Bundeskriminalamt

BKA

Angriffe auf Geldautomaten

Bundeslagebild 2018

Angriffe auf Geldautomaten 2018 in Zahlen

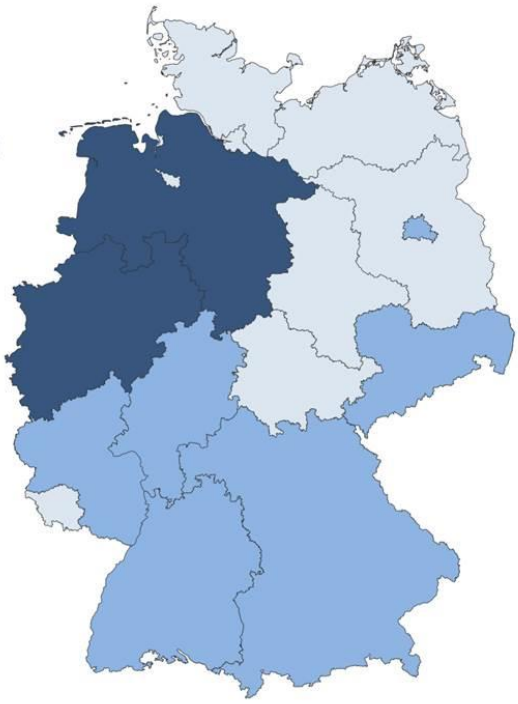
Sprengungen von Geldautomaten

369 Sprengungen (+38 %)
➡ Brennpunkt Nordrhein-Westfalen

Rund 18 Mio. Euro Beuteschaden

128 Tatverdächtige (+38 %);
überwiegend aus den Niederlanden

Deutlicher Anstieg der Versuchsfälle



Technische Manipulation von Geldautomaten

449 Skimming-Fälle (-10 %)
➡ Brennpunkt Berlin

1,4 Mio. Euro Schaden (-36 %)

Überwiegend Tatverdächtige
aus Bulgarien und Rumänien

Signifikanter Anstieg von Jackpotting- und
Blackboxing-Attacken

Inhaltsverzeichnis

Gender-Hinweis
Aus Gründen der besseren Lesbarkeit wird in diesem Lagebild das generische Maskulinum verwendet.

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 Lagebilds 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

Gemäß der dem Bundeskriminalamt vorliegenden polizeilichen Erkenntnisse ereigneten sich im Jahr 2018 rund 590 besonders schwere Fälle des Diebstahls von und aus Geldautomaten. Im Vergleich zum Vorjahr (ca. 500 Angriffe) ist die Fallzahl um rund ein Fünftel gestiegen.

Dabei kamen folgende Modi Operandi zur 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)

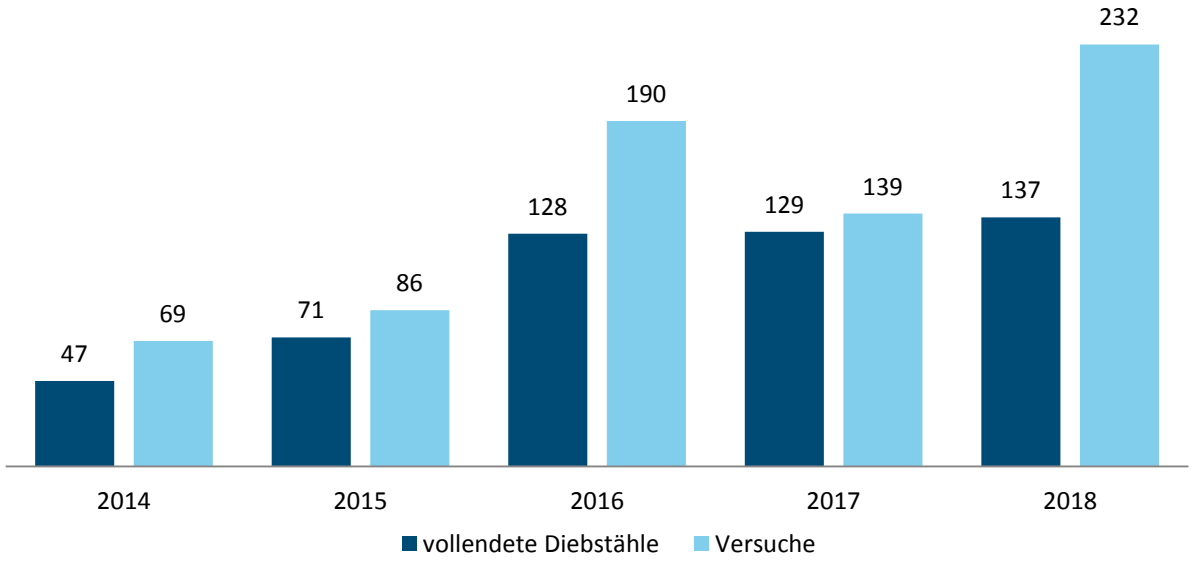
2.1.1 Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten

Fallzahlen

Im Jahr 2018 wurden dem Bundeskriminalamt im Phänomenbereich „Sprengung von Geldautomaten“ 369 versuchte und vollendete Fälle bekannt. Gegenüber dem Vorjahr (268 Fälle) ist damit ein deutlicher Anstieg der Fallzahl um 38 % zu verzeichnen. In 240 Fällen (2017: 212 Fälle; +13 %) führten die Täter eine Explosion herbei, in 129 Fällen (2017: 55 Fälle; +135 %) wurde die beabsichtigte Sprengung nicht ausgelöst und es blieb beim Versuch. Der Anstieg der Gesamtfallzahl ist somit im Wesentlichen auf die deutliche Zunahme der Versuchsfälle zurückzuführen.

Von den insgesamt 369 versuchten und vollendeten Fällen gelangten die Täter in 137 Fällen an Bargeld (2017: 129; +6%). Daneben wurden 232 Fälle (2017: 139 Fälle; +77%) registriert, bei denen kein Bargeld erbeutet wurde. Neben der Tatsache, dass die beabsichtigte Sprengung in diesen Fällen nicht ausgelöst wurde, kommt hier der Umstand zu tragen, dass die Täter auch bei erfolgreichen Sprengungen des Öfteren nicht an Bargeld gelangten. Verstärkte Präventionsmaßnahmen der Banken könnten hierzu beigetragen haben.

