Bundeskriminalamt

BKA

Angriffe auf Geldautomaten

Bundeslagebild 2017

Angriffe auf Geldautomaten 2017 in Zahlen

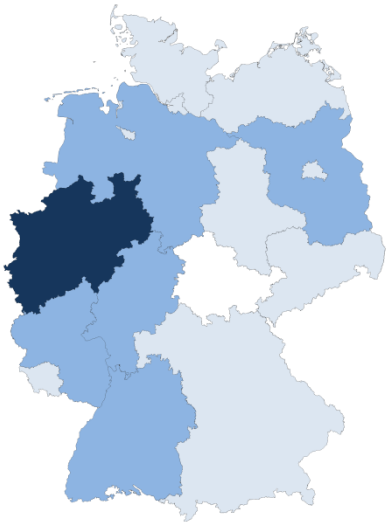
SPRENGUNGEN VON GELDAUTOMATEN

268 Sprengungen (-16 %)

➡ Brennpunkt
Nordrhein-Westfalen

35 Festnahmen

überwiegend Tatverdächtige
aus den Niederlanden



TECHNISCHE MANIPULATION VON GELDAUTOMATEN – SKIMMING

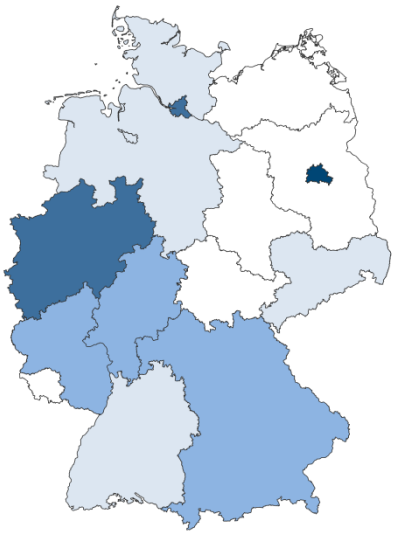
499 Skimming-Fälle

➡ Brennpunkt Berlin

überwiegend Tatverdächtige
aus Bulgarien und Rumänien

2,2 Mio. Euro Schaden (+15 %)

Entwicklung neuer Modi Operandi



Inhaltsverzeichnis

1 Vorbemerkung

Das Bundeslagebild „Angriffe auf Geldautomaten“[1] 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.

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

2 Darstellung und Bewertung der Kriminalitätslage

2.1 PHYSISCHE ANGRIFFE AUF 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 2017 rund 500 besonders schwere Fälle des Diebstahls aus Geldautomaten ereigneten. Im Vergleich zum Vorjahr (ca. 700 Angriffe) ist die Fallzahl um rund ein Drittel gesunken.

Gemäß der dem Bundeskriminalamt vorliegenden polizeilichen Erkenntnisse finden 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)

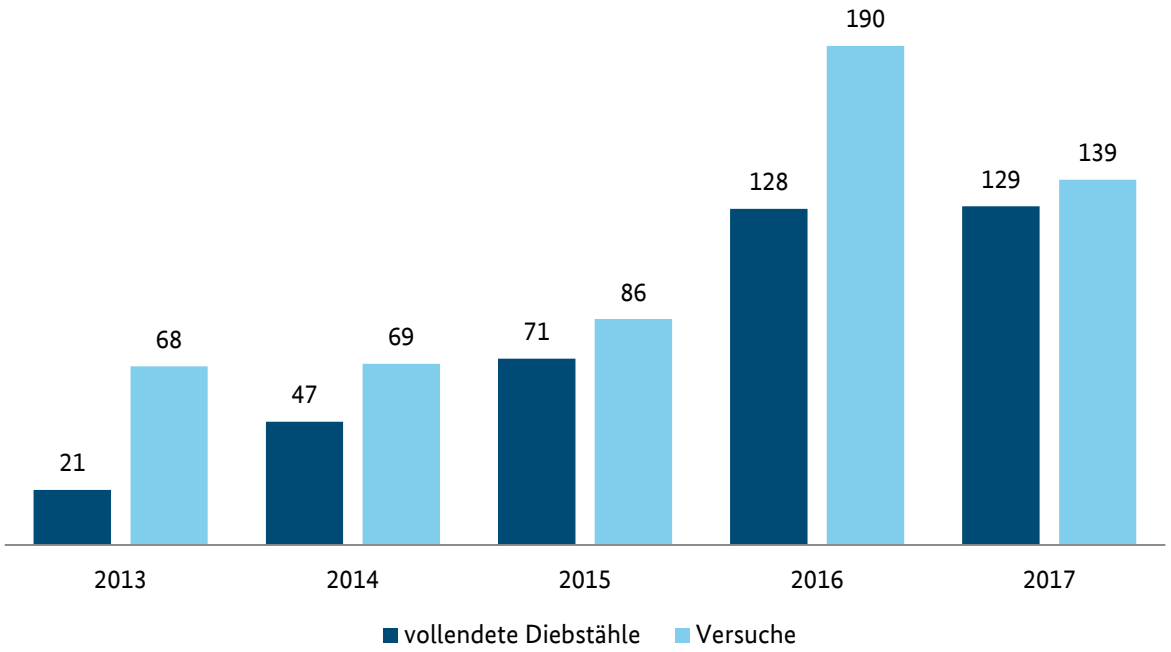
2.1.1 Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten

Nach polizeilichen Erkenntnissen 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 sowie auf die Zündquelle und die Zündleitung. In Einzelfällen wurde gewerblicher Sprengstoff, teilweise auch Pyrotechnik, zur Sprengung eingesetzt.

Fallzahlen

Im Jahr 2017 wurden dem Bundeskriminalamt im Phänomenbereich „Sprengung von Geldautomaten“ 268 Fälle bekannt. Gegenüber dem Vorjahr (318 Fälle) ist damit ein Rückgang der Fallzahl um 16 % zu verzeichnen. In 129 Fällen (48 %) gelangten die Täter an Bargeld, in 139 Fällen (52 %) blieb es beim versuchten Diebstahl.

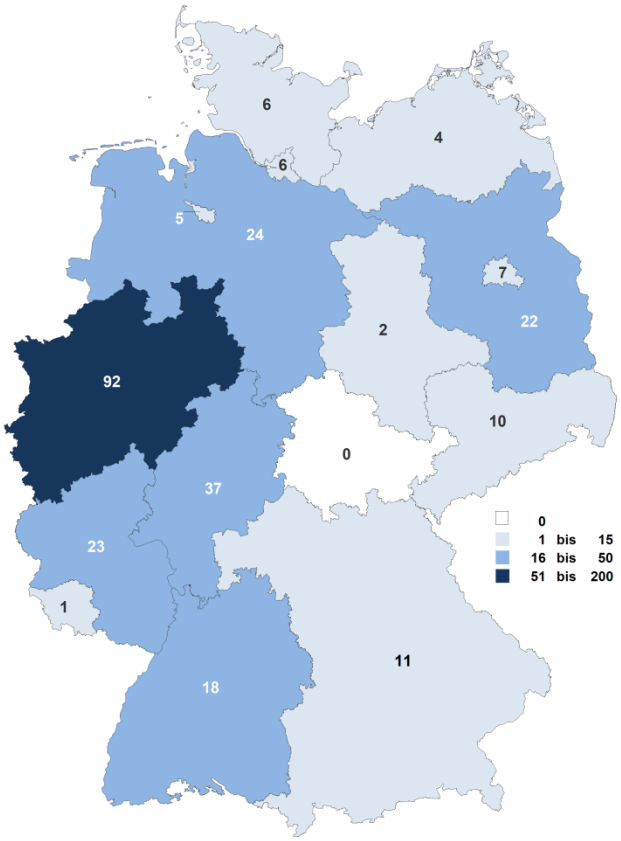
Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten (inkl. Versuche) in Deutschland – Fallentwicklung



In 212 Fällen (2016: 198 Fälle) führten die Täter eine Explosion herbei. In 55 Fällen wurde die beabsichtigte Sprengung nicht ausgelöst und es bleib beim Versuch. 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 bergen Trümmerteile und Splitter Risiken, die von den Tätern nicht abgeschätzt werden können. Zudem können Einsatzkräfte von Feuerwehr und Polizei einer erheblichen Gefährdung ausgesetzt sein.

Die durch die Straftaten verursachten Sachschäden übersteigen die Beuteschäden in vielen Fällen deutlich. Bei einzelnen Straftaten entstanden Sachschäden in siebenstelliger Höhe. Fälle, bei denen Personen verletzt wurden, sind indes nicht bekannt geworden.

Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten in Deutschland nach Ländern (2017)



Der regionale Brennpunkt lag wie im vergangenen Jahr in Nordrhein-Westfalen. Darüber hinaus waren die Länder Hessen, Niedersachsen, Rheinland-Pfalz, Brandenburg und Baden-Württemberg überdurchschnittlich betroffen. Das relativ hohe Fallaufkommen in Hessen und Rheinland-Pfalz stellt eine neue Entwicklung dar: Die Fallzahlen 2017 in Hessen sind von 20 (2016) auf 37 und in Rheinland-Pfalz von 5 (2016) auf 23 gestiegen. Intensive polizeiliche Maßnahmen wie beispielsweise in Nordrhein-Westfalen und Niedersachsen eingerichteten zentralen Ermittlungskommissionen sowie eine intensive Zusammenarbeit mit den niederländischen Strafverfolgungsbehörden könnten der Grund für die dort sinkenden Fallzahlen gewesen sein. Damit einhergehend ist ein Verdrängungseffekt oder eine Ausweitung der Aktivitäten nach Hessen und Rheinland-Pfalz wahrscheinlich.

Tatverdächtige

Im Jahr 2017 wurden dem Bundeskriminalamt insgesamt 93 Personen bekannt, die im Zusammenhang mit Sprengungen von Geldautomaten festgenommen (35) oder zumindest als dringend tatverdächtig identifiziert wurden (58).

Sprengungen von Geldautomaten werden in der Regel arbeitsteilig durch Tätergruppierungen begangen; nur in wenigen Fällen sind Einzeltäter aktiv. Im Rahmen von Ermittlungen konnten sowohl reisende als auch regional agierende Straftätergruppierungen identifiziert werden.

Von den Festgenommenen oder zumindest Identifizierten sind 75 Personen als reisende Täter einzustufen. Der größte Anteil stammte mit 46 Personen aus den Niederlanden. Insbesondere die Ermittlungen in Nordrhein-Westfalen ergaben, dass dort vorrangig aus Ballungszentren in den Niederlanden (z. B. Amsterdam und Utrecht) stammende niederländische Staatsangehörige mit marokkanischem Migrationshintergrund entsprechende Straftaten verübten. Diese agierten vor Ort arbeitsteilig als Mitglieder von Netzwerken mit einem hohen Maß an Professionalität in allen Tatphasen. Zur Flucht wurden hochmotorisierte Kraftfahrzeuge oder Motorroller genutzt.

Neben Tatverdächtigen aus den Niederlanden wurden vor allem solche aus Bulgarien (13 Personen), die allesamt einer Tätergruppierung zuzuordnen sind, und Tatverdächtige aus Polen (6 Personen) festgenommen bzw. identifiziert. Im Rahmen der im Jahr 2017 geführten polizeilichen Ermittlungen wurden weitergehende Bezüge ins Ausland, insbesondere nach Polen, festgestellt. Diese legen den Schluss nahe, dass polnischen Tatverdächtigen eine größere Bedeutung beim Phänomen Sprengung von Geldautomaten beizumessen sein dürfte, als es die reine Anzahl an bekannt gewordenen Tatverdächtigen in Deutschland vermuten lässt.

Landgericht Köln verurteilt Geldautomatensprenger zu Gefängnisstrafen

Das Landgericht Köln hat im August 2017 zwei Niederländer marokkanischer Abstammung wegen der Sprengung mehrerer Geldautomaten in Nordrhein-Westfalen zu Gefängnisstrafen von jeweils fünfeinhalb Jahren verurteilt. Laut Urteil erbeuteten sie mit ihren Taten insgesamt 470.000 Euro. Zudem verursachten die 22 und 30 Jahre alten Täter erheblichen Sachschaden.

Der Tatablauf sei in Grundzügen immer gleich gewesen: Nachts füllten die Täter die Geldautomaten mit einem Gasgemisch, dann sprengten sie sie per Fernzündung. Anschließend flohen die Täter mit einem getunten Fahrzeug.

Verurteilt wurden die beiden Männer wegen des Herbeiführens von Sprengstoffexplosionen und schweren Raubes. Die Taten hatten sie eingeräumt. Der Anklagevorwurf, als Mitglieder einer Bande gehandelt zu haben, konnte hingegen nicht nachgewiesen werden.

