Bundeskriminalamt

BKA

Angriffe auf Geldautomaten

Bundeslagebild 2016

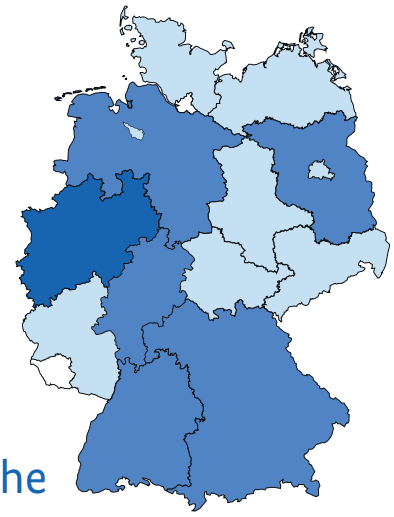
Sprengung von Geldautomaten

318 (+102 %)
Sprengungen

Brennpunkt
Nordrhein-Westfalen

45
Festnahmen

darunter **20** niederländische
Tatverdächtige



Phänomenbetroffene Länder

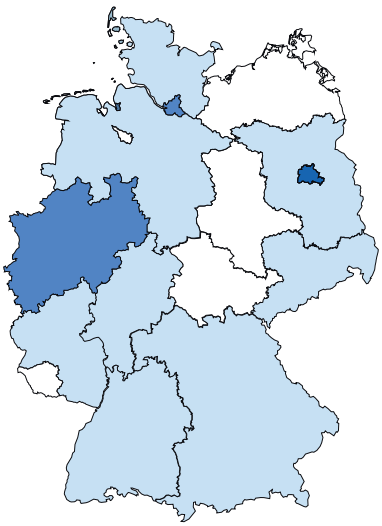
Technische Manipulation von Geldautomaten - Skimming

369 (+ 94 %)
Skimming-Fälle

Brennpunkt Berlin

überwiegend Tatverdächtige
aus Bulgarien, Rumänien und
Republik Moldau

1,9 Mio. €
Schaden



Phänomenbetroffene Länder

fortlaufend neue Modi Operandi

Inhalt

1 Vorbemerkung

Das Bundeslagebild „Angriffe auf Geldautomaten“[01] enthält im Überblick die aktuellen Erkenntnisse des Bundeskriminalamtes zu physischen Angriffen auf und technischen Manipulationen von Geldautomaten mit dem Ziel der Erlangung von Bargeld.

Hinsichtlich der physischen Angriffe auf Geldautomaten betreibt das Bundeskriminalamt eine Sonderauswertung zu Sprengungen von Geldautomaten. Die Daten hierzu basieren weitgehend auf den Informationen, die dem Bundeskriminalamt aus dem polizeilichen Nachrichtenaustausch bekannt geworden sind. Gleiches gilt für Diebstähle von Geldautomaten. Diese Informationen werden durch Erkenntnisse zu unterschiedlichen Modi Operandi ergänzt.

Der Bereich der technischen Manipulationen von Geldautomaten umfasst primär das Fälschen von Zahlungskarten mit zuvor ausgespähten Magnetstreifendaten (sog. Skimming) und den anschließenden Einsatz dieser Karten zur Erlangung von Bargeld. Darüber hinaus beinhaltet dieser Teil des Lagebildes die dem Bundeskriminalamt vorliegenden Erkenntnisse zur Manipulation von „Point-of-Sale“-Terminals (POS-Terminals), zu Skimming-Verwertungstaten im Ausland sowie zu weiteren Modi Operandi der technischen Manipulation von Geldautomaten.

Das Phänomen des Diebstahls digitaler Daten von Zahlungskarten und deren anschließende Verwertung im Internet werden im Bundeslagebild Cybercrime dargestellt.

