Bundeskriminalamt

BKA

Angriffe auf Geldautomaten

Bundeslagebild 2019

Angriffe auf Geldautomaten 2019

PHYSISCHE ANGRIFFE AUF GELDAUTOMATEN

369 Fälle, (-6,9 %) ↘
davon 349 Fälle von Sprengungen (-5,4 %) ↘
von Geldautomaten

Sprengungen von Geldautomaten

- 142 vollendete Diebstähle (+3,5 %) ↗
- 207 versuchte Diebstähle (-10,8 %) ↘

132 Tatverdächtige, (+3,1 %) ↗
davon ca. 68 % reisende Täter

Ca. 15,2 Mio. Euro Beuteschaden;
daneben hohe Begleitschäden

ENTWICKLUNGEN

- Weiterhin hohes Gefährdungs- und Schadenspotential durch Sprengungen von Geldautomaten.
- Reisende Täter stammen überwiegend aus den Niederlanden; erstmals keine Tatverdächtigen aus Polen.

TECHNISCHE MANIPULATION VON GELDAUTOMATEN

	Fälle	Krimineller Ertrag
Skimming	244 (-46 %) ↓	ca. 1,4 Mio. € (±0 %) →
Jackpotting	21 (+5 %) ↗	ca. 125.000 € (-77 %) ↓
Blackboxing	47 (+9 %) ↗	ca. 940.000 € (+109 %) ↑
Netzwerkattacken	1 (-67 %) ↓	ca. 10.000 € (-73 %) ↓

ENTWICKLUNGEN

- Starker Rückgang der Skimming-Fälle bei gleichbleibend hohem kriminellen Ertrag
- Starker Anstieg des kriminellen Ertrages beim Jackpotting mittels Blackbox

Inhaltsverzeichnis

1 Vorbemerkung

Das Bundeslagebild „Angriffe auf Geldautomaten“[1] enthält 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 und Erkenntnisse hierzu basieren weitgehend auf den Informationen, die dem Bundeskriminalamt aus dem polizeilichen Nachrichtenaustausch bekannt geworden sind. Gleiches gilt für Diebstähle von Geldautomaten.

Der Bereich der technischen Manipulationen von Geldautomaten umfasst das Fälschen von Zahlungskarten mit zuvor ausgespähten Kartendaten (sog. Skimming) und den anschließenden Einsatz dieser Karten zur Erlangung von Bargeld. In diesem Zusammenhang werden auch Verwertungstaten im Ausland sowie Abgriffe deutscher Kartendaten im Ausland betrachtet. Darüber hinaus beinhaltet dieser Teil des Lagebilds die dem Bundeskriminalamt vorliegenden Erkenntnisse zu verschiedenen Modi Operandi logischer Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke.

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 waren im Jahr 2019 bundesweit 549 physische Angriffe auf Geldautomaten zu verzeichnen. Im Vergleich zum Vorjahr ergab sich somit ein Rückgang von 6,9 % (2018: 590 Angriffe).

Folgende Modi Operandi kamen bei diesen Taten zur Anwendung:

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

Aus strafrechtlicher Sicht handelt es sich bei diesen Tatbegehungsweisen um besonders schwere Fälle des Diebstahls gem. § 243 StGB. Tateinheitlich betroffen sind daneben u. a. auch der Straftatbestand der Sachbeschädigung gem. § 303 StGB sowie bei Sprengungen von Geldautomaten der Straftatbestand der Herbeiführung einer Sprengstoffexplosion gem. § 308 StGB.

2.1.1 Besonders schwere Fälle des Diebstahls durch Sprengung von Geldautomaten

Fallzahlen

Im Jahr 2019 wurden dem Bundeskriminalamt im Phänomenbereich „Sprengung von Geldautomaten“ 349 versuchte und vollendete Fälle bekannt. Im Vergleich zum Vorjahr ist somit ein Rückgang um 5,4 % zu verzeichnen. Die Gesamtfallzahl bleibt indes auf einem hohen Niveau.

