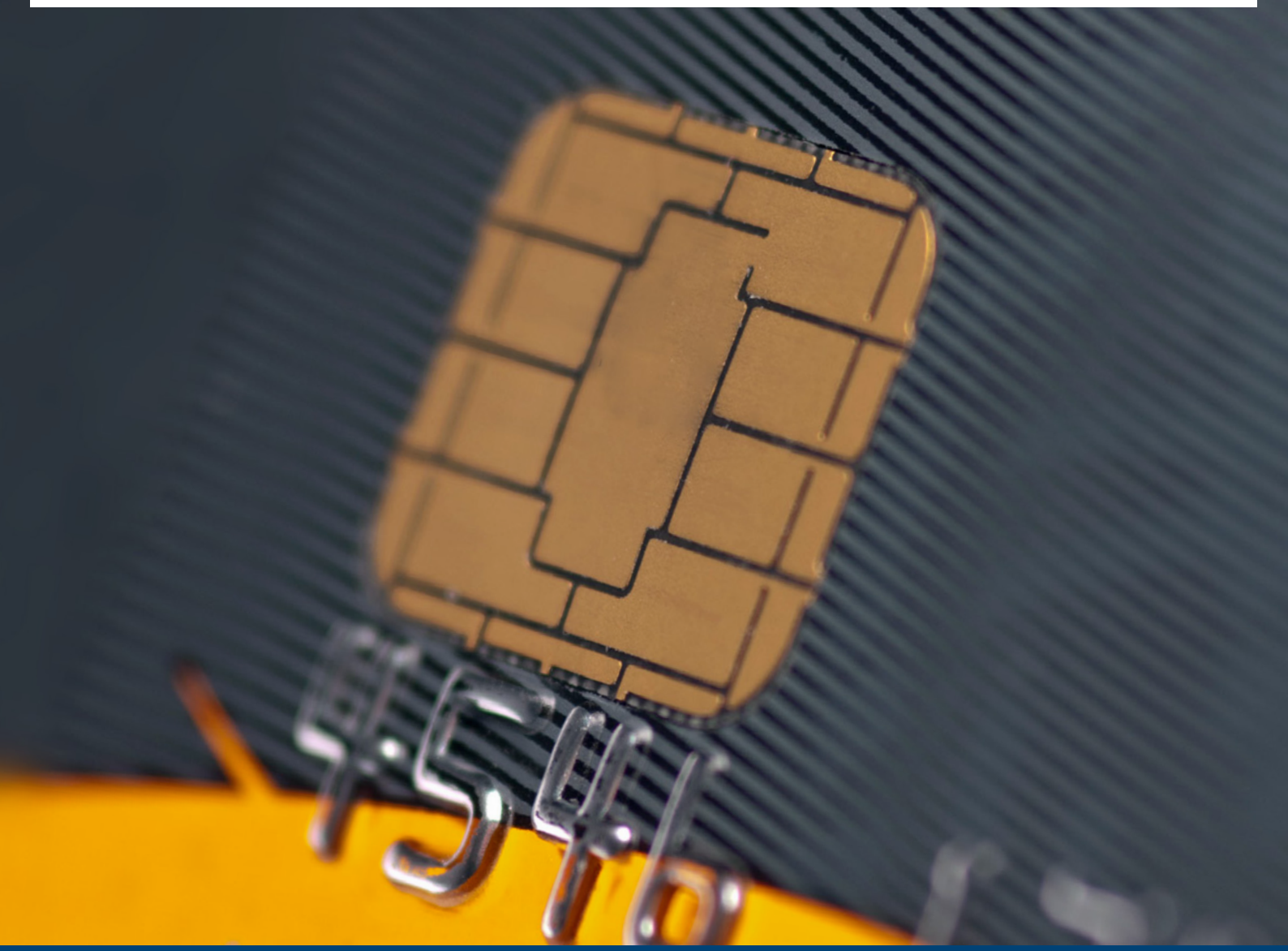
Bundeskriminalamt



Zahlungskarten-kriminalität

Bundeslagebild 2014

INHALT

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-[01] und Kreditkarten, die zusammenfassend als Zahlungskarten bezeichnet werden. Das Phänomen des Diebstahls digitaler Daten von Zahlungskarten und deren anschließende Verwertung im Internet werden im Bundeslagebild Cybercrime 2014 dargestellt.

2. DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

Inhaber von Zahlungskarten deutscher Emittenten verfügen im internationalen Vergleich über eine hohe Bonität. Daher sind deren Karten bzw. Kartendaten bevorzugtes Ziel von Straftätergruppierungen. Das Bundeskriminalamt schätzt, dass in Deutschland über 130 Mio. Zahlungskarten im Gebrauch sind, davon rund drei Viertel Debitkarten 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 2014 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. Dem Bundeskriminalamt liegen aufgrund der Informationspolitik der Deutschen Kreditwirtschaft keine Daten zu Verlusten und Missbrauchsumsätzen vor.
Angaben zur Schadenhöhe lassen sich nur aus vereinzelten Presseveröffentlichungen der Firma EURO-Kartensysteme (EKS) ableiten. Deren Angaben zufolge beläuft sich der Schaden aus Skimming-Fällen[03] zum Nachteil deutscher Kreditinstitute 2014 auf ca. 2,8 Mio. Euro. Aufgrund internationaler Haftungsregelungen (Liability Shift) ergibt sich bei verschiedenen Staaten die Möglichkeit der Schadenrückbelastung an das Land, in dem die betrügerischen Geldabhebungen erfolgt sind. Es liegen jedoch keine Angaben zur Höhe der insgesamt im Rahmen der Haftungsumkehr rückbelasteten Umsätze vor.

Chiptechnik schränkt Fälschungsmöglichkeiten ein

Nach wie vor bevorzugen die Täter das Fälschen von Debitkarten mit zuvor ausgespähten Magnetstreifendaten. Mit gefälschten Karten bieten sich bessere Einsatzmöglichkeiten als mit gestohlenen Karten, da letztere durch die Kartenorganisationen gesperrt werden, sobald der Diebstahl bemerkt wird. Dadurch werden sie für die Täterseite unbrauchbar. Seit 2011 ist es den Tätern jedoch nicht mehr möglich, die mit Magnetstreifendaten ausgestatteten Kartendubletten im SEPA-Raum[04] einzusetzen, da innereuropäisch die Abrechnung ausschließlich über den Chip und nicht mehr über den Magnetstreifen erfolgt. Dies führt zu einer Verlagerung der Verwertungstaten außerhalb des SEPA-Raums (so genannte „Nicht-Chip-Länder“).

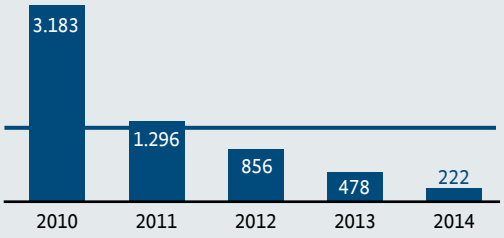
01 Debitkarten: (von englisch to debit = belasten) räumen keinen Kredit ein; bei Zahlungen mit Debitkarten wird das Konto sofort belastet. Die bekannteste Debitkarte in Deutschland ist die von Banken und Sparkassen ausgegebene ec-Karte.
02 Die im Bundeslagebild angeführten Falldaten basieren auf Erkenntnissen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

2.1 MANIPULATIONEN IM INLAND

Deutlicher Rückgang der Angriffe auf Geldautomaten

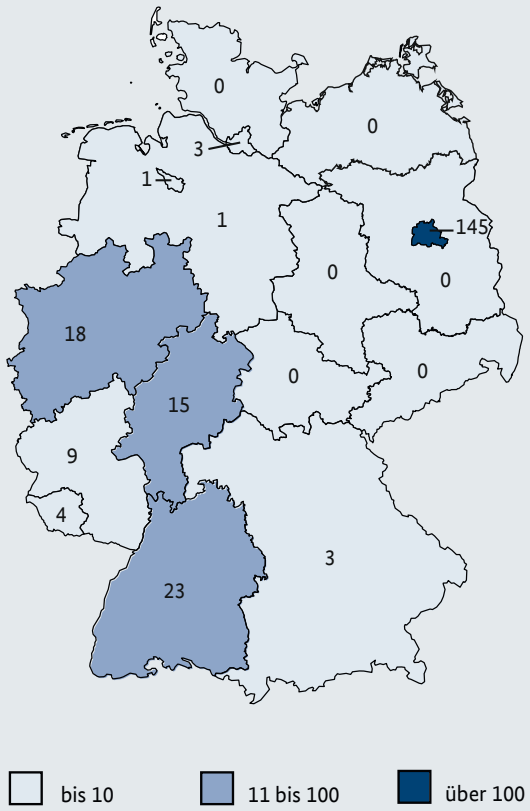
Die seit 2011 in Deutschland festzustellende rückläufige Entwicklung der Skimming-Fälle bei Geldautomaten setzte sich auch im Jahr 2014 fort. Es wurden 222 Angriffe auf Geldautomaten zur Erlangung von Kartendaten (Magnetstreifendaten) und PIN registriert, ein Rückgang um 54 %. Die aktuelle Fallzahl liegt deutlich (82 %) unter dem Mittelwert der letzten fünf Jahre (1.207 Fälle).

