaten waren bundesweit davon 784 Automaten (2010: 1.765) betroffen, ein Rückgang von 56 %.

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. Lediglich in acht gemeldeten Fällen ist der Datenabgriff durch Türöffnermanipulationen erfolgt.

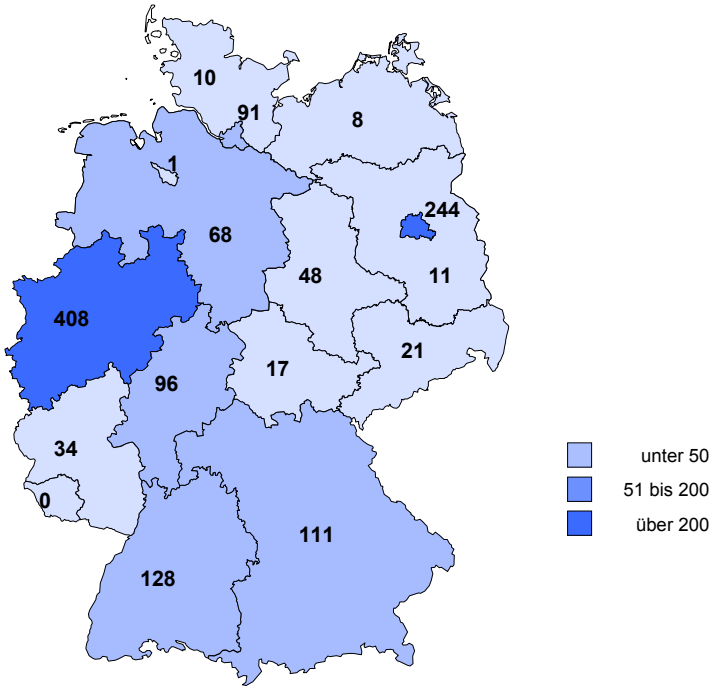
Anzahl der Angriffe auf Geldautomaten in Deutschland 2007-2011



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

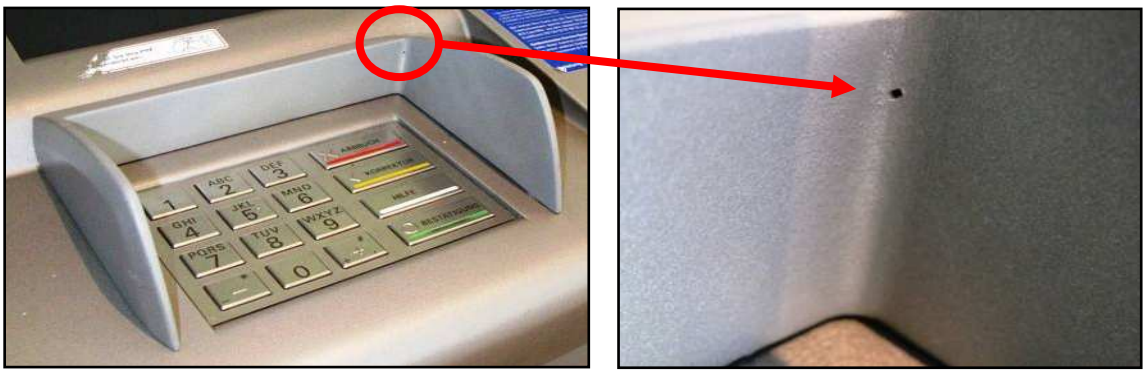
Die Angriffe auf Geldautomaten erfolgten 2011 nahezu im gesamten Bundesgebiet. Lediglich das Saarland war nicht betroffen. Die meisten Angriffe wurden in Nordrhein-Westfalen (408 Fälle) und Berlin (244 Fälle) verübt.

Angriffe auf Geldautomaten nach Bundesländern 2011



Die Modi Operandi zur Erlangung der PIN/Geheimzahl sind im Wesentlichen unverändert. Nach wie vor installieren die Täter Vorbaugeräte zum Auslesen der Kartendaten 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.

Manipulierter Sichtschutz mit Öffnung für die Kamera



2.2.2 Manipulationen von POS[5]-Terminals

Im Jahr 2011 wurden erstmals nach 2008 wieder erfolgreich POS-Terminals manipuliert. Betroffen waren Bau- und Lebensmittelmärkte sowie Gartencenter in Niedersachsen, Hamburg, Schleswig-Holstein, Nordrhein-Westfalen und Hessen. In 14 Fällen gelang es den Tätern, Kartendaten und PIN zu erlangen. Die mit diesen Daten hergestellten „white plastics“ wurden überwiegend in den USA, in Mexiko sowie in Kolumbien eingesetzt. In weiteren acht Fällen konnten die manipulierten POS-Terminals aufgrund unterschiedlicher Sicherungssysteme und Präventionsmaßnahmen frühzeitig entdeckt werden, bevor auch hier Kartendaten und PIN in den Besitz der Täter gelangt sind.