In 218 Fällen (-9,1 %) führten die Täter eine Explosion herbei, in 131 Fällen (+1,6 %) wurde die beabsichtigte Sprengung nicht ausgelöst.

In insgesamt 142 Fällen gelangten die Täter nach erfolgreicher Sprengung des Geldautomaten an Bargeld (+3,5 %). Daneben wurden 207 Fälle registriert, bei denen kein Bargeld erbeutet wurde (-10,8 %). Der Versuchsanteil liegt somit bei 59,3 % (2018: 62,9 %).

Neben der Tatsache, dass in einigen Fällen bereits die beabsichtigte Sprengung nicht herbeigeführt wurde, kommt an dieser Stelle auch der Umstand zum Tragen, dass die Täter selbst bei erfolgreichen Sprengungen des Öfteren nicht an Bargeld gelangten. Hierzu dürften auch Sicherheitsvorkehrungen bei den Banken beitragen.

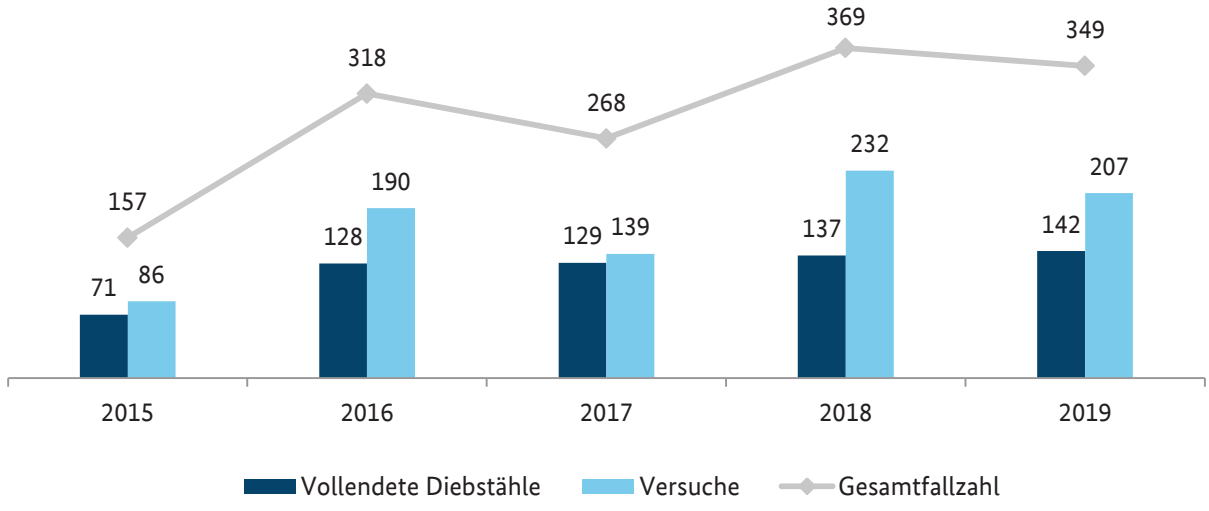
Modus Operandi

Sprengung von Geldautomaten

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 verwendeten Gases, die eingeleitete Menge und den Ort der Einleitung sowie auf die Zündquelle und die Zündleitung.

Dem Bundeskriminalamt wurden für das Jahr 2019 auch 18 Sprengungen von Geldautomaten bekannt, die nicht mit Gas bzw. Gasgemischen, sondern mit Explosivstoffen (z. B. pyrotechnische Sätze, Selbstlaborate, gewerbliche Sprengstoffe) verübt wurden (2018: 20 Fälle).