Anzahl der Angriffe auf Geldautomaten in Deutschland 2010 - 2014



Bedingt durch Mehrfachangriffe einzelner Geldautomaten waren 2014 bundesweit 138 Automaten (2013: 341) betroffen, ein Rückgang von 60 %.
Durch den Abbau bzw. die sicherheitstechnische Aufrüstung von Türöffnern zu Bankfoyers sind Kartendatenabgriffe in diesem Bereich nahezu bedeutungslos geworden. Im Jahr 2014 ist der Datenabgriff lediglich in 15 Fällen durch Türöffnermanipulationen erfolgt. Der überwiegende Teil dieser Fälle konnte einer Serie zugeordnet werden, die im Zeitraum Juni bis August 2014 in der Region Trier/Saarbrücken erfolgt ist.

Angriffe auf Geldautomaten nach Bundesländern 2014



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 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 das Auslesen der Kartendaten erheblich.

Keine POS-Terminalmanipulationen in Deutschland

Im Jahr 2014 wurden in Deutschland keine POS-Terminals[05] (2013: 84 Terminals) manipuliert. Bei sieben POS-Terminal-Fällen kam es im Jahr 2014 zwar zu Schadensfällen (Einsätze von „White Plastics“[06] in mehreren asiatischen Ländern), die entsprechenden Manipulationsfälle (Datenabgriffe) ereigneten sich jedoch bereits im Jahr 2013.

Manipulationen von Tankautomaten

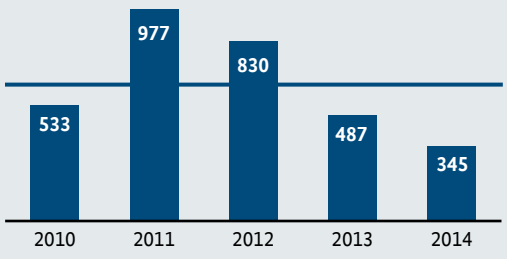
Im Jahr 2014 erfolgten im Inland Skimming-Attacken an Tankautomaten im niedrigen zweistelligen Bereich. Bei diesen Vorfällen wurden jedoch nicht die Daten von Debit- oder Kreditkarten, sondern Daten (Magnetstreifendaten und PIN) von Tankkarten erlangt. Attackiert wurden die Tankautomaten mehrerer Mineralölunternehmen, die in Deutschland und dem benachbarten Ausland Tankstationen ohne Personal betreiben. Die mit diesen Daten versehenen „White Plastics“ können nur an Tankautomaten missbräuchlich eingesetzt werden. Gleichartige Vorgehensweisen wurden auch aus anderen europäischen Staaten gemeldet.

2.2 MANIPULATIONEN IM AUSLAND

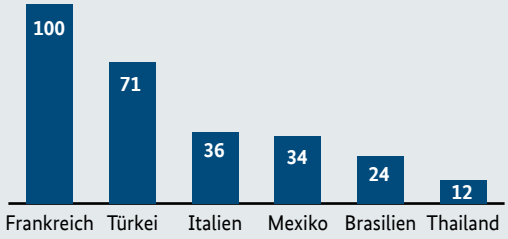
Weiterhin Abgriffe deutscher Kartendaten im Ausland

Im Jahr 2014 wurden im Ausland bei Manipulationen von insgesamt 345 Geldautomaten und POS-Terminals deutsche Kartendaten und PIN abgegriffen, ein Rückgang von 29 %. Zudem liegt die Fallzahl um 46 % unter dem Durchschnittswert der letzten fünf Jahre (634 Fälle). 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)[07] 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 2010 - 2014



Staaten, in denen deutsche Kartendaten 2014 am häufigsten ausgespäht wurden



05 POS: Point of Sale-Terminals = Kassenterminals.
06 „White Plastics“ = Rohlinge von Magnetstreifenkarten.
07 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).

