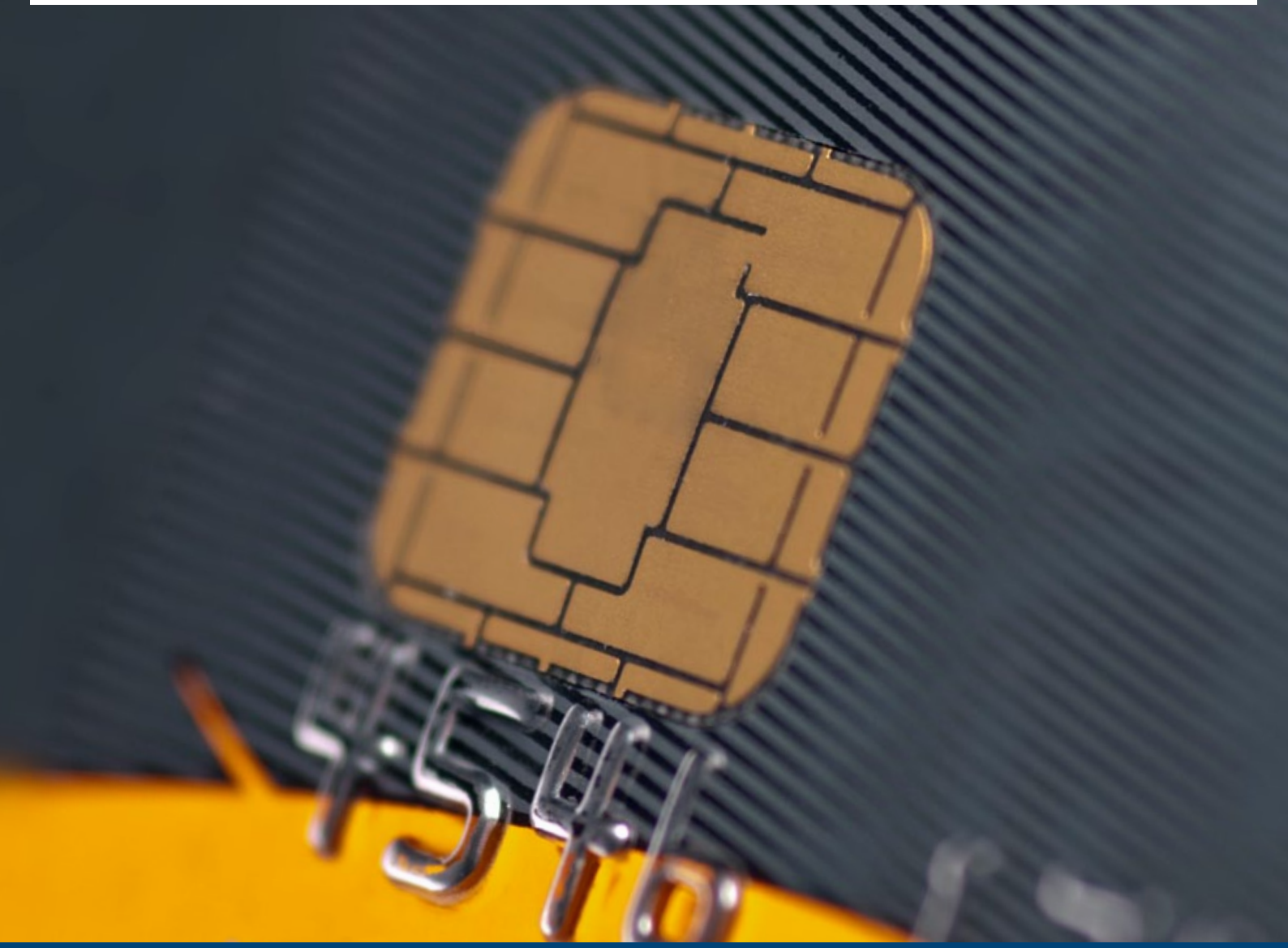
Bundeskriminalamt



Zahlungskarten-kriminalität

Bundeslagebild 2013

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- 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 2013 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 2013 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. Belastbare Schätzungen zum Schaden, der durch den Einsatz gefälschter Zahlungskarten mit deutschen Kartendaten entsteht, sind daher nicht möglich.