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

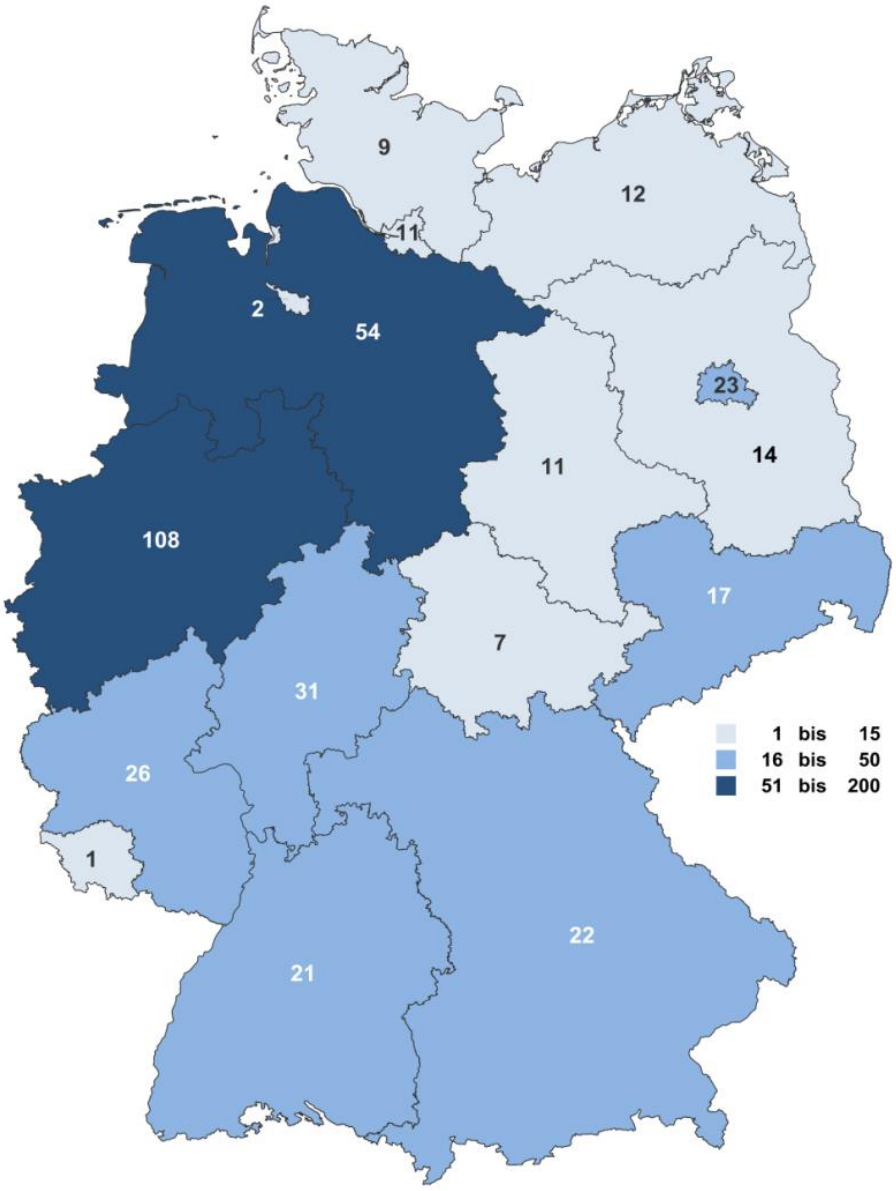


Nach polizeilichen Erkenntnissen werden Geldautomaten häufig durch Einleitung eines Gases bzw. Gasgemisches und dessen anschließender Zündung gesprengt. Ausgehend von diesem Grundprinzip unterscheiden sich die Tatbegehungen insbesondere in Bezug auf die Art des Gases, die eingeleitete Menge und den Ort der Einleitung sowie auf die Zündquelle und die Zündleitung.
Für das Jahr 2018 wurden dem Bundeskriminalamt auch 20 Sprengungen bekannt, die nicht mit Gas bzw. Gasgemischen, sondern mit Explosivstoffen (z. B. pyro-technische Sätze, Selbstlaborate, gewerbliche Sprengstoffe) verübt wurden.
Durch Sprengungen von Geldautomaten kam es im Jahr 2018 vereinzelt zu Verletzungen von unbeteiligten Dritten.

So führte in einem Fall die Sprengung eines Geldautomaten, der in einer an ein Wohnhaus angrenzenden Bankfiliale stand, zu Rauchgasentwicklungen, die bei den Hausbewohnern Rauchgasvergiftungen nach sich zogen. Selbst wenn häufig Tatzeiten und Tatörtlichkeiten ausgewählt werden, in denen kein Kundenbetrieb mehr zu erwarten ist, verbleibt ein grundsätzlich hohes Risiko für Leib und Leben von Passanten und Anwohnern der betroffenen Objekte. Unabhängig vom Aufstellort 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 Täter erlangten durch Sprengungen von Geldautomaten im Jahr 2018 ca. 18 Mio. Euro Bargeld. In den meisten Fällen überstiegen dabei die durch die Straftaten verursachten Sachschäden die Beuteschäden deutlich. Vereinzelt wurden auch im Jahr 2018 Fälle bekannt, in denen der entstandene Sachschaden die Millionen-Euro-Grenze überschritten haben dürfte. Das Bundeskriminalamt geht davon aus, dass durch Geldautomatensprengungen im Jahr 2018 Begleitschäden im mittleren zweistelligen Millionenbereich verursacht wurden.

Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten in Deutschland nach Ländern (2018)



Im Jahr 2018 wurden in allen Bundesländern Geldautomaten gesprengt. Der regionale Brennpunkt lag erneut in Nordrhein-Westfalen. Darüber hinaus waren Niedersachsen, Hessen und Rheinland-Pfalz überdurchschnittlich stark betroffen.

In nahezu allen Bundesländern ist die Fallzahl gestiegen. In Niedersachsen (54 Fälle; 2017: 24), Berlin (23 Fälle; 2017: 7) und Bayern (22 Fälle; 2017: 11) hat sie sich mindestens verdoppelt. Die deutlichen Anstiege der Fallaufkommen in Berlin und Bayern stellen hierbei eine neue Entwicklung dar.

Tatverdächtige

Im Jahr 2018 wurden dem Bundeskriminalamt 128 Tatverdächtige im Zusammenhang mit Sprengungen von Geldautomaten bekannt. Gegenüber dem Vorjahr (93 Tatverdächtige) bedeutet dies einen Anstieg um 38 %.

Sprengungen von Geldautomaten werden in der Regel arbeitsteilig durch Tätergruppierungen begangen, nur in wenigen Fällen sind Einzeltäter aktiv. Im Rahmen von Ermittlungen wurden sowohl reisende[2] als auch regional agierende Straftätergruppierungen identifiziert.