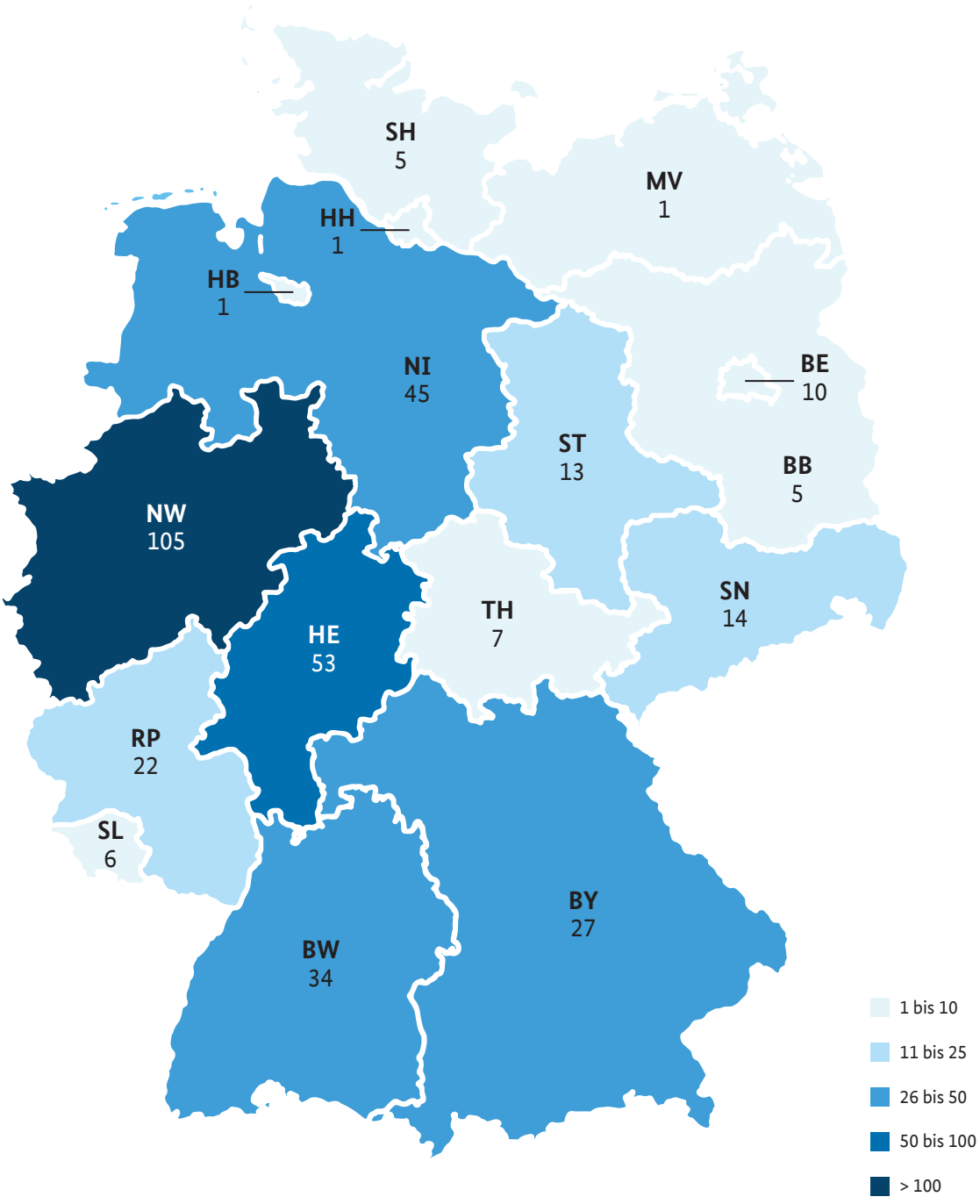
Sprengungen von Geldautomaten (inkl. Versuche) – Fallentwicklung



In 2019 kam es wie auch im Vorjahr in allen Ländern zu Sprengungen von Geldautomaten. Bei der Verteilung der Fälle auf die Länder sind sehr starke regionale Unterschiede festzustellen. Der regionale Brennpunkt lag erneut in Nordrhein-Westfalen (105 Fälle). Des Weiteren waren Hessen, Niedersachsen und Baden-Württemberg überdurchschnittlich stark betroffen.