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. Seit 2011 ist es den Tätern nicht mehr möglich, gefälschte Debitkarten im SEPA-Raum[03] einzusetzen, da innereuropäisch die Abrechnung ausschließlich über den Chip und nicht mehr über den Magnetstreifen erfolgt. Dies führt zu einer Verlagerung der Verwertungstaten in außereuropäische Staaten (so genannte „Nicht-Chip-Länder“).

Zur Verhinderung missbräuchlicher Einsätze von Kartendaten, die durch Manipulationen von Geldautomaten, POS-Terminals etc. erlangt wurden, haben deutsche Banken und Sparkassen im Jahr 2013 die Daten von rund 85.000 Zahlungskarten gesperrt.

01 Debitkarten: (von englisch (to) debit = belasten) räumen keinen Kredit ein; bei Zahlungen mit Debitkarten wird das Konto sofort belastet.

02 Die im Bundeslagebild angeführten Falldaten basieren auf Erkenntnissen aus dem nationalen und internationalen Informationsaustausch.

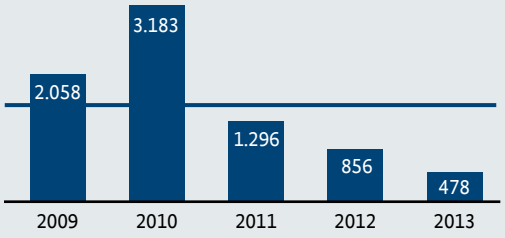
03 SEPA: Single Euro Payments Area.

2.1 MANIPULATIONEN IM INLAND

Weiterhin rückläufige Entwicklung bei Angriffen auf Geldautomaten

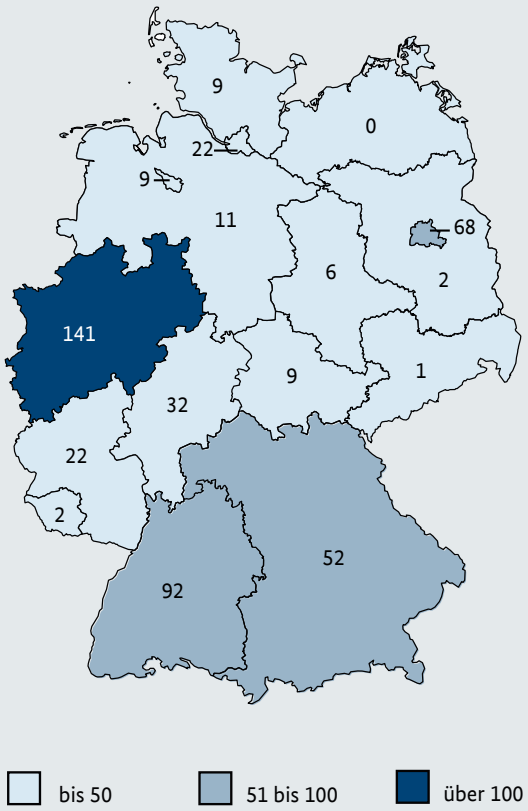
Im Jahr 2013 wurde in Deutschland mit insgesamt 478 Angriffen auf Geldautomaten zur Erlangung von Kartendaten und PIN erneut ein Rückgang der Skimming-Straftaten[04] um rund 44 % registriert. Im Verhältnis zur durchschnittlichen Zahl der Angriffe auf Geldautomaten in den letzten fünf Jahren (1.574 Fälle) liegt die aktuelle Fallzahl um 70 % deutlich unter dem Mittelwert.

Anzahl der Angriffe auf Geldautomaten in Deutschland 2009 - 2013



Bedingt durch Mehrfachangriffe einzelner Geldautomaten waren 2013 bundesweit 341 Automaten (2012: 505) betroffen, ein Rückgang von 32 %. Die Manipulationszeiträume sind oftmals sehr kurz. Sie betragen teilweise nur wenige Stunden. Durch den Abbau bzw. die sicherheitstechnische Aufrüstung von Türöffnern zu Bankfoyers sind Kartendatenabgriffe in diesem Bereich nahezu bedeutungslos geworden. Im Jahr 2013 ist der Datenabgriff lediglich in acht Fällen durch Türöffnermanipulationen erfolgt.

Angriffe auf Geldautomaten nach Bundesländern 2013



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 zur Aufzeichnung der PIN-Eingaben. Zum Teil werden unmittelbar auf der Originaltastatur Tastaturattrappen angebracht, die die eingegebenen PIN-Daten speichern. Vereinzelt erfolgt die Anbringung von Skimming-Equipment auch im Inneren der Geldautomaten.
Die Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen (mechanisch und elektronisch) erschwert der Täterseite jedoch zunehmend den erfolgreichen Einsatz ihrer Skimming-Technik.