2.2.3 Manipulationen von Fahrkarten- und Tankautomaten

2011 wurden in Deutschland erstmals Manipulationen von Fahrkartenautomaten der Deutschen Bahn AG festgestellt. Insgesamt sind 25 Fälle aus Rheinland-Pfalz, Nordrhein-Westfalen, Niedersachsen, Hamburg und Berlin gemeldet worden. Da der Anteil der Kartenzahlungen im Vergleich zu Barzahlungen an den betroffenen Fahrkartenautomaten relativ niedrig ist, konnten die Täter bei diesen Manipulationsfällen nur verhältnismäßig wenige Kartendaten und PIN erlangen.

Nachdem im Jahr 2010 erstmals zwei Fälle der Manipulation von unbeaufsichtigten Tankautomaten registriert wurden, sind 2011 insgesamt sechs Fälle in Nordrhein-Westfalen und Rheinland-Pfalz bekannt geworden, bei denen Kartendaten und PIN an unbeaufsichtigten Tankstellen von Supermärkten abgegriffen wurden. In einem Fall wurden dabei über einen Zeitraum von mehreren Wochen über Tausend Kartendaten und PIN erlangt.

Sicherstellte Geräte und Bauteile für die Herstellung von Skimming-Equipment

[5] Point of Sale-Terminals = Kassenterminals.

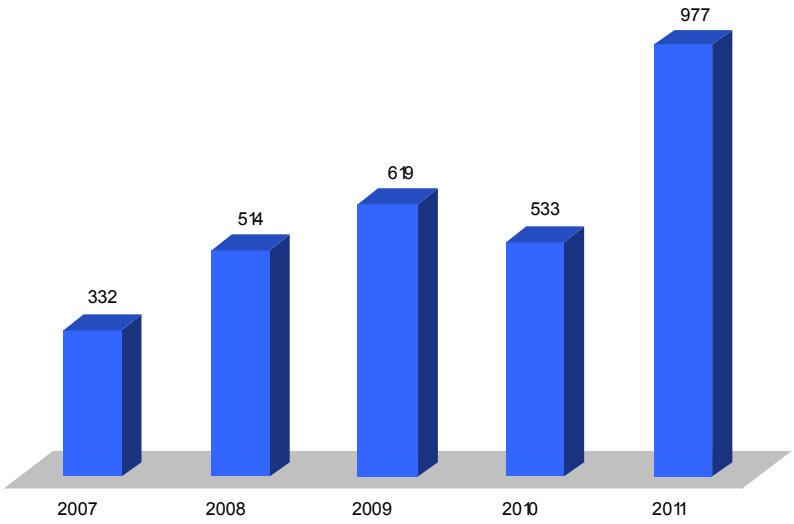
2.3 Manipulationen von Geldautomaten und POS-Terminals im Ausland

Im Jahr 2011 wurden im Ausland bei Manipulationen von insgesamt 977 Geldautomaten und POS-Terminals deutsche Kartendaten abgegriffen. Das entspricht einer Steigerung von 83 % gegenüber 2010 (533 Geldautomaten). Am häufigsten erfolgten die Datenabgriffe in Italien, Frankreich und der Türkei.

Die Zahl der registrierten Fälle steht jedoch unter dem Vorbehalt, dass in vielen Auslandsfällen der „Point of Compromise“ (PoC)[6] nicht eindeutig identifiziert werden kann und somit eine Vielzahl von Fällen nicht in die Statistik einfließt.

Es liegen keine gesicherten Erkenntnisse vor, die belegen könnten, dass ein Zusammenhang zwischen dem Rückgang der nationalen Skimming-Fälle und dem Anstieg der Auslandsfälle besteht.

Manipulierte Geldautomaten und POS-Terminals im Ausland mit Abgriffen deutscher Kartendaten (2007 - 2011)



Im Jahr 2011 wurden aus der Türkei (insbesondere aus den Urlaubsregionen Antalya und Side) zahlreiche Fälle mit einem neuen besonderen Modus Operandi gemeldet. Betroffen waren Urlauber, die zur Abhebung von Bargeld eine Wechselstube aufsuchten. Die Geschädigten nutzten nach Aufforderung durch den Inhaber/Mitarbeiter der Wechselstube ein mobiles Terminal (POS-Terminal). Nach Einführen der Zahlungskarte und Eingabe der PIN wurde der Vorgang dann aufgrund einer angeblichen Systemstörung abgebrochen. Die Kunden erhielten daraufhin ein anderes POS-Terminal, an dem nach Eingabe von Karte und PIN die Transaktion genehmigt wurde und die Geldauszahlung problemlos erfolgte. Die Täter erhielten über das erste, angeblich nicht funktionierende POS-Terminal die

[6] 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).