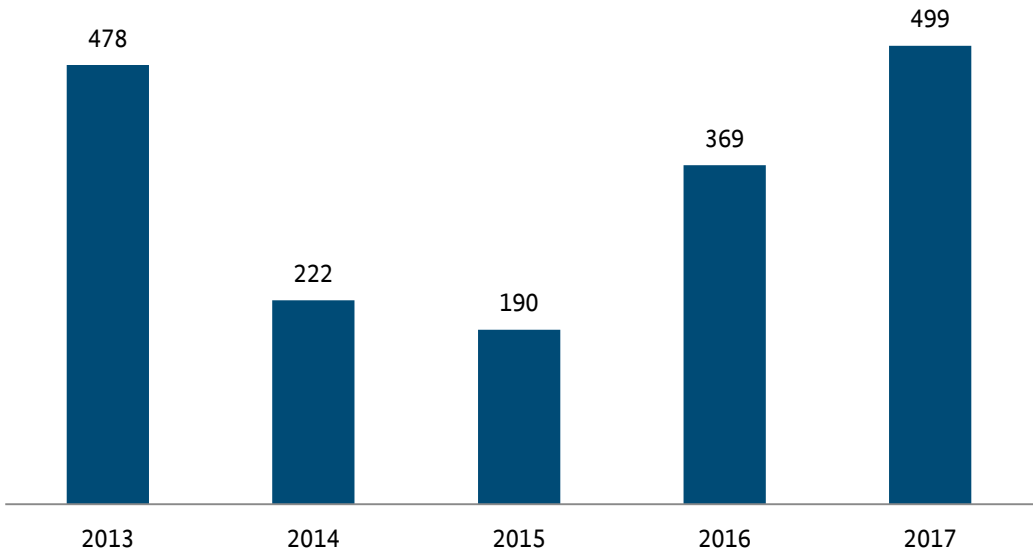
2.2 TECHNISCHE MANIPULATION VON GELDAUTOMATEN

2.2.1 Skimming

Die Modi Operandi im Bereich Skimming sind seit Jahren im Wesentlichen unverändert. Nach wie vor installieren die Täter Gerätschaften 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 eingegebene PIN speichern. Die zunehmende Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen (mechanisch und elektronisch) erschwert der Täterseite das Auslesen der Kartendaten.

Gleichwohl war im Jahr 2017 eine erneute Zunahme der bis 2015 rückläufigen Anzahl von Skimming-Fällen zu verzeichnen. Es erfolgten 499 Angriffe[2] (2016: 369; +35 %) auf Geldautomaten zur Erlangung von Kartendaten (Magnetstreifendaten) und PIN.[3] Bedingt durch Mehrfachangriffe auf einzelne Geldautomaten waren insgesamt 223 Geldautomaten (2016: 159; +40 %) betroffen.

Anzahl der Skimming-Angriffe auf Geldautomaten in Deutschland



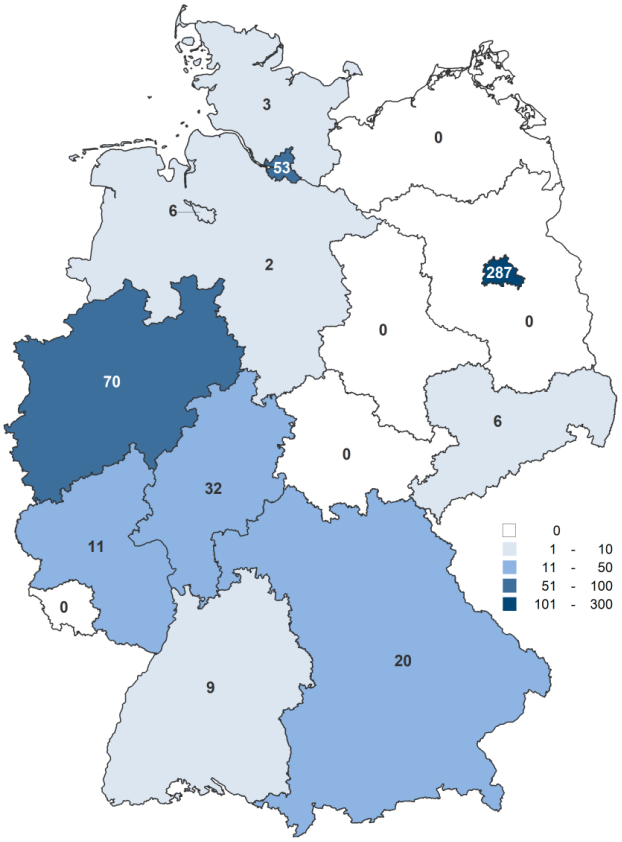
Trotz der steigenden Anzahl an Skimming-Angriffen gegenüber dem Vorjahr bewegt sich das Fallzahlenaufkommen im Vergleich zu 3.183 Attacken im Jahr 2010, die den bisherigen Höchststand markierten, auf einem relativ niedrigen Niveau.