01 Der Begriff „Geldautomat“ wird in diesem Lagebild [auch für Geldausgabeautomat] durchgängig verwendet.

2 Darstellung und Bewertung der Kriminalitätslage „Physische Angriffe“ auf Geldautomaten

2.1 Besonders schwere Fälle des Diebstahls aus Geldautomaten

Besonders schwere Fälle des Diebstahls aus Geldautomaten werden in der Polizeilichen Kriminalstatistik nicht gesondert erfasst. Dem Bundeskriminalamt wird zudem im Rahmen des Kriminalpolizeilichen Meldedienstes nur ein Teil der tatsächlichen Fälle bekannt.

Unter Berücksichtigung der dem Bundeskriminalamt vorliegenden polizeilichen Erkenntnisse ist davon auszugehen, dass sich im Jahr 2016 rund 700 besonders schwere Fälle des Diebstahls aus Geldautomaten ereigneten. Im Vergleich zum Vorjahr 2015 (ca. 400 Angriffe) hat sich die Zahl fast verdoppelt.

Gemäß der dem Bundeskriminalamt vorliegenden polizeilichen Erkenntnisse finden außerdem folgende Modi Operandi Anwendung:

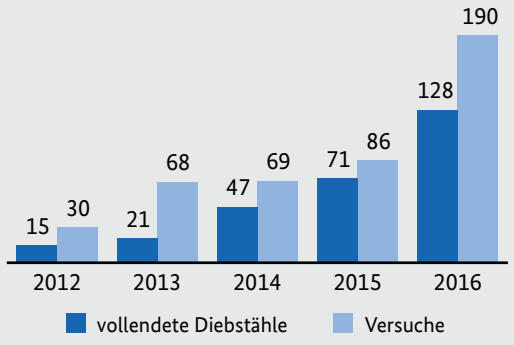
- Sprengung von Geldautomaten
- Öffnung von Geldautomaten
  - mit Winkelschleifern
  - mit hydraulischen Spreizern
  - mit manuellen Hebelwerkzeugen (z. B. Brecheisen, Spaltkeile)
  - mit thermischen Schneidgeräten (z. B. autogene Schneidbrenner)
- Komplettentwendung von Geldautomaten (durch Herausreißen oder Demontage aus dem Aufstellort)

2.2 Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten

Nach Erkenntnissen des Bundeskriminalamtes werden Geldautomaten häufig durch Einleitung eines Gases bzw. Gasgemisches und dessen anschließende Zündung gesprengt. Ausgehend von diesem Grundprinzip unterscheiden sich die Tatbegehungen insbesondere in Bezug auf die Art des Gases, die eingeleitete Menge und den Ort der Einleitung, die Zündquelle und die Zündleitung. In Einzelfällen wurde gewerblicher oder militärischer Sprengstoff, teilweise auch Pyrotechnik, zur Sprengung eingesetzt.

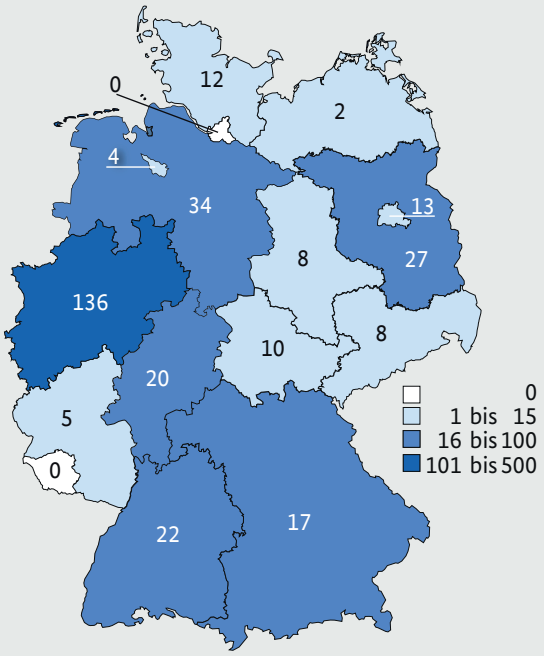
Im Jahr 2016 wurden dem Bundeskriminalamt im Phänomenbereich „Sprengung von Geldautomaten" 318 Fälle bekannt. In 128 Fällen gelangten die Täter an Bargeld (ca. 40 %), in 190 Fällen blieb es beim versuchten Diebstahl.

Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten (inkl. Versuche) in Deutschland – Fallentwicklung



Die Entwicklung der Fallzahlen bleibt insbesondere bei vollendeten Taten seit 2012 weiterhin steigend. Gegenüber dem Vorjahr 2015 haben sowohl die vollendeten Taten (+ 80 %) als auch die Versuche (+ 121 %) deutlich zugenommen.

Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten in Deutschland – Fallbelastung nach Ländern (2016)



Der regionale Schwerpunkt liegt wie im vergangenen Jahr weiterhin in Nordrhein-Westfalen. Auffällig bei der Betrachtung der Tatörtlichkeit bleibt die hohe Anzahl von Tatorten in der Nähe zur Grenze zwischen den Niederlanden und Deutschland. Mehrere Indikatoren sprechen für einen Verdrängungseffekt eines Teils dieses Kriminalitätsphänomens aus den Niederlanden nach Deutschland, wie beispielsweise die Herkunft der Tätergruppierungen, verstärkte Präventionsmaßnahmen der Geldinstitute in den Niederlanden sowie intensive repressive Maßnahmen der niederländischen Strafverfolgungsbehörden.

Darüber hinaus sind die Länder Niedersachsen, Brandenburg, Baden-Württemberg, Hessen und Bayern überdurchschnittlich betroffen. Das relativ hohe Fallaufkommen in Baden-Württemberg und Bayern stellt eine neue Entwicklung dar. Im Vorjahr ereigneten sich in diesen beiden Ländern nur wenig entsprechende Straftaten (BW: 2, BY: 0).

Bei der Auswahl der Tatobjekte bevorzugen die Täter Geldautomaten, die sich in ländlichen Regionen oder am Stadtrand befinden und eine gute Verkehrsanbindung aufweisen.

Physische Angriffe auf Geldautomaten werden in der Regel arbeitsteilig durch Tätergruppierungen begangen. Nur in wenigen Fällen sind Einzeltäter aktiv. Im Rahmen der Ermittlungen konnten sowohl reisende als auch regionale Straftätergruppierungen identifiziert werden.

Gemäß der dem Bundeskriminalamt vorliegenden Informationen wurden im Jahr 2016 in Deutschland insgesamt 45 Tatverdächtige im Zusammenhang mit Sprengungen von Geldautomaten festgenommen.

Nach Erkenntnissen des Bundeskriminalamtes sind niederländische Gruppierungen in diesem Phänomenbereich in Deutschland besonders aktiv. Dies belegt u. a. die verhältnismäßig große Anzahl an Festnahmen von niederländischen Tatverdächtigen (20) im Jahr 2016. Neben Tätergruppierungen aus den Niederlanden sind in Deutschland vor allem polnische Tätergruppierungen bei Geldautomatensprengungen aktiv. Zwar erfolgten im Jahr 2016 nur drei Festnahmen von Tatverdächtigen aus Polen, jedoch ergaben sich aus Ermittlungsverfahren zu entsprechenden Straftaten zahlreiche Hinweise auf die Tatbeteiligung polnischer Tatverdächtiger/Gruppierungen.

Durch Sprengungen von Geldautomaten entstehen im Einzelfall erhebliche Gefahren für unbeteiligte Dritte. Auch wenn in den meisten Fällen Tatzeiten und Tatörtlichkeiten ausgewählt werden, in denen keine Kundenfrequenz mehr zu erwarten ist, verbleibt ein Risiko für Leib und Leben von Passanten und Bewohnern der betroffenen Objekte. Unabhängig vom Aufstellungsort des Geldautomaten kann es zu einer Trümmer- und Splitterverteilung kommen, die von den Tätern nicht abgeschätzt werden kann. Zudem können Einsatzkräfte von Feuerwehr und Polizei einer erheblichen Gefährdung ausgesetzt sein.