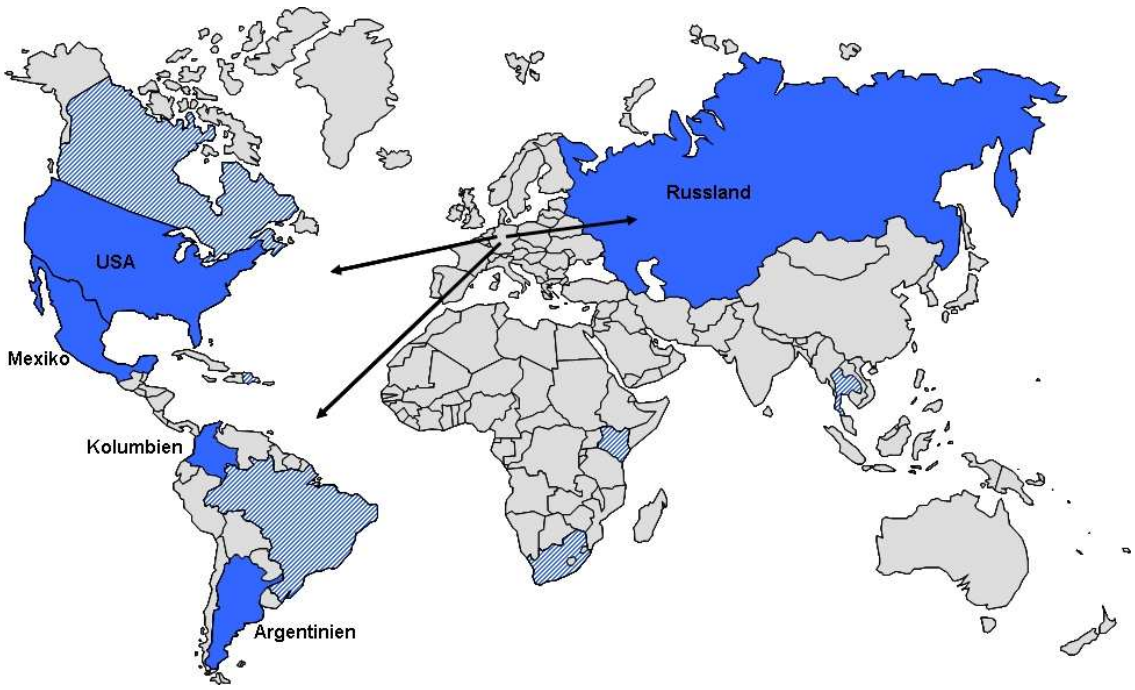
Kartendaten und PIN. Anschließend wurden mit den erlangten Daten „white plastics“ hergestellt, die überwiegend an Geldautomaten in Thailand für betrügerische Geldabhebungen eingesetzt wurden.

2.4 Einsatz gefälschter Debitkarten mit deutschen Kartendaten

Seit dem 01.01.2011 werden 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[7], in sogenannte „Nicht-Chip-Länder“, zu verlagern.

Während im ersten Halbjahr 2010 der Einsatz gefälschter Debitkarten noch überwiegend in Europa erfolgte, zeichnete sich bereits in der zweiten Jahreshälfte 2010 eine Verlagerung der missbräuchlichen Karteneinsätze in den außereuropäischen Raum ab. 2011 wurden gefälschte Debitkarten vorrangig in den USA, Russland, Mexiko, Argentinien und Kolumbien eingesetzt. Als weitere Verwertungsländer wurden u. a. Kanada, die Dominikanische Republik, Brasilien, Südafrika, Kenia, der Libanon und Thailand sowie zahlreiche weitere Länder in Südamerika, Asien und Afrika registriert.

Haupteinsatzländer gefälschter Debitkarten mit deutschen Kartendaten



[7] Mit Ausnahme Russlands („Nicht-Chip-Land“).

2.5 Tatverdächtige

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 positive Entwicklung im Bereich der „Skimming-Kriminalität“ in Deutschland hatte sich bereits im zweiten Halbjahr 2010 mit Beginn des Umstellungsprozesses auf Chipkarten abgezeichnet. Ob die deutlich gesunkenen Fallzahlen für das Jahr 2011 auf eine anhaltende Entwicklung hindeuten und mit einem weiteren Rückgang der Fallzahlen in den nächsten Jahren zu rechnen ist, bleibt abzuwarten.

Zu dem starken Rückgang der Fallzahlen haben verschiedene Faktoren beigetragen. Neben dem Abbau bzw. der sicherheitstechnischen Aufrüstung der Türöffner bei Geldinstituten hat der im Jahr 2010 im Bankenbereich erfolgte 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.

Auch die neuen Modi Operandi (Manipulationen von Fahrkarten- oder Tankautomaten) oder die erneut festgestellten POS-Terminal-Manipulationen werden die positive Gesamtentwicklung im Skimming-Bereich nicht grundlegend verändern. Die aktuellen Maßnahmen der Geldinstitute entfalten ihre positive Wirkung auch bei den vorgenannten Vorgehensweisen, so dass auch diese spezifischen Skimming-Fälle künftig aufgrund eingeschränkter Verwertungsmöglichkeiten an Bedeutung verlieren werden.

Bundeskriminalamt

65173 Wiesbaden

info@bka.de

www.bka.de