



Bundeskriminalamt

ZAHLUNGSKARTEN- KRIMINALITÄT

Bundeslagebild 2011



ZAHLUNGSKARTENKRIMINALITÄT

Bundeslagebild 2011

Bundeskriminalamt

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

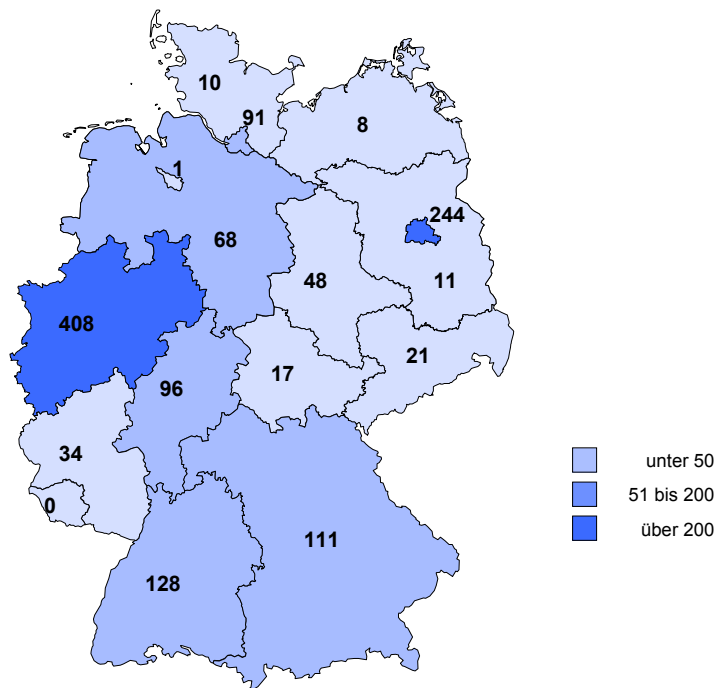
1. VORBEMERKUNG

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.

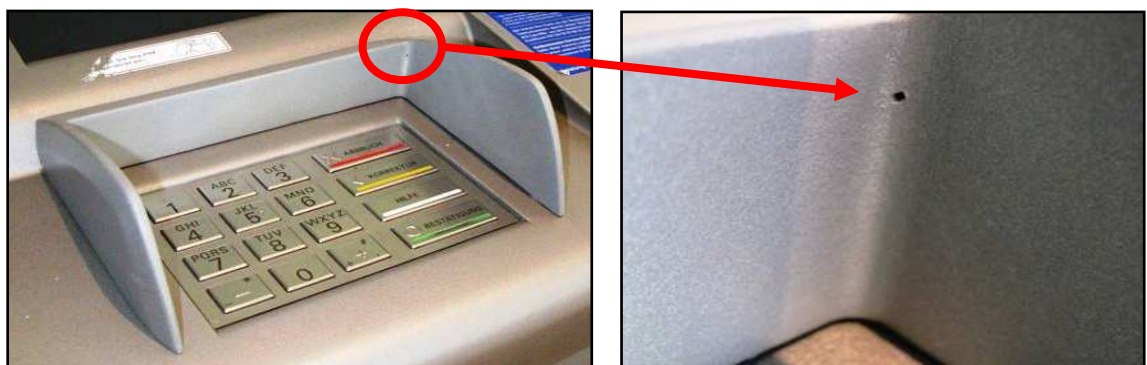
Die Angriffe auf Geldautomaten erfolgten 2011 nahezu im gesamten Bundesgebiet. Lediglich das Saarland war nicht betroffen. Die meisten Angriffe wurden in Nordrhein-Westfalen (408 Fälle) und Berlin (244 Fälle) verübt.

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 POS⁵-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.

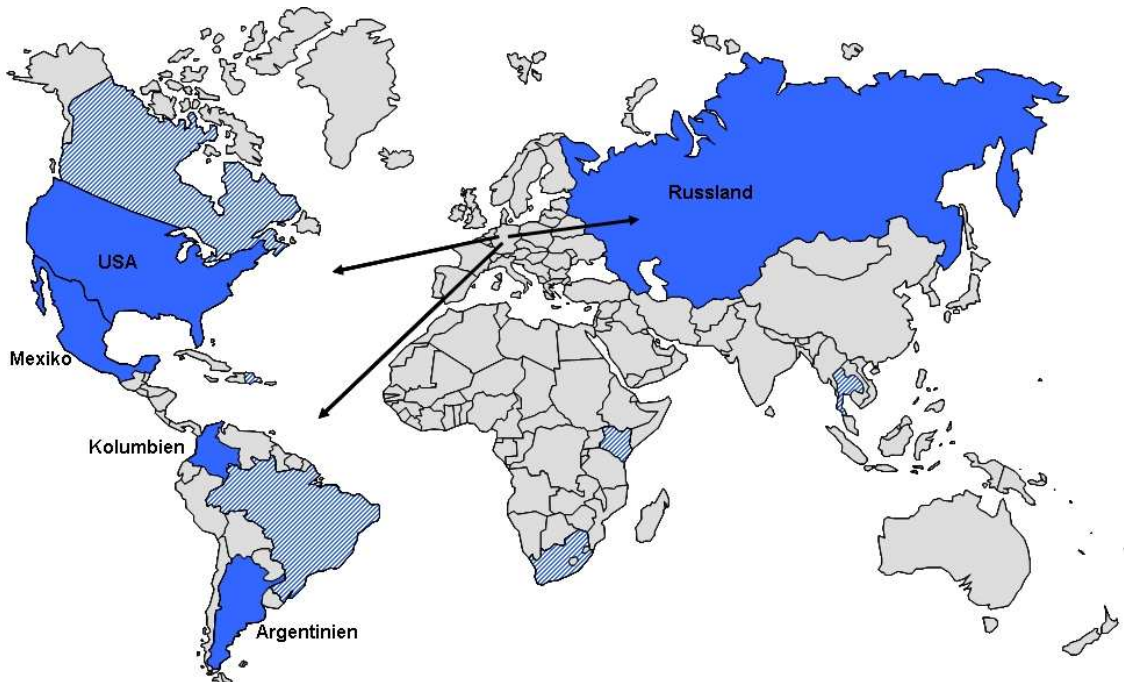
Kartendaten und PIN. Anschließend wurden mit den erlangten Daten „white plastics“ hergestellt, die überwiegend an Geldautomaten in Thailand für betrügerische Geldabhebungen eingesetzt wurden.

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 Ausland⁷, 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“).

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