Der durch die Straftaten verursachte Sachschaden übersteigt den Beuteschaden in vielen Fällen deutlich. Bei einzelnen Straftaten entstand ein Sachschaden in sechsstelliger Höhe.

2.3 Cash-Trapping

Eine weitere Angriffsvariante ist die Unterschlagung in Form des sog. Cash Trapping. Dabei wird der Geldausgabeschacht von Geldautomaten durch das Anbringen eines täuschend echt aussehenden Verschlusses präpariert. Dieser ist innen mit einer doppelseitigen Klebefolie versehen, die verhindert, dass das Geld ausgegeben oder wieder vom Automaten eingezogen wird. Die ausgegebenen Geldscheine bleiben im Ausgabeschacht an der Klebefolie haften. Der Bankkunde bemerkt davon nichts. Der Geldauswurf des Automaten wird nicht geöffnet und nach kurzer Zeit erscheint der Hinweis auf eine Störung. Einige Bankkunden gehen davon aus, dass der Automat defekt ist und verlassen daraufhin die Bank. Nachdem sich der Kunde entfernt hat, holt der Täter das ausgegebene Geld aus dem Schacht.

Dem Bundeskriminalamt liegen keine Fallzahlen vor, die eine quantitative Entwicklung dieses Kriminalitätsphänomens beschreiben können.

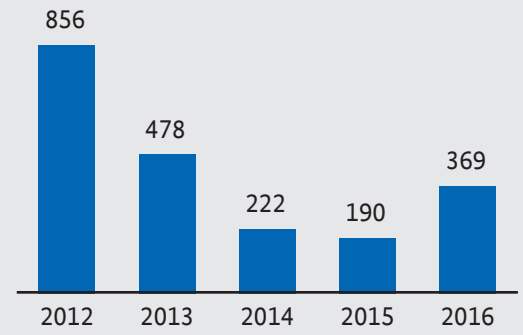
3 Technische Manipulation von Geldautomaten

3.1 Skimming

Die Modi Operandi sind seit Jahren im Wesentlichen unverändert. Nach wie vor installieren die Täter Vorbaugeräte zum Auslesen der Kartendaten (sog. 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.

Im Jahr 2016 war entgegen der rückläufigen Entwicklung der vergangenen Jahre jedoch wieder eine Zunahme der Skimming-Fälle an Geldautomaten zu verzeichnen. Dabei erfolgten in Deutschland insgesamt 369 einschlägige Angriffe[02] (2015: 190; + 94 %) auf Geldautomaten zur Erlangung von Kartendaten (Magnetstreifendaten) und PIN. Bedingt durch Mehrfachangriffe auf einzelne Geldautomaten waren insgesamt 159 Geldautomaten (2015: 118; + 35 %) betroffen.

Anzahl der Skimming-Angriffe auf Geldautomaten in Deutschland [03]



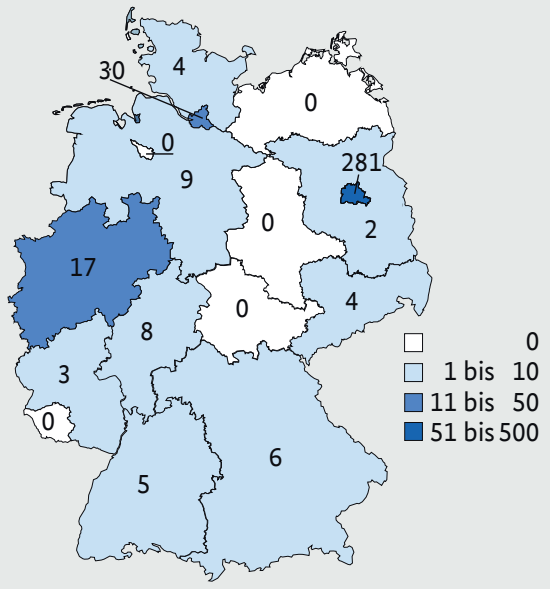
02 Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimmingequipment an einem Geldautomaten installieren.