04 Skimming: Auslesen der Kartendaten einer Zahlungskarte und das Übertragen auf eine Kartenfälschung

Erneuter Anstieg der Manipulationsfälle von POS-Terminals [05]

Im Jahr 2013 wurden in Deutschland insgesamt 84 manipulierte POS-Terminals festgestellt (2012: 77 Terminals). Hiervon haben die Täter in 24 Fällen die Kartendaten und PIN erfolgreich ausgespäht (2012: 50 Fälle, - 52 %) und diese anschließend im außereuropäischen Ausland eingesetzt. In den anderen 60 Fällen konnte die Manipulation aufgrund unterschiedlicher Sicherungssysteme und Präventionsmaßnahmen frühzeitig erkannt werden, bevor es zu missbräuchlichen Umsätzen kommen konnte.
In weiteren etwa 400 Fällen wurden POS-Terminals in Geschäften aufgrund von Verdachtsmeldungen vorsorglich durch die Netzbetreiber ausgetauscht, da Manipulationen nicht ausgeschlossen werden konnten.
Im Jahr 2013 waren die Geräte verschiedener Hersteller von POS-Terminal-Manipulationen betroffen.

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 spätestens am nächsten Tag 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 bei allen Varianten innerhalb des POS-Terminals installiert. Die Veränderungen sind daher 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.
Inzwischen gibt es erste technische Sicherheitsmaßnahmen, mit denen POS-Terminal-Manipulationen frühzeitig erkannt werden können. Diese Maßnahmen kommen jedoch noch nicht flächendeckend zum Einsatz.

05 Point of Sale-Terminals = Kassenterminals.

2.2 MANIPULATIONEN VON GELDAUTOMATEN UND POS-TERMINALS IM AUSLAND

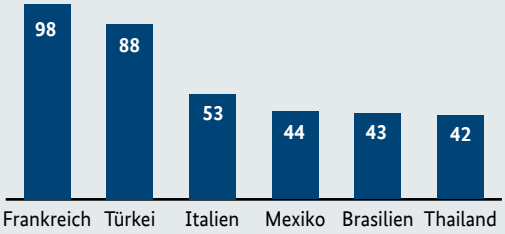
Weiterhin Abgriffe deutscher Kartendaten im Ausland

Im Jahr 2013 wurden im Ausland bei Manipulationen von insgesamt 487 Geldautomaten und POS-Terminals deutsche Kartendaten abgegriffen. Das entspricht einem Rückgang von rund 41 % gegenüber 2012. Zudem liegt die aktuelle Fallzahl um 29 % deutlich unter dem durchschnittlichen Wert der letzten fünf Jahre (689 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)[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 2009 - 2013