[2] Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimming-Equipment an einem Geldautomaten installierten.
[3] Euro Kartensysteme GmbH.

Die Manipulationen erfolgten in elf Bundesländern. Mit Abstand die meisten Angriffe wurden in Berlin (287) registriert. Eine Ursache für den Brennpunkt Berlin dürfte die dortige hohe Anzahl von ausländischen, insbesondere außereuropäischen Touristen sein, deren Zahlungskarten teilweise noch nicht mit dem EMV[4]-Chip ausgestattet sind. Daten dieser Karten lassen sich durch die Täter leichter verwerten.

Im Deliktsbereich Skimming sind die Täter seit Jahren nahezu ausschließlich bulgarischer und rumänischer Herkunft.

Skimming-Angriffe auf Geldautomaten nach Ländern (2017)



Schaden

Belastbare Daten zur bundesweiten Schadensentwicklung liegen der Polizei auch für das Jahr 2017 nicht vor. Ein Großteil der Straftaten wird nicht angezeigt, da der Schaden des betroffenen Karteninhabers durch die Geldinstitute und Kreditkartenorganisationen in der Regel erstattet wird. Daten zu Verlusten und Missbrauchsumsätzen werden von der Deutschen Kreditwirtschaft nicht zur Verfügung gestellt.

[4] EMV: Europay International, Mastercard, Visa.

Angaben der Firma EURO Kartensysteme (EKS) zufolge beläuft sich der Schaden aus Skimmingfällen zum Nachteil deutscher Kreditinstitute 2017 auf ca. 2,2 Mio. Euro. Dies bedeutet eine Steigerung um 15 %. In Anbetracht einer Schadenssumme von ca. 55 Mio. Euro im Jahr 2010 handelt es sich dabei jedoch um ein vergleichsweise geringes Schadensniveau.