Während das Fallaufkommen in Hessen (53 Fälle; 2018: 31), Baden-Württemberg (34 Fälle; 2018: 21) oder dem Saarland (6 Fälle; 2018: 1) nicht unerheblich anstieg, konnten in Berlin (10 Fälle; 2018: 23), Mecklenburg-Vorpommern (1 Fall; 2018: 12) und Hamburg (1 Fall; 2018: 11) deutliche Rückgange verzeichnet werden.

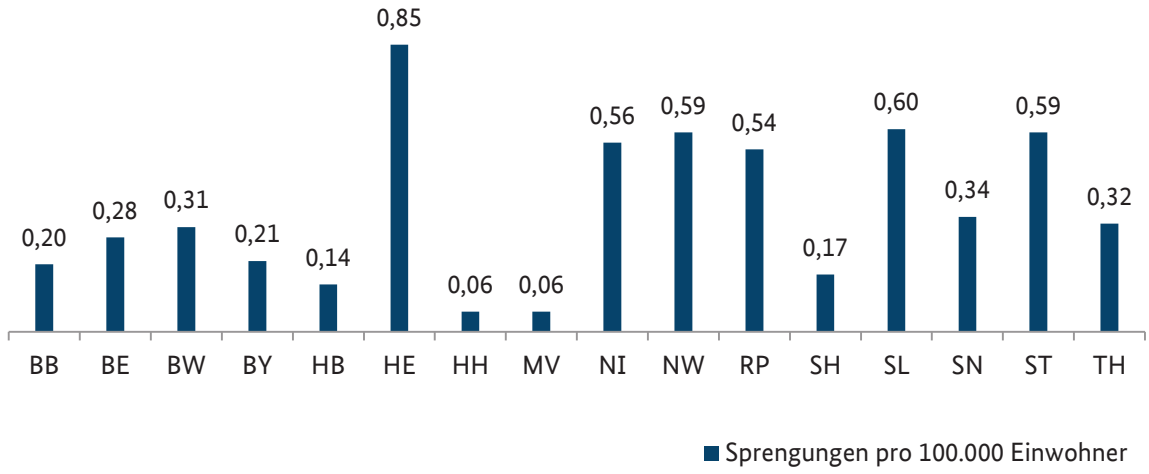
Sprengungen von Geldautomaten (inkl. Versuche) – Verteilung nach Ländern (2019)



Die Betrachtung der absoluten Fallzahlen in den Ländern ist nur bedingt aussagekräftig, da die Anzahl der in einer Region aufgestellten Geldautomaten grundsätzlich abhängig von der jeweiligen Bevölkerungsdichte ist. Insofern ist die Häufigkeitszahl (Sprengungen von Geldautomaten pro 100.000 Einwohner) ein wichtiger Indikator, um die Fallzahlen bewerten sowie Entwicklungen erkennen zu können.

In Bezug auf die Häufigkeitszahl war Hessen in 2019 besonders stark betroffen (0,85 Fälle pro 100.000 Einwohner), gefolgt vom Saarland (0,60), Nordrhein-Westfalen und Sachsen-Anhalt (beide jeweils 0,59). Insbesondere fällt hier die starke Betroffenheit des Saarlands und Sachsen-Anhalts auf, welche im Ländervergleich verhältnismäßig niedrige Gesamtfallzahlen aufweisen.