Von den im Jahr 2018 festgestellten Tatverdächtigen sind 92 Personen als reisende Täter einzustufen. Der größte Anteil stammte mit 65 Personen aus den Niederlanden, gefolgt von Tatverdächtigen aus Polen (22 Personen).

Festnahme einer Tätergruppierung in Bayern

Im Oktober 2018 nahmen Spezialeinsatzkräfte der bayerischen Polizei in Germering einen Straftäter anlässlich der Vorbereitung einer unter Einsatz von Gas beabsichtigten Sprengung eines Geldautomaten fest. Dieser hatte versucht, sich mit einem hochmotorisierten PKW rücksichtslos dem Zugriff zu entziehen und verletzte dabei drei Polizeibeamte, einen davon schwer. Ein zweiter Tatbeteiligter konnte sich der Festnahme entziehen.

Im Zuge unmittelbarer Anschlussmaßnahmen wurden in einer nahegelegenen Wohnung drei mutmaßliche Logistikhelfer festgenommen, welche innerhalb der Tätergruppe für das Auskundschaften geeigneter Tatobjekte verantwortlich gewesen sein dürften.

Die Festgenommenen gehören einem kriminellen Netzwerk an, dessen Mitglieder zur Tatbegehung aus den Niederlanden nach Deutschland einreisen. Nach Erkenntnissen der niederländischen Polizei handelt es sich um mehrere hundert Personen, vornehmlich niederländische Staatsangehörige mit marokkanischer Herkunft. Bei der Tatausübung gehen die Personen hochprofessionell vor. Sie sind in der Lage, Geldautomaten innerhalb weniger Minuten zu öffnen und verwenden zur Flucht hauptsächlich hochmotorisierte Kraftfahrzeuge, z. T. aber auch Motorroller.

Kurzbewertung:
Der Sachverhalt ist ein Beispiel für das Agieren von Mitgliedern krimineller Netzwerke, die in allen Tatphasen professionell und arbeitsteilig vorgehen. Das rücksichtslose Fluchtverhalten unter Inkaufnahme von Verletzungen der vor Ort eingesetzten Polizeikräfte unterstreicht das hohe Maß an Gewaltbereitschaft, das die Straftäter an den Tag legen.

[2] Eine reisende Tätergruppierung ist ein Zusammenschluss von Straftätern, die in einem größeren geographischen Raum länderübergreifend und/oder grenzüberschreitend agieren.

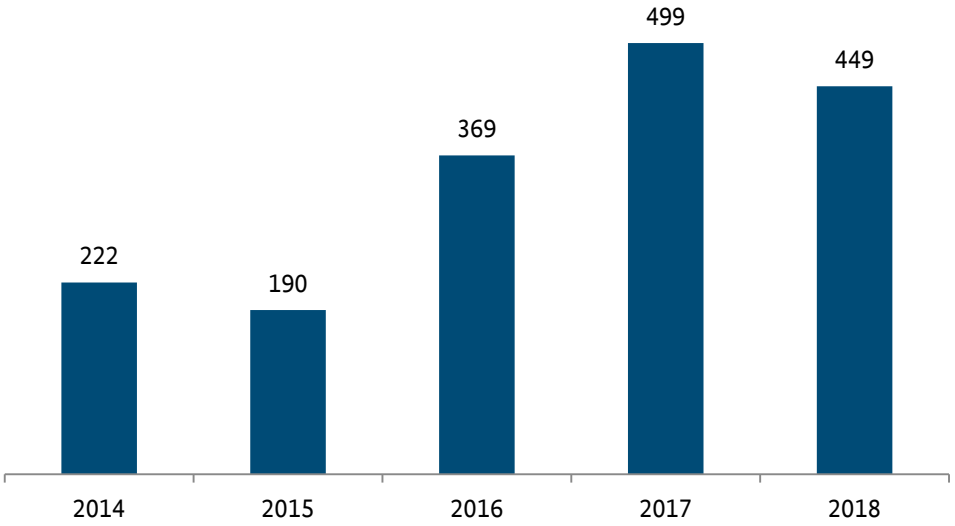
2.2 TECHNISCHE MANIPULATION VON GELDAUTOMATEN

2.2.1 Skimming

Die Modi Operandi im Bereich Skimming sind seit Jahren weitgehend 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 (PIN-Pad) 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.