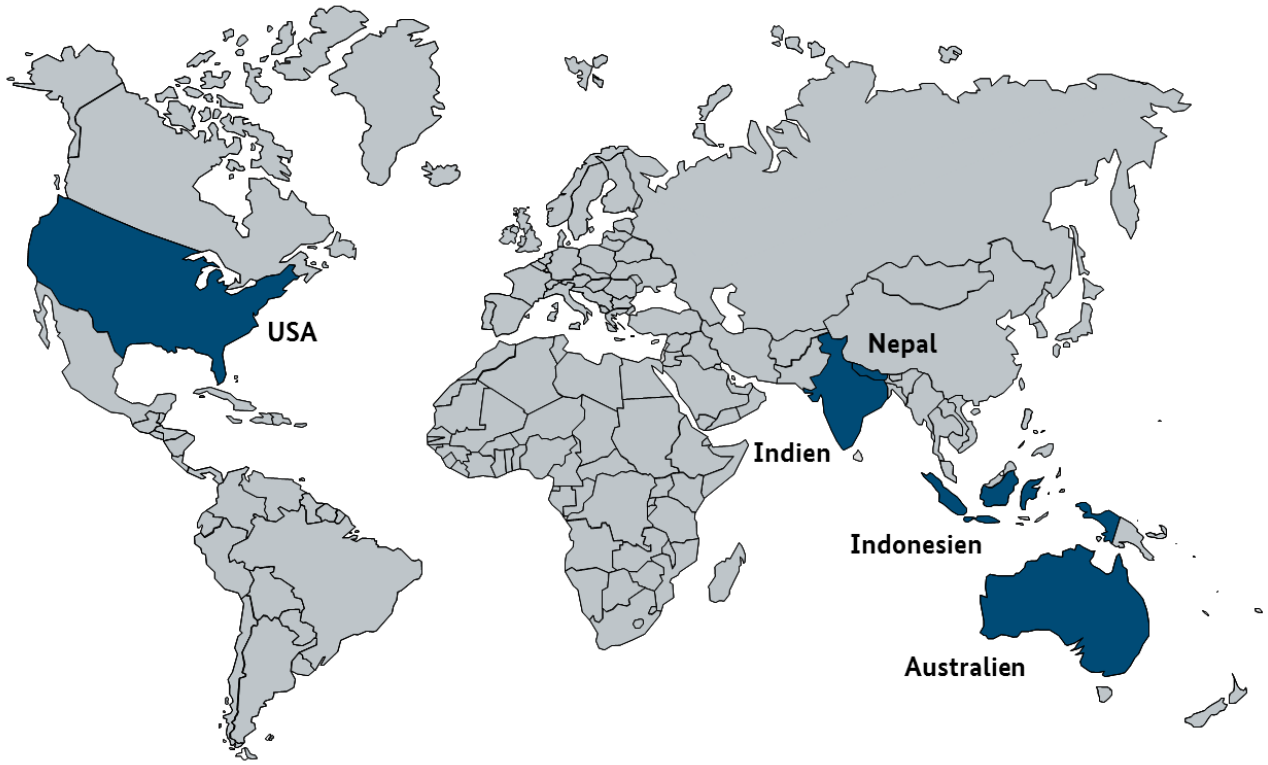
Verwertungstaten im Ausland

Seit dem 01.01.2011 werden Transaktionen mit Zahlungskarten im SEPA[5]-Raum nicht mehr über den Magnetstreifen, sondern über den EMV-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 Durchführung 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 2017 die Staaten Indonesien, USA, Indien, Australien und Nepal. Weitere Verwertungstaten erfolgten hauptsächlich in Mittel- und Südamerika sowie Südostasien.

Gegen Ende des Jahres 2017 wurden Verwertungstaten in Deutschland und Rumänien festgestellt, deren Ursache in dem Kartenprodukt einer Großbank begründet ist, welches über keinen EMV-Chip, sondern ausschließlich über einen Magnetstreifen verfügt. Die Täter wurden auf dieses Kartenprodukt aufgrund der „leichten" Verwertung aufmerksam und griffen gezielt Geldautomaten dieses Finanzinstitutes an. Die Verwertungstaten legen nahe, dass es sich um rumänische Täter handelte.

Haupteinsatzstaaten gefälschter Zahlungskarten mit deutschen Kartendaten (2017)



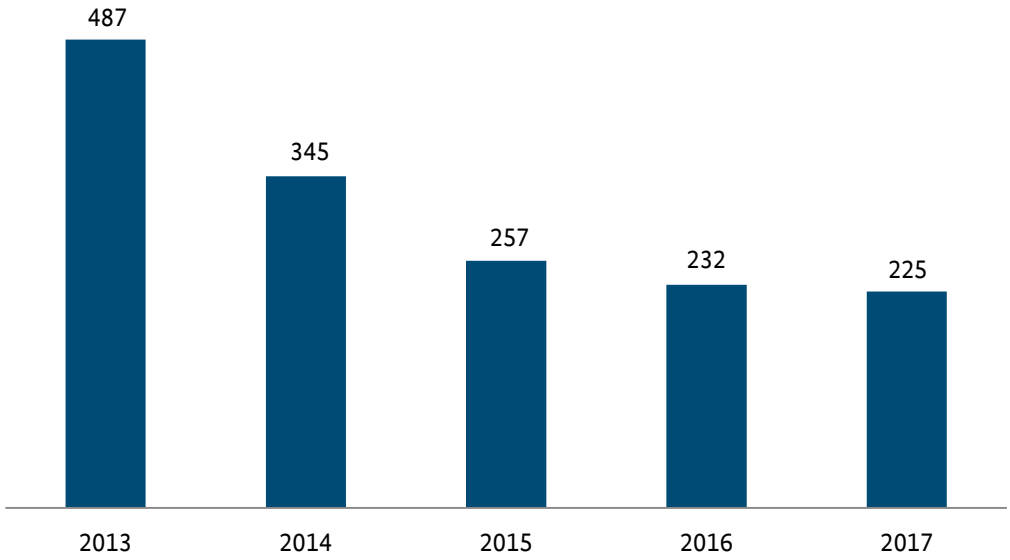
[5] SEPA: Single Euro Payments Area.