Staaten, in denen deutsche Kartendaten 2013 am häufigsten ausgespäht wurden



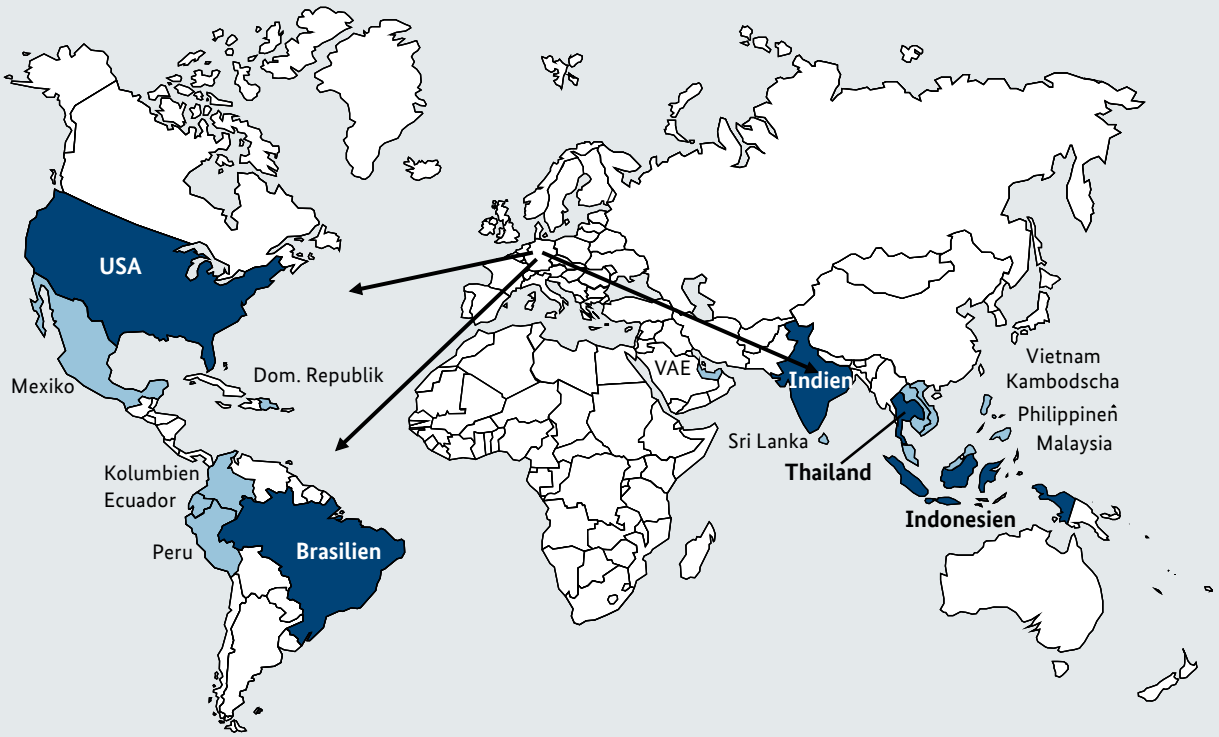
2.3 EINSATZ GEFÄLSCHTER DEBITKARTEN MIT DEUTSCHEN KARTENDATEN

Haupteinsatzgebiete vorwiegend in Amerika, Indien und Südostasien

Seit 2011 werden Transaktionen mit Debitkarten im SEPA-Raum nur noch über den Chip autorisiert. Dadurch sind die Täter gezwungen, den Einsatz ihrer noch auf Magnetstreifenbasis funktionierenden „White Plastics“ ins außereuropäische Ausland zu verlagern.
Im Jahr 2013 wurden die gefälschten Zahlungskarten am häufigsten in den USA, gefolgt von Brasilien, Indonesien, Indien und Thailand eingesetzt. Neben den in der nachfolgenden Grafik dargestellten Einsatzgebieten gefälschter deutscher Debitkarten wurden in Einzelfällen weitere Verwertungsstaaten in Mittel- und Südamerika, Asien und Afrika registriert.

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).

Haupteinsatzstaaten gefälschter Debitkarten mit deutschen Kartendaten 2013



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 Straftäter spielen in diesem Kriminalitätsbereich nahezu keine Rolle.
Für die 2013 in Deutschland festgestellten Fälle von POS-Terminal-Manipulationen war neben mehreren rumänischen Tätergruppierungen auch eine international organisierte kanadische Tätergruppe verantwortlich, die im gleichen Zeitraum auch Taten in Frankreich verübt hat. 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 Täter agieren in kleinen Gruppen und halten sich zum Abgriff der Kartendaten meist nur relativ kurze Zeit, in einzelnen Fällen aber auch 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 dem Beginn des Umstellungsprozesses auf Chipkarten festzustellende positive Entwicklung bei der Bekämpfung der „Skimming-Kriminalität“ in Deutschland hat sich auch 2013 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 beispielsweise die grundsätzliche Deaktivierung der Magnetstreifen, 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.
Trotz der im Jahr 2013 leicht gestiegenen Zahl manipulierter POS-Terminals konnte in rund zwei Dritteln der Fälle aufgrund verschiedener technischer Sicherungssysteme und Präventionsmaßnahmen verhindert werden, dass die Täter in den Besitz der ausgespähten Daten gelangt sind.

Aufgrund der Entwicklung der Fallzahlen 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.
Es bleibt abzuwarten, ob die rückläufige Entwicklung der Skimming-Angriffe auf Geldautomaten anhält und auch die Manipulation von POS-Terminals aufgrund der eingeschränkten Verwertungsmöglichkeiten der erlangten Kartendaten an Bedeutung verlieren wird oder ob die Täter mit einer Anpassung der Modi Operandi an die Sicherheitsmaßnahmen im Bereich des unbaren Zahlungsverkehrs reagieren werden.

IMPRESSUM

Herausgeber
Bundeskriminalamt
65173 Wiesbaden

Stand
2013

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de