Im Jahr 2018 war ein Rückgang der Anzahl von Skimming-Fällen zu verzeichnen. Es wurden 449 Angriffe[3] (2017: 499; -10 %) auf Geldautomaten zur Erlangung von Kartendaten (Magnetstreifendaten) und PIN festgestellt[4]. Bedingt durch Mehrfachangriffe auf einzelne Geldautomaten waren insgesamt 202 Geldautomaten (2017: 232; -13 %) betroffen.

Anzahl der Skimming-Angriffe auf Geldautomaten in Deutschland



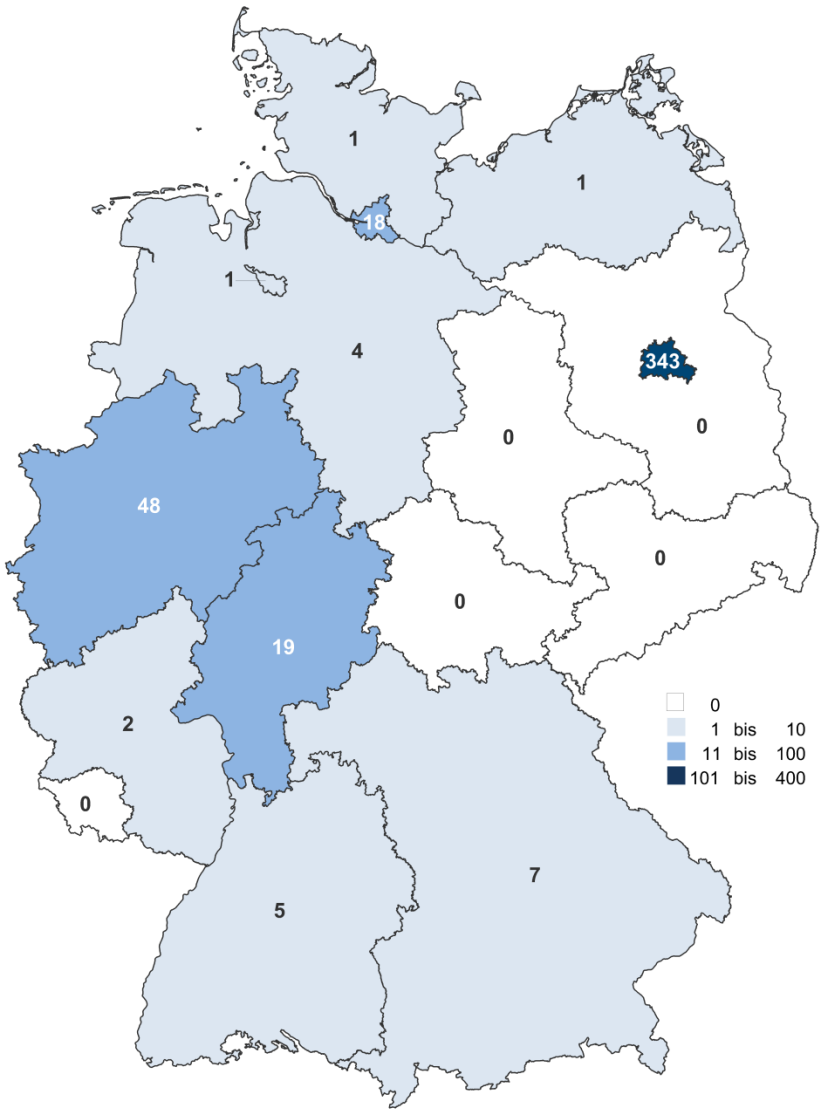
Wenngleich sich die Fallzahlen bei Skimming-Angriffen im Langzeitvergleich gegenüber 2014 in etwa verdoppelt haben, bewegen sie sich angesichts eines bisherigen Höchstwertes von 3.183 Attacken im Jahr 2010 auf einem relativ niedrigen Niveau.

[3] Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimming-Equipment an einem Geldautomaten installieren.
[4] Angaben laut Auskunft der Euro Kartensysteme GmbH.

Mit Abstand die meisten Angriffe wurden in Berlin (343) registriert. Dies dürfte im Wesentlichen der dortigen hohen Anzahl an ausländischen, insbesondere außereuropäischen Touristen geschuldet sein, deren Zahlungskarten teilweise noch nicht mit dem EMV[5]-Chip ausgestattet sind. Daten dieser Karten lassen sich durch die Täter leichter verwerten.