03 Quelle: Euro Kartensysteme GmbH

Die Manipulationen erfolgten in elf Ländern. Mit Abstand die meisten Angriffe wurden in Berlin (281), gefolgt von Hamburg (30) und Nordrhein-Westfalen (17) registriert. Eine Ursache für den Brennpunkt in Berlin dürfte die hohe Anzahl von ausländischen, insbesondere außereuropäischen Touristen, in Berlin darstellen, deren Zahlungskarten teilweise noch nicht mit dem EMV-Chip ausgestattet sind. Die in Berlin festgestellten Tatverdächtigen stammen fast ausschließlich aus Bulgarien.

Im Deliktsbereich Skimming bzw. Manipulation von Geldautomaten sind die Täter seit Jahren nahezu ausschließlich bulgarischer, rumänischer und moldawischer Herkunft.

Skimming-Angriffe auf Geldautomaten nach Ländern (2016)



Datenabgriffe an Türöffnern zu Bankfoyers oder Kontoauszugsdruckern wurden im Jahr 2016 nicht festgestellt.

Belastbare Gesamtzahlen zur bundesweiten Fall- und Schadensentwicklung liegen der Polizei auch für das Jahr 2016 nicht vor. 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 keine Daten zu Verlusten und Missbrauchsumsätzen vor, da diese von der Deutschen Kreditwirtschaft nicht zur Verfügung gestellt werden.

Angaben der Fa. EURO Kartensysteme zufolge beläuft sich der Schaden aus Skimming-Fällen zum Nachteil deutscher Kreditinstitute im Jahr 2016 auf ca. 1.9 Mio. Euro[04]. Aufgrund internationaler Haftungsregelungen (Liability Shift) besteht bei verschiedenen Staaten die Möglichkeit der Schadensrückbelastung an das Land, in dem die betrügerischen Geldabhebungen erfolgt sind. Angaben zur Höhe der insgesamt im Rahmen der Haftungsumkehr rückbelasteten Umsätze liegen nicht vor.

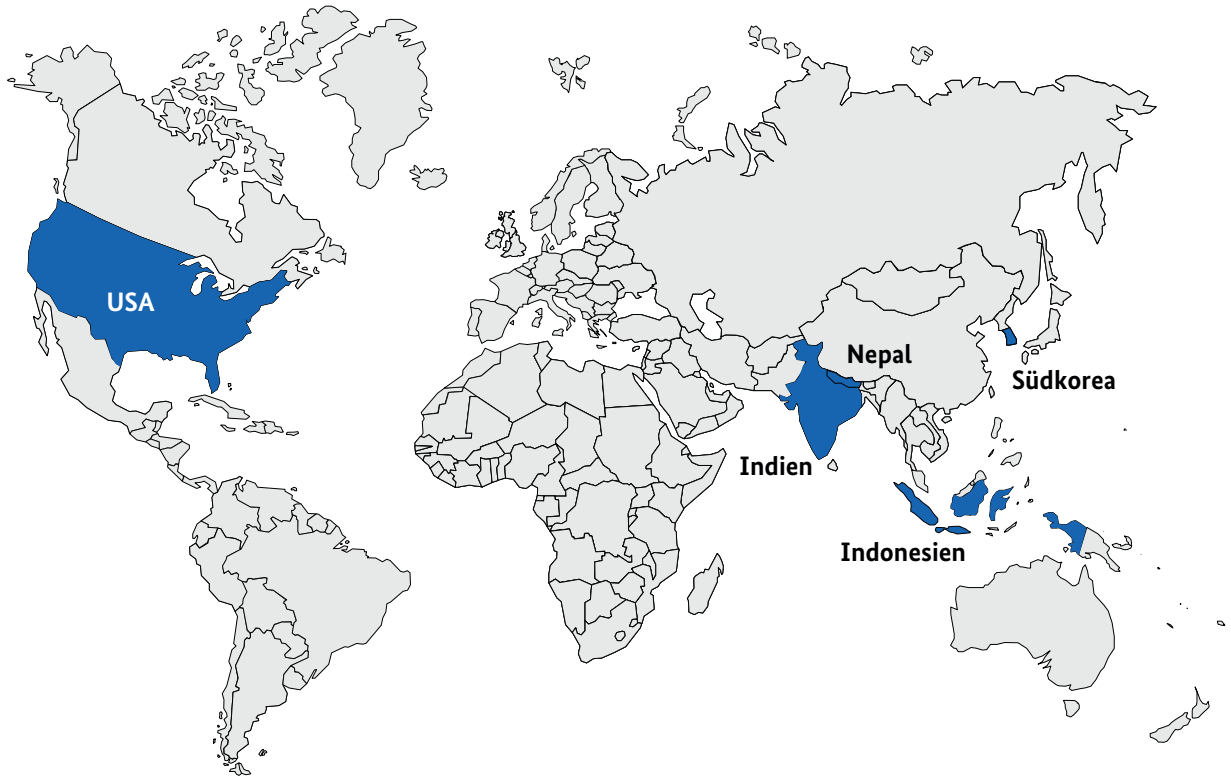
Nach wie vor bevorzugen die Täter das Fälschen von Zahlungskarten mit zuvor ausgespähten Magnetstreifendaten. Mit gefälschten Karten bieten sich bessere Einsatzmöglichkeiten als mit gestohlenen Karten, da letztere durch die Kartenorganisationen gesperrt werden, sobald der Diebstahl bemerkt wird. Dadurch werden sie für die Täterseite unbrauchbar.