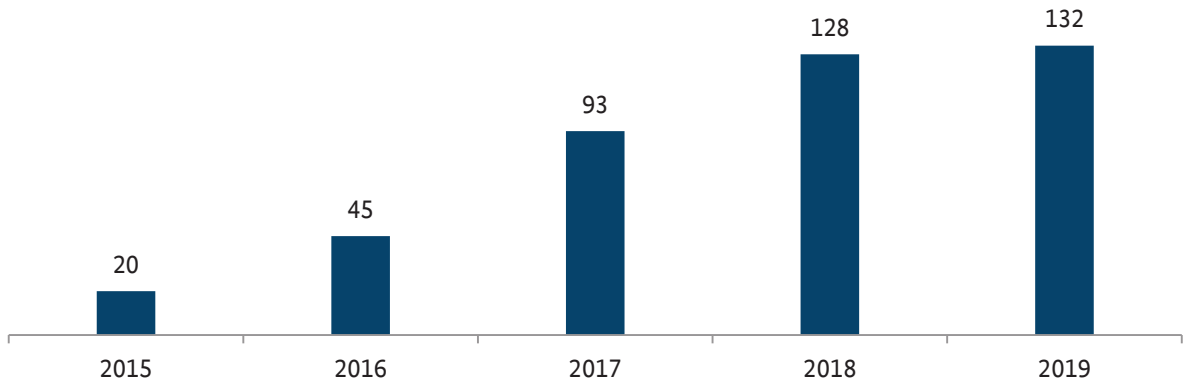
Sprengungen von Geldautomaten (inkl. Versuche) – Häufigkeitszahl (2019)



Tatverdächtige

Im Jahr 2019 wurden dem Bundeskriminalamt 132 Tatverdächtige im Zusammenhang mit Sprengungen von Geldautomaten bekannt. Gegenüber dem Vorjahr (128 Tatverdächtige) bedeutet dies einen leichten Anstieg um 3,1 %.

Sprengungen von Geldautomaten (inkl. Versuche) – Zahl der Tatverdächtigen



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[2] als auch regional agierende Tätergruppierungen festgestellt werden.

Von den im Jahr 2019 festgestellten Tatverdächtigen sind 90 Personen als reisende Täter einzustufen (2018: 92). Wie bereits in den Vorjahren stammte mit 68 Personen der größte Teil reisender Täter aus den Niederlanden, gefolgt von Tatverdächtigen aus Moldawien (10 Personen) und Rumänien (6).

Verurteilung eines Täters zu sechseinhalb Jahren Freiheitsstrafe

Im Juni 2019 wurde ein 33-jähriger, in den Niederlanden lebender marokkanischer Staatsangehöriger vom Mainzer Landgericht zu einer Freiheitsstrafe von sechseinhalb Jahren verurteilt. Das Gericht sah es als erwiesen an, dass der Mann an erfolglosen Geldautomatensprengungen in Mainz 2017 und Karlsruhe 2018 mitgewirkt und sich so in zwei Fällen des Versuchs eines besonders schweren Diebstahls in Tateinheit mit dem Herbeiführen einer Sprengstoffexplosion sowie Sachbeschädigung strafbar gemacht hatte. Der Verurteilte soll Mitglied einer aus den Niederlanden agierenden Bande gewesen sein.

Kurzbewertung:
Der Sachverhalt zeigt, dass die Justiz Sprengungen von Geldautomaten aufgrund der von ihnen ausgehenden hohen Risiken für die Allgemeinheit konsequent verfolgt und sanktioniert. Der Fall ist zugleich ein Beispiel für reisende Täter, die als Mitglied einer Bande oder eines kriminellen Netzwerks länder- und grenzübergreifend agieren.

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

Bei reisenden Tätern aus den Niederlanden handelt es sich überwiegend um Personen aus der Region Utrecht/Amsterdam, die häufig einen marokkanischen Migrationshintergrund aufweisen. Diese Personen agieren in Form eines kriminellen Netzwerks, dessen Mitglieder anlassbezogen in wechselnder Zusammensetzung und wechselnden Tatbeteiligungsverhältnissen agieren. Feste Tätergruppierungen, die auf Dauer angelegt und hierarchisch durchstrukturiert sind, bilden die Ausnahme.