Datenabgriffe im Ausland

Im Jahr 2017 wurden im Ausland bei Manipulationen von insgesamt 225 Geldautomaten und POS-Terminals (2016: 232; -3 %) deutsche Kartendaten und PIN abgegriffen. Am häufigsten erfolgten die Datenabgriffe in Mexiko und Italien. Seit 2013 ist die die Zahl der Datenabgriffe im Ausland stetig gesunken und hat sich mehr als halbiert (2013: 487).

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

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



Weiterentwicklung bei Skimming-Geräten

Der Trend des Einsatzes von sog. „Deep Insert Skimmern“ setzte sich auch im Jahr 2017 fort. Im Berichtsjahr wurden aus Metall und aus Kunststoff hergestellte, in den Geldautomaten installierte Auslesegeräte sichergestellt. Von Seiten der Automatenhersteller wurden erste technische Maßnahmen getroffen, um diese zu detektieren bzw. die Geldautomaten vor solchen Angriffen zu schützen. Die Täter setzten jedoch weiterhin auch herkömmliche Vorsatz-Skimmer erfolgreich ein. Im Jahr 2017 wurden in Spanien und Bulgarien mehrerer Werkstätten ausgehoben, in welchen Skimmer in einer hohen Anzahl und Vielfalt produziert wurden.

[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 die Verfügungsgewalt der Täter gelangt sind.

2.2.2 Jackpotting/Blackboxing/Netzwerkattacken

Im April und Oktober 2017 wurden zwei Jackpotting[7]-Fälle in Deutschland festgestellt. In beiden Fällen wurden Geldautomaten derselben Bank angegriffen. Der Schaden belief sich auf ca. 1,3 Mio. Euro.

Im Juli und Dezember 2017 erfolgten in Deutschland insgesamt drei Blackbox[8]-Attacken, die erfolglos verliefen. Im europäischen Ausland fanden bedeutend mehr erfolgreiche Jackpotting- und Blackbox-Attacken statt. Brennpunkte waren Österreich und die Schweiz.

Im November 2017 wurde erstmals der versuchte Einsatz einer bestimmten Schadsoftware festgestellt, die es auch technisch weniger versierten Tätern ermöglichen soll, Geldautomaten zu manipulieren und einen sog. „Cashout" durchzuführen. Die Schadsoftware wird online, u. a. über das Darknet, vertrieben.

Erstmals im Jahr 2017 erfolgten Netzwerkattacken auf Geldautomaten. Den Tätern gelingt es immer häufiger, die Netzwerke von Zahlungskarteninstituten zu infiltrieren und Schadsoftware zu installieren. Meistens werden mit der Malware die Limits von Kreditkarten außer Kraft gesetzt, so dass die Täter mit echten Kreditkarten an Geldautomaten sehr große Summen innerhalb kürzester Zeit abheben können. Missbräuchliche Abhebungen fanden u. a. auch in Deutschland statt, während die betroffenen Zahlungskarteninstitute/Banken ihre Stammsitze in Zentralasien und Afrika haben. In 2017 erfolgten in Deutschland drei solcher Netzwerkattacken, bei denen die Täter insgesamt ca. 1,5 Mio. Euro erbeuteten. In allen drei Fällen fanden parallel Abhebungen im Ausland statt, so dass von organisierten Strukturen bzw. international agierenden Tätern ausgegangen werden muss.

Trotz der in Deutschland von Seiten der Industrie erfolgreich eingeleiteten Präventionsmaßnahmen muss aufgrund der Aussicht auf hohe kriminelle Erträge für die Täter weiterhin von einem hohen Bedrohungspotenzial ausgegangen werden.

[7] Jackpotting: Einspielen einer Schadsoftware auf den Rechner des Geldautomaten, um durch den Zugriff auf das Auszahlungsmodul des Geldautomaten zahlreiche unautorisierte Bargeldauszahlungen nacheinander zu veranlassen.

[8] Blackbox-Attacken: Täter öffnen den Geldautomaten, übernehmen die Kommunikation mit dem Auszahlungsmodul durch Installation eines „eigenen" Rechners (Blackbox), um anschließend zahlreiche unautorisierte Bargeldauszahlungen nacheinander zu veranlassen (Variante des Jackpotting).