04 https://www.heise.de/security/meldung/Datenklau-an-Geldautomaten-steigt-an-Schaden-sinkt-3592571.html

Seit dem 01.01.2011 werden Transaktionen mit Zahlungskarten im SEPA-Raum[05] nicht mehr über den Magnetstreifen, sondern über den EMV[06] -Chip autorisiert. Daher ist es den Tätern nicht mehr möglich, die mit Magnetstreifendaten ausgestatteten Kartendubletten im SEPA-Raum einzusetzen. Dies zwingt die Täter zu einer Verlagerung der Verwertungstaten außerhalb des SEPA-Raums (sog. „Nicht-Chip-Länder"), wo die von ihnen erstellten, auf Magnetstreifenbasis funktionierenden, „White Plastics" noch eingesetzt werden können.

Brennpunkte des Einsatzes gefälschter Zahlungskarten mit deutschen Kartendaten waren im Jahr 2016 die Staaten USA, Indonesien, Indien, Südkorea und Nepal. Weitere Verwertungstaten erfolgten hauptsächlich in Mittel- und Südamerika, z. B. in Belize, und in Südostasien, z. B. Philippinen.

Haupteinsatzstaaten gefälschter Zahlungskarten mit deutschen Kartendaten (2016)



05 SEPA: Single Euro Payments Area.

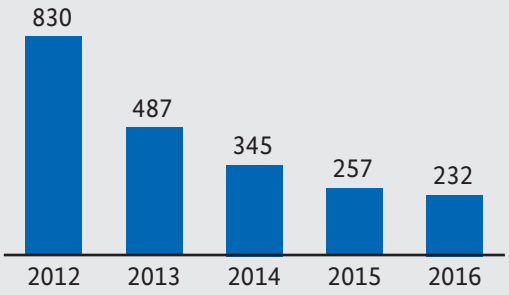
06 **E**uropay International, **M**asterCard, **V**isa.

Datenabgriffe im Ausland

Im Jahr 2016 wurden im Ausland bei Manipulationen von insgesamt 232 Geldautomaten (2015: 257, - 10 %) und POS-Terminals deutsche Kartendaten und PIN abgegriffen. Am häufigsten erfolgten die Datenabgriffe in Italien und Großbritannien. Entgegen der Jahre 2014/2015 nehmen Frankreich und die Türkei nicht mehr die ersten beiden Positionen der Rangfolge ein.

Die Zahl der registrierten Fälle steht jedoch unter dem Vorbehalt, dass in vielen Auslandsfällen der „Point of Compromise“ (PoC)[07] nicht eindeutig identifiziert werden konnte und somit diese Fälle nicht in die Statistik eingeflossen sind.