2.3 EINSATZ GEFÄLSCHTER DEBITKARTEN MIT DEUTSCHEN KARTENDATEN

Haupteinsatzgebiete vorwiegend in Amerika und Südostasien

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.
Neben den in der nachfolgenden Grafik dargestellten Haupteinsatzgebieten gefälschter deutscher Debitkarten im Jahr 2014 wurden zahlreiche weitere Verwertungsstaaten weltweit registriert.

Haupteinsatzstaaten gefälschter Debitkarten mit deutschen Kartendaten 2014

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 und bulgarische Staatsangehörige. 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.

3. GESAMTBEWERTUNG

Wie in den Vorjahren haben sich im Jahr 2014 die Fallzahlen des „Skimming“ im Bereich der Manipulation von Geldautomaten erneut deutlich rückläufig entwickelt. Zudem wurden im Jahr 2014 keine Manipulationsfälle von POS-Terminals registriert.
Der starke Rückgang der Fallzahlen beruht insbesondere auf der im SEPA-Raum erfolgten Umstellung auf die Chiptechnologie. Darüber hinaus haben die seit mehreren Jahren wirksamen Maßnahmen der Kreditwirtschaft wie der Austausch von Geldautomaten „älterer Bauart“ und der Einsatz wirksamer Anti-Skimming-Module das Auslesen der Magnetstreifendaten einer Zahlungskarte durch die Täterseite zunehmend erschwert. Letztlich haben die von zahlreichen Geldinstituten zusätzlich ergriffenen Maßnahmen, die zusammenfassend mit dem Begriff „Magstripe-Controlling“ bezeichnet werden, die Einsatzmöglichkeiten gefälschter Karten erheblich beschränkt. Die „Magstripe-Controlling“-Strategie umfasst beispielsweise die grundsätzliche Deaktivierung der Magnetstreifen. Die Aktivierung des Magnetstreifens für den Einsatz in „Nicht-Chip-Ländern“ kann dabei nur auf Initiative des Kunden erfolgen. Weiterhin können Einsatzmöglichkeiten in Risikoländern reduziert und Limits für Auslandsabhebungen festgelegt werden.
Der vollständige Rückgang der POS-Terminal-Manipulationen basiert zum Teil auf erfolgreichen Maßnahmen der Strafverfolgungsbehörden gegen Tätergruppierungen, die im Jahr 2013 für die in Deutschland erfolgten Manipulationen verantwortlich waren. Zudem ist davon auszugehen, dass die Netzbetreiber, Terminalhersteller und vor allem Groß- und Einzelhandelsunternehmen durch den intensiven Informationsaustausch sowie die Übermittlung von Warnhinweisen und Präventionsempfehlungen in die Lage versetzt wurden, POS-Terminal-Manipulationen zu erschweren.
Durch die im SEPA-Raum erfolgte Umstellung auf Chiptechnologie sowie die von vielen Kreditinstituten getroffenen Maßnahmen zur Reduzierung missbräuchlicher Transaktionen im außereuropäischen Ausland bzw. außerhalb des SEPA-Raums

a) sind die Einsatzmöglichkeiten gefälschter Karten („White Plastics“) zunehmend erschwert worden,
b) ist das Geschäft für die Täter nicht mehr so lukrativ wie in den Jahren zuvor.

Es bleibt abzuwarten, ob Zahlungskartenkriminalität in Deutschland aufgrund der derzeitigen Rahmenbedingungen dauerhaft an Bedeutung verliert oder ob die Täterseite mit einer Anpassung der Modi Operandi reagieren wird. Künftig wird mit technisch verfeinerten und teilweise gänzlich neuen Angriffsszenarien zu rechnen sein, wobei insbesondere mögliche Schwachstellen im NFC-Bereich (Near Field Communication[08]) ein noch weitgehend unerforschtes Gebiet darstellen.
Um entsprechende Tendenzen möglichst frühzeitig zu erkennen, sind insbesondere die Entwicklungen im Bereich der Chipkartenzahlungen sowie der NFC-Technik intensiv zu beobachten. Daher ist es nach wie vor von Bedeutung, den engen Informationsaustausch sowie die Kooperation mit den Netzbetreibern, den Terminalherstellern, den großen Handelsunternehmen und den Dachorganisationen des Einzelhandels fortzusetzen.

08 Internationaler Übertragungsstandard zur drahtlosen Datenübertragung über kurze Strecken. Im Zahlungskartenbereich ist insbesondere die kontaktlose Zahlungsabwicklung an Terminals von Bedeutung.

IMPRESSUM

Herausgeber
Bundeskriminalamt
65173 Wiesbaden

Stand
2014

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de