3 Gesamtbewertung

Im Jahr 2017 war in Deutschland ein Rückgang von besonders schweren Fällen des Diebstahls durch Sprengung von Geldautomaten zu verzeichnen. Die Anzahl der Angriffe liegt jedoch weiterhin deutlich über dem Fünfjahresdurchschnitt, so dass daraus noch keine Trendwende abgeleitet werden kann. Im Zusammenhang mit Sprengungen von Geldautomaten erlangen die Täter teils beträchtliche Geldbeträge, wodurch den geschädigten Geldinstituten hohe finanzielle Schäden entstehen. Die im Rahmen der Straftaten verursachten Sach- und Gebäudeschäden sind ebenfalls erheblich und in der Gesamtschau zuweilen höher als die entwendeten Bargeldsummen. Darüber hinaus gilt es zu berücksichtigen, dass durch Sprengungen von Geldautomaten im Einzelfall erhebliche Gefahren für Anwohner, Passanten und Einsatzkräfte von Feuerwehr und Polizei ausgehen können.

Die polizeilichen Erkenntnisse weisen darauf hin, dass in Deutschland insbesondere reisende Täter Sprengungen von Geldautomaten verüben. Hier dominieren Tätergruppierungen aus den Niederlanden mit einem hohen Professionalisierungsgrad. Intensive Bekämpfungsmaßnahmen in Nordrhein-Westfalen und in Niedersachsen dürften zum Rückgang der Fallzahlen in diesen Ländern geführt haben. Zudem ist ein Verdrängungseffekt feststellbar, da niederländische Tätergruppierungen ihren Aktionsradius insbesondere auf Hessen, Rheinland-Pfalz und Baden-Württemberg ausgeweitet haben.

Erstmals seit Jahren war im Berichtsjahr in Deutschland ein erneuter Anstieg der Skimmingfälle zu verzeichnen, jedoch liegen diese immer noch weit unter dem Höchststand zu Beginn dieses Jahrzehnts. Unabhängig von der Steigerung der Fallzahlen zeigt sich, dass die in den letzten Jahren mit der Umstellung auf Chiptechnologie eingeführten, überwiegend technischen Sicherheitsmaßnahmen greifen. Skimmingdelikte bleiben, zumindest für Deutschland, kein Kriminalitätsphänomen mit herausragender Bedeutung.

Eine neue Qualität der Straftaten stellt die Herstellung und Verbreitung von Manipulations-Tools dar, welche es auch technisch nicht versierten Tätern ermöglichen, Manipulationen an Geldautomaten vorzunehmen. Hier ist künftig mit steigenden Fallzahlen und entsprechend hohen Schadenssummen zu rechnen.

Es wird deutlich, dass die Täter durch andersartig gestaltete Angriffe auf Geldautomaten auf die Veränderung im Skimmingbereich reagieren und sich neu aufstellen. Beispiel hierfür sind vermehrte Hackingangriffe auf Geldautomaten-Netzwerke, die im Gegensatz zum Skimming eine wesentlich höhere Gewinnerwartung versprechen.

Grundsätzlich eröffnen die fortschreitenden technischen Entwicklungen, wie z. B. die auch in Deutschland immer weiter verbreitete NFC[9]-Funktion bei Zahlungskarten, neue Tatgelegenheiten. Zwar wurden im Jahr 2017 im NFC-Bereich – trotz des bereits erkannten Bedrohungspotenzials – keine Straftaten polizeilich bekannt, dennoch sind die Entwicklungen im Bereich der NFC-Technik, wie auch jene bei Chipkartenzahlungen aufmerksam zu beobachten sowie die stetige und enge Kooperation mit den Netzbetreibern, den Terminalherstellern, der Fa. EURO Kartensysteme, den großen Handelsunternehmen und den Dachorganisationen des Einzelhandels fortzusetzen.

[9] Near Field Communication (NFC): Drahtlose Übertragungstechnik, die zum kontaktlosen Datenaustausch zwischen Geräten oder Gegenständen dienen soll, wie z. B. kontaktloses Bezahlen mit der Zahlungskarte oder dem Mobiltelefon.

Impressum

Herausgeber

Bundeskriminalamt, 65173 Wiesbaden

Stand

April 2018

Gestaltung

Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis

Bundeskriminalamt

Weitere Publikationen des Bundeskriminalamtes zum Herunterladen finden Sie ebenfalls unter:
www.bka.de/Lagebilder