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



Neuartige Skimming-Geräte

In 2016 wurden in Deutschland neuartige Skimmer, sogenannte „Deep Insert Skimmer“[08] festgestellt, die technisch anspruchsvoller und somit schwerer detektierbar sind.

Eine neue Art des Kartendatenabgriffes wurde in Mexiko registriert, bei der ein sogenannter Sniffer zwischen die LAN-Verbindung des Geldautomaten mit dem Geldautomaten-Netzwerk installiert wurde, um den Datenverkehr zwischen dem Geldautomaten und dem Netzwerk auszulesen und so an Kartendaten zu gelangen. Ein solcher Modus Operandi wurde in Deutschland bisher noch nicht festgestellt.

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).

08 Skimmer, die innerhalb des Karteneinzugs installiert werden.

3.2 Jackpotting/Blackboxing

Beim sog. Jackpotting erfolgt das Einspielen einer Schadsoftware auf den Rechner des Geldautomaten, um durch den Zugriff auf das Auszahlungsmodul des Geldautomaten zahlreiche unautorisierte Bargeldauszahlungen nacheinander zu veranlassen.

Im Jahr 2016 wurden keine Jackpotting-Fälle in Deutschland festgestellt. Auch im europäischen Ausland war die Zahl der Meldungen von Jackpotting-Fällen rückläufig.

Beim sog. Blackboxing öffnen die Täter den Geldautomaten und übernehmen nach der Installation einer Blackbox die Kommunikation mit dem Auszahlungsmodul, um anschließend zahlreiche unautorisierte Bargeldauszahlungen nacheinander zu veranlassen (Variante des Jackpotting).

Im Jahr 2016 kam es in den Monaten April, Juni und Juli in Deutschland zu sieben Blackbox-Attacken in Baden-Württemberg, Rheinland-Pfalz und dem Saarland. Drei der sieben Taten waren erfolgreich und verursachten einen Schaden von insgesamt ca. 170.000 Euro.

Im Vergleich zum Vorjahr wurde im Jahr 2016 in Deutschland eine Veränderung des Modus Operandi festgestellt. Während in 2015 bis April 2016 die Geldautomaten zur Manipulation geöffnet wurden, erfolgten seit Juni 2016 die Angriffe mittels Aufbohren bzw. Aufschmelzen der Geldautomaten. Dieses Vorgehen wurde zunächst im europäischen Ausland bekannt. 2016 fanden in fast allen europäischen Staaten Blackbox-Attacken statt, wobei die meisten in Italien erfolgten.

Blackbox-Attacken sind möglich, wenn insbesondere bei Geldautomat-Typen älterer Baureihen die Kommunikation zwischen Auszahlungsmodul und Rechner des Automaten unverschlüsselt erfolgt. Diese Problematik ist den Finanzinstituten bekannt. In Deutschland wurden entsprechende Präventionsmaßnahmen von Seiten der Industrie eingeleitet.

4 Gesamtbewertung

Für das Jahr 2016 ist in Deutschland ein deutlicher Anstieg von **besonders schweren Fällen des Diebstahls durch Sprengung von Geldautomaten** zu verzeichnen. Nordrhein-Westfalen erweist sich in diesem Zusammenhang weiterhin als Brennpunkt. Die Herkunft der Tätergruppierungen, die verstärkten Präventionsmaßnahmen der Geldinstitute in den Niederlanden sowie repressive Maßnahmen der niederländischen Strafverfolgungsbehörden sprechen für einen Verdrängungseffekt dieses Kriminalitätsphänomens aus den Niederlanden in die grenznahen Bundesländer Nordrhein-Westfalen und Niedersachsen. Mittlerweile ist jedoch auch feststellbar, dass niederländische Tätergruppierungen ihren Aktionsradius auf Bayern, Hessen und Rheinland-Pfalz ausweiten. Bei den reisenden Tätern dominieren neben den Gruppierungen aus den Niederlanden polnische Tätergruppierungen.