Bei rund 68 % der Tatverdächtigen handelt es sich um reisende Täter.

Im Jahr 2019 wurden dem Bundeskriminalamt erstmals keine Tatverdächtigen aus Polen bekannt (2018: 22). Dies dürfte auf erfolgreich geführte Ermittlungsverfahren polnischer und deutscher Strafverfolgungsbehörden im Jahr 2018 zurückzuführen sein.

Abbildung 1: Sicherheitsvorkehrungen, wie austretender Nebel, hindern die Täter an einer weiteren Tatausführung.

Weiter hohe Beute- und Sachschäden

Durch Sprengungen von Geldautomaten gelangten die Täter im Jahr 2019 an etwa 15,2 Mio. Euro Bargeld (2018: ca. 18 Mio. Euro). Die durchschnittliche Beutesumme lag bei rund 107.000 Euro.

Die durch die Straftaten verursachten Sachschäden übersteigen die Beuteschäden in den meisten Fällen deutlich.

In den meisten Fällen überstiegen die durch die Straftaten verursachten Sachschäden die Beuteschäden deutlich. Auch im Jahr 2019 wurden einzelne Fälle bekannt, in denen der entstandene Sachschaden einen mindestens hohen sechsstelligen Betrag erreicht haben dürfte. Es ist davon auszugehen, dass durch alle registrierten Geldautomatensprengungen – wie in den Vorjahren – Begleitschäden im mittleren zweistelligen Millionenbereich verursacht wurden.

Risiken für unbeteiligte Dritte

Auch im Jahr 2019 wurden seitens der Täter in der Regel Tatzeiten und Tatörtlichkeiten gewählt, in denen kein Kundenbetrieb zu erwarten war. Dennoch besteht auch unter diesen Umständen ein grundsätzlich hohes Risiko für Leib und Leben von Passanten sowie Anwohnern der angegriffenen Objekte. So mussten in vereinzelten Fällen Anwohner wegen Einsturzgefahr nach erfolgten Sprengungen vorsorglich ihre Häuser bzw. Wohnungen verlassen. Unabhängig vom Aufstellort des Geldautomaten bergen Trümmerteile und Splitter einer erfolgten Sprengung hohe Risiken, die von den Tätern nicht abgeschätzt werden können. Zudem können Einsatzkräfte von Feuerwehr und Polizei an den Tatorten u. a aufgrund der Einsturzgefahr beschädigter Gebäude, durch herumliegende Trümmerteile und – insbesondere bei versuchten Sprengungen – aufgrund einer möglicherweise weiterhin bestehenden Explosionsgefahr einer erheblichen Gefährdung ausgesetzt sein.

Geldautomat in Aachen gesprengt – Flüchtige Tatverdächtige festgenommen

Im Juli 2019 wurde in Aachen/NW ein Geldautomat neben einem angrenzenden Verbrauchermarkt gesprengt. Durch die Wucht der Explosion wurde u. a. großflächig die Vorderfront des Bankraumes herausgerissen.

Die Täter flohen mit einem Pkw mit niederländischen Kennzeichen. Nur wenige Stunden nach der Tat konnte die niederländische Polizei fünf Tatverdächtige festnehmen. Diese gehören möglicherweise zu einem Netzwerk von mehreren hundert Personen, die regelmäßig aus den Niederlanden einreisen, um Geldautomatensprengungen in Deutschland zu begehen.

Kurzbewertung:
Der Sachverhalt zeigt beispielhaft das große Schadenspotenzial von Geldautomatensprengungen. Es ist zudem ein weiteres Beispiel für ein kriminelles Netzwerk, dessen Mitglieder in größeren geografischen Räumen 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.