Im Deliktsbereich Skimming treten bereits seit Jahren überwiegend rumänische und bulgarische Tatverdächtige in Erscheinung.

Skimming-Angriffe auf Geldautomaten nach Ländern (2018)



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

Schaden

Belastbare Daten zur bundesweiten Schadensentwicklung liegen der Polizei auch für das Jahr 2018 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.

Angaben der Firma EURO Kartensysteme (EKS) zufolge belief sich der Schaden aus Skimmingfällen zum Nachteil deutscher Kreditinstitute 2018 auf ca. 1,4 Mio. Euro. Dies bedeutet einen Rückgang um 36 %. In Anbetracht einer Schadenssumme von ca. 55 Mio. Euro im Jahr 2010 handelt es sich dabei um ein vergleichsweise geringes Schadensniveau. Auch im Vergleich mit der Schadenssumme von ca. 14,5 Mio. Euro im Zusammenhang mit verlorenen und gestohlenen Zahlungskarten erscheint die Schadenssumme bei Dublettenfällen relativ niedrig.

Verwertungstaten im Ausland

Seit dem 01.01.2011 werden Transaktionen mit Zahlungskarten im SEPA[6]-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"[7] noch eingesetzt werden können.

Brennpunkte des Einsatzes gefälschter Zahlungskarten mit deutschen Kartendaten waren im Jahr 2018 Indien, Indonesien, USA und Puerto Rico. Weitere Verwertungstaten erfolgten hauptsächlich in Mittel- und Südamerika sowie Südostasien.

[6] SEPA: Single Euro Payments Area.
[7] „White Plastics" sind die Kartenrohlinge, auf welche die durch die Täter erlangten Kartendaten übertragen werden.

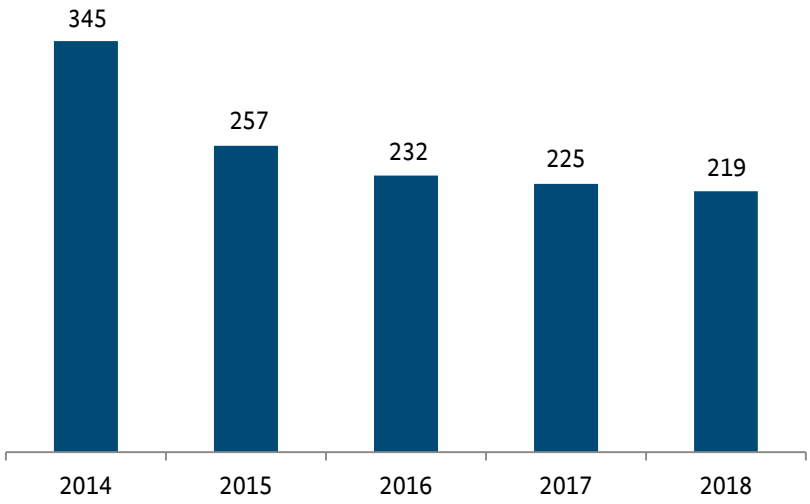
Datenabgriffe im Ausland

Im Jahr 2018 wurden im Ausland bei Manipulationen von insgesamt 219 Geldautomaten und POS-Terminals (2017: 225; -3 %) deutsche Kartendaten und PIN abgegriffen. Der rückläufige Trend der letzten Jahre setzte sich somit fort.

Am häufigsten erfolgten die Datenabgriffe in Mexiko, im Vereinigten Königreich, Italien und Indonesien. Indonesien tritt somit wiederholt nicht nur als Verwertungs-, sondern auch als Datenerlangungsland in Erscheinung.

Die Zahl der registrierten Fälle steht jedoch unter Vorbehalt, da in vielen Auslandsfällen der „Point of Compromise“ (PoC)[8] 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 2018 fort. Erneut 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. Geldautomaten vor solchen Angriffen zu schützen. Gleichwohl wurden seitens der Täter auch im Berichtsjahr herkömmliche, außen am Kartenleser des Geldautomaten angebrachte Vorsatz-Skimmer erfolgreich eingesetzt.

[8] 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 Logische Angriffe auf Geldautomaten bzw. auf Geldautomaten-Netzwerke

Für logische Angriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke existiert keine Legaldefinition. Eine Unterscheidung lässt sich indes anhand folgender Modi Operandi vornehmen:

Jackpotting

Beim Jackpotting wird eine Schadsoftware auf den Rechner des Geldautomaten eingespielt. Anschließend erfolgt über den infizierten Rechner des Geldautomaten ein Zugriff auf das Auszahlungsmodul des Geldautomaten mit dem Ziel, zahlreiche unautorisierte Bargeldauszahlungen nacheinander zu veranlassen.

Blackboxing

Beim Blackboxing handelt es sich um eine Variante des Jackpotting, bei der die Täter den Geldautomaten öffnen, die Kommunikation zwischen dem Rechner des Geldautomaten und dem Auszahlungsmodul unterbrechen und anschließend einen „tätereigenen“ Rechner (Blackbox) an das Auszahlungsmodul anschließen, um unautorisierte Bargeldauszahlungen zu veranlassen.

Netzwerkattacken

Bei Netzwerkattacken werden entweder die Geldautomaten-Netzwerke von Zahlungskarteninstituten oder Netzwerke von kartenausgebenden Banken bzw. deren Processinggesellschaften infiltriert und Schadsoftware in ihnen installiert. So werden u. a. mit der Malware die verschiedenen Zahlungslimits von Kreditkarten außer Kraft gesetzt, woraufhin die Täter mit echten Kreditkarten an Geldautomaten sehr große Summen innerhalb kürzester Zeit abheben können. Derartige missbräuchliche Abhebungen fanden u. a. auch in Deutschland statt, während die betroffenen Zahlungskarteninstitute/Banken ihre Stammsitze in Zentralasien und Afrika haben.

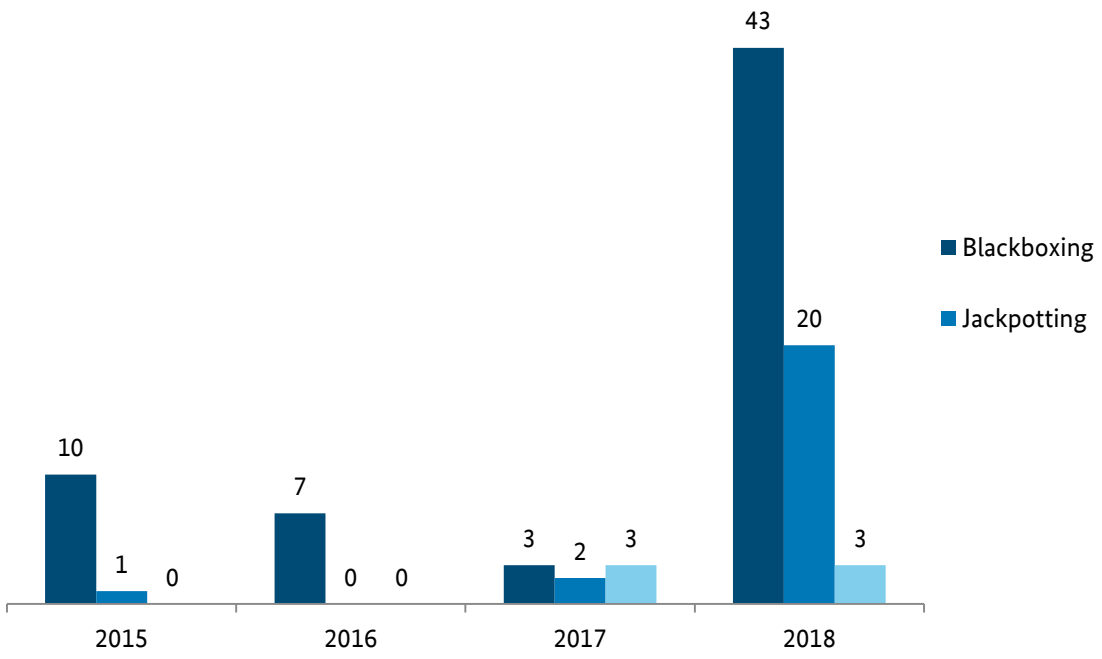
Bei den Netzwerkattacken im Jahr 2018, die dem Bundeskriminalamt bekannt wurden, erfolgten die Malwareangriffe auf Finanzinstitute in Asien. Die anschließenden Cash Outs fanden weltweit, u.a. auch in Deutschland, statt.

Fallzahlen

Im Jahr 2018 kam es zu einem signifikanten Anstieg von Jackpotting-und Blackboxing-Attacken in Deutschland. Die Mehrzahl der Attacken verlief erfolglos, da die Sicherheitsvorkehrungen, z. B. Verschlüsselung der Festplatte (betrifft Jackpotting) bzw. Verschlüsselung der Kommunikation zwischen dem Geldautomaten-Rechner und dem Auszahlungsmodul (betrifft Blackboxing), diese Arten der Angriffe abwehrten.

Die dem Bundeskriminalamt bekannten Schadenssummen belaufen sich auf ca. 540.000 Euro beim Jackpotting und ca. 450.000 Euro beim Blackboxing. Zudem wurden ca. 37.000 Euro bei den in Deutschland durchgeführten kartenbezogenen Cash Outs im Zusammenhang mit Netzwerkattacken durch die Täter erbeutet. Hierbei gilt es zu bedenken, dass die tatsächliche Schadenssumme bedeutend höher gelegen hätte, wenn nicht die meisten Transaktionen abgelehnt worden wären.

Fallzahlen zu logischen Angriffen auf Geldautomaten (2018)



Trotz der in Deutschland von Seiten der Industrie erfolgreich eingeleiteten Präventionsmaßnahmen in Bezug auf logische Angriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke dürfte die Aussicht auf hohe kriminelle Erträge auch weiterhin Anreize für potenzielle Täter bieten. Insofern ist von einer unveränderten Bedrohungslage auszugehen.

3 Gesamtbewertung

Nachdem im Vorjahr ein Rückgang von besonders schweren Fällen des Diebstahls durch Sprengung von Geldautomaten zu verzeichnen war, ist die bundesweite Fallzahl in 2018 deutlich angestiegen und stellt einen neuen Höchstwert seit Beginn der Auswertung dieses Deliktsbereichs durch das Bundeskriminalamt im Jahr 2012 dar.

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 von Geldautomatensprengungen im Einzelfall erhebliche Gefahren für unbeteiligte Dritte wie z. B. Anwohner, Passanten sowie Einsatzkräfte von Feuerwehr und Polizei ausgehen.

Die polizeilichen Erkenntnisse indizieren, dass in Deutschland insbesondere reisende Täter Sprengungen von Geldautomaten verüben. Hier dominieren Tätergruppierungen aus den Niederlanden mit einem hohen Professionalisierungsgrad. Diese dürften auch mitverantwortlich für die neuerlichen Anstiege der Fallzahlen in Nordrhein-Westfalen und Niedersachsen im Jahr 2018 gewesen sein. Gleichwohl sind auch die Fallzahlen in den meisten anderen Ländern angestiegen, womit sich das Phänomen nunmehr bundesweit ausgebreitet hat.

Bereits seit 2015 beschäftigt sich das Bundeskriminalamt verstärkt mit dem Phänomen Geldautomatensprengung. Mit dem Anstieg der Fallzahlen und angesichts der Gefahr, die von diesen Taten ausgeht, rückte dieser Deliktsbereich nicht nur medial in den Vordergrund, sondern stellt inzwischen auch einen Schwerpunkt der polizeilichen Kriminalitätsbekämpfung dar.

Die Fallzahl im Bereich Skimming ist im Jahr 2018 gesunken und befindet sich weiterhin deutlich unter dem Höchststand zu Beginn dieses Jahrzehnts. Die Entwicklung zeigt, dass die in den letzten Jahren mit der Umstellung auf Chiptechnologie eingeführten, überwiegend technischen Sicherheitsmaßnahmen greifen. Skimmingdelikte bleiben, zumindest für Deutschland, kein Kriminalitätsphänomen von herausragender Bedeutung.

Eine neue Qualität der Tatbegehung stellt die Herstellung und Verbreitung von Manipulations-Tools dar, welche es auch technisch nicht versierten Tätern ermöglicht, Manipulationen an Geldautomaten vorzunehmen. Es wird deutlich, dass die Täter auf die Veränderung im Skimmingbereich reagieren und sich mit andersartig gestalteten Angriffen auf Geldautomaten neu aufstellen. Beispiel hierfür sind vermehrte Hackingangriffe auf Geldautomaten-Netzwerke sowie der Anstieg von Jackpotting- und Blackboxing-Fällen, die im Gegensatz zum Skimming eine wesentlich höhere Gewinnerzielung versprechen.

Impressum

Herausgeber

Bundeskriminalamt, 65173 Wiesbaden

Stand

Mai 2019

Gestaltung

Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis

Bundeskriminalamt

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