Im Zusammenhang mit Sprengungen von Geldautomaten erlangen die Täter beträchtliche Geldbeträge, wodurch den geschädigten Geldinstituten hohe finanzielle Schäden entstehen. Zudem sind die im Rahmen der Straftaten verursachten Sach- und Gebäudeschäden ebenfalls erheblich und in der Gesamtschau zuweilen höher als die entwendeten Bargeldsummen.

Geldautomaten stellen ein attraktives Ziel für Straftäter dar. Neben repressiven Maßnahmen der Strafverfolgungsbehörden (z. B. Ermittlungskommissionen der Landeskriminalämter Brandenburg, Niedersachsen und Nordrhein-Westfalen) werden im Bereich der polizeilichen Kriminalprävention derzeit Empfehlungen zur Verbesserung des Schutzes gegen Sprengungen von Geldautomaten weiterentwickelt. Möglichst flächendeckende und einheitliche technische Präventionsmaßnahmen der Geldinstitute können zu einem Rückgang der Fallzahlen führen, wie die Erfahrungen aus den Niederlanden unterstreichen.

Erstmals seit 2011 ist in Deutschland ein Anstieg der **Skimmingfälle** zu verzeichnen. Die Anzahl der im Jahr 2016 erfassten Skimmingfälle liegt jedoch unter dem Durchschnitt der letzten fünf Jahre.

Hinsichtlich der Schadenssummen gibt es nach Angaben der Zahlungskartenindustrie eine positive Entwicklung. Während im Jahr 2010 die Schadenssumme bei ca. 55 Mio. Euro lag, betrug der Schaden im Jahr 2016 ca. 1,9 Mio. Euro.

Anhand dieser Schadenssumme lässt sich nachvollziehen, dass Skimmingdelikte, zumindest für Deutschland, kein Kriminalitätsphänomen mit herausragender Bedeutung sind. Gleichwohl kann festgestellt werden, dass die in diesem Kriminalitätsbereich aktiven Tätergruppierungen analog zu den Abwehrstrategien der Banken neue Modi Operandi entwickeln. Die Täter bringen neuartige Skimmer zum Einsatz und agieren mit der Platzierung von Residenten in Asien sowie Nord- und Südamerika logistisch professionell, um die Verwertungstaten, welche nur außerhalb des SEPA-Raumes möglich sind, schnell zu ermöglichen.

Neben Jackpotting- und Blackboxing-Fällen in Europa im Juli 2016 zeigt ein Hackingangriff auf ein Netzwerk von Geldautomaten in Taiwan mit einem Schaden von ca. 3,4 Mio. USD, dass die Tätergruppierungen auch neue Modi Operandi wählen.

Es sind daher künftig auch weiterhin technisch verfeinerte und teilweise gänzlich neue Angriffsszenarien zu erwarten, wobei insbesondere mögliche Schwachstellen im NFC[09]-Bereich neue Herausforderungen darstellen.

Im Rahmen technischer Präventionsmaßnahmen müssen die Entwicklungen von Sicherheitsvorkehrungen im Bereich der Chipkartenzahlungen sowie der NFC-Technik kontinuierlich vorangetrieben werden. Grundvoraussetzung für eine effektive Stärkung der Systeme ist der enge Informationsaustausch sowie die Kooperation von Netzbetreibern, Terminalherstellern, der Zahlungskartenindustrie, den großen Handelsunternehmen und den Dachorganisationen des Einzelhandels.

Mit Blick auf eine effektive Bekämpfung der genannten Phänomene ist die anlassbezogene Intensivierung der Zusammenarbeit zwischen Polizei und Zahlungskartenorganisationen fortzuführen. Auf polizeilicher Ebene erfolgt eine intensive, internationale Zusammenarbeit, um die überwiegend transnationale Tatbegehung zu bekämpfen.

09 Near Field Communication: Internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten per Funktechnik.

Impressum

Herausgeber
Bundeskriminalamt
65173 Wiesbaden

Stand
2016

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de