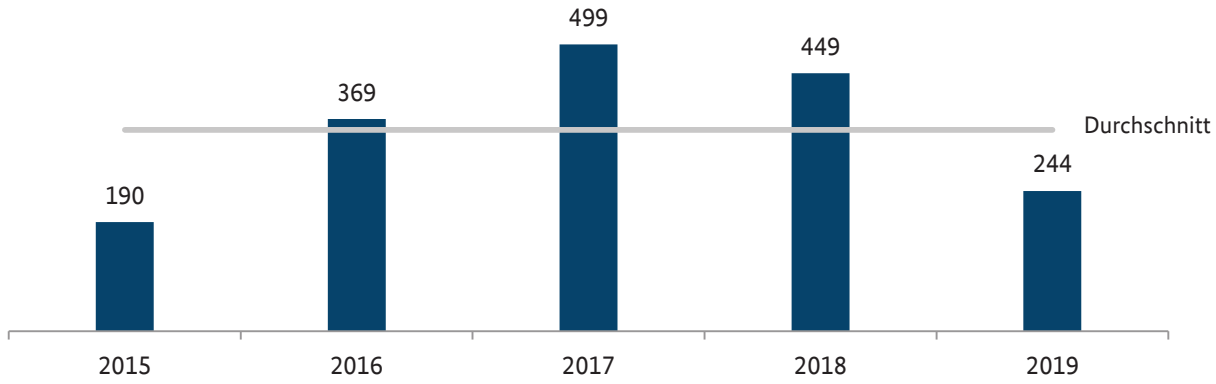
Fallzahlen[3]

In Deutschland wurden im Jahr 2019 insgesamt 244 Skimming-Angriffe[4] festgestellt. Dies stellt einen Rückgang der Fallzahl um ca. 46 % dar (2018: 449 Attacken). Bedingt durch Mehrfachangriffe auf einzelne Geldautomaten waren insgesamt 129 Geldautomaten (2018: 202; -36,2 %) betroffen.

Skimming

Beim sog. „Skimming" (aus dem Englischen: „to skim" – „abschöpfen") greifen die Täter mithilfe technisch manipulierter Lesegeräte Daten von Zahlungskarten ab, die sie selbst verwenden oder gewinnbringend an Dritte veräußern. Mit einer Kopie der Karte und der ausgespähten Geheimzahl (PIN) nehmen die Täter unberechtigte Bargeldabhebungen an Geldautomaten vor.

Skimming-Angriffe auf Geldautomaten – Fallentwicklung



Erstmals kam es nach den Anstiegen in den Jahren 2016 und 2017 und einer moderaten Abnahme in 2018 zu einem deutlichen Rückgang der Fallzahl im Bereich Skimming. Dies indiziert, dass die in den letzten Jahren eingeführten Sicherheitsmaßnahmen, insbesondere die immer weitere Verbreitung von Zahlungskarten mit dem EMV[5]-Chip, greifen. Der Rückgang der Fallzahlen dürfte zudem im Zusammenhang stehen mit der zunehmenden Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen (mechanisch und elektronisch), die ein Auslesen von Kartendaten (Magnetstreifendaten) erschweren.

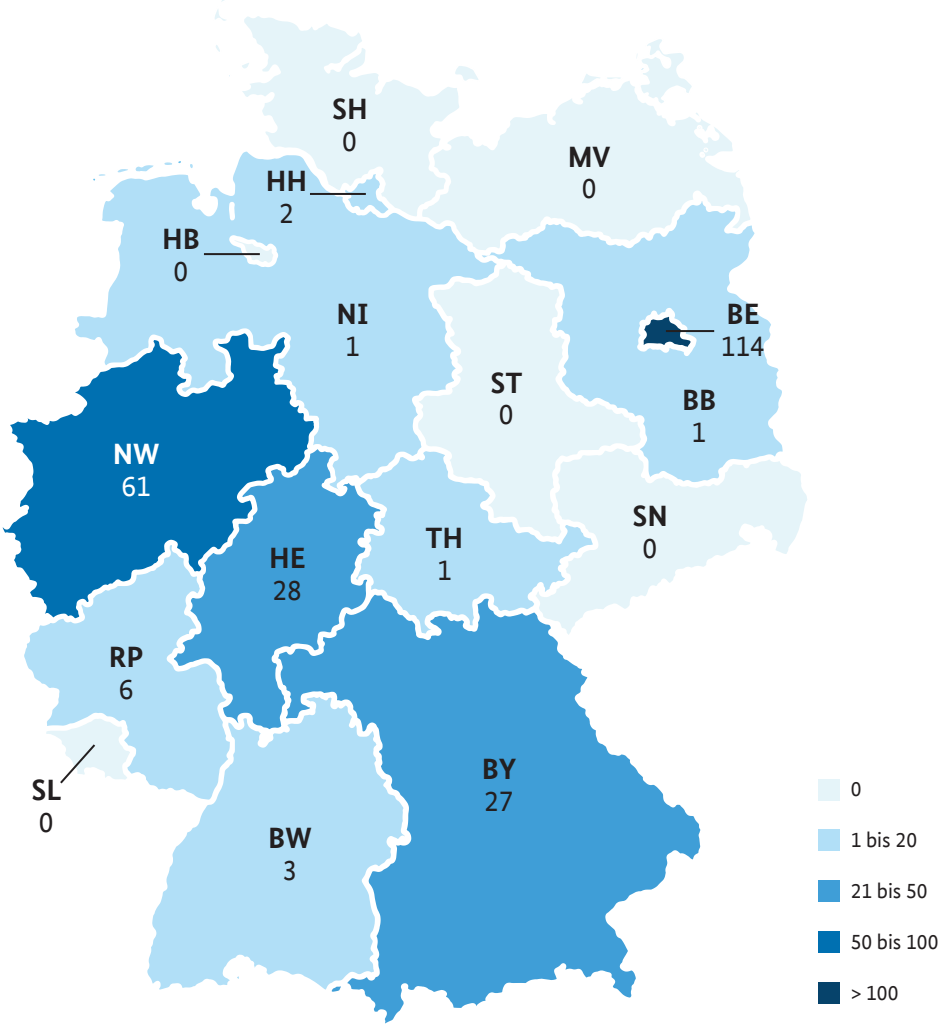
3 Angaben laut Auskunft der Euro Kartensysteme GmbH (EKS), Stand Mai 2020.
4 Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimming-Equipment an einem Geldautomaten installieren.
5 EMV: Europay International, Mastercard, Visa. Durch den EMV-Chip lassen sich Kartendaten schwerer auslesen als bei Zahlungskarten, die lediglich über einen Magnetstreifen verfügen.

Auch angesichts des bisherigen Höchstwerts von 3.183 Skimming-Angriffen im Jahr 2010 kann derzeit von einem verhältnismäßig geringen Bedrohungspotenzial gesprochen werden. Dennoch bleibt festzuhalten, dass die Täterseite weiterhin verbesserte Skimming-Geräte zum Einsatz bringt und sich Verwertungstaten außerhalb des SEPA[6]-Raumes etablieren.

Manipulationen von Geldautomaten erfolgten in zehn Ländern. Bremen, Mecklenburg-Vorpommern, das Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein waren nicht betroffen. Die mit Abstand meisten Angriffe wurden in Berlin registriert (114 Fälle). Zwar zeigt sich auch dort der bundesweite Trend einer deutlich rückläufigen Anzahl an Skimming-Fällen (2018: 343 Fälle; -66,8 %), dennoch ist die Fallzahl im bundesweiten Vergleich weiterhin hoch. Dies dürfte im Wesentlichen darin begründet sein, dass die Täter Geldautomaten an Orten angreifen, an denen sie mit einer hohen Anzahl an ausländischen, insbesondere außereuropäischen Touristen rechnen können, deren Zahlungskarten teilweise nicht mit dem EMV-Chip ausgestattet sind. Abgegriffene Daten dieser Karten lassen sich durch Täter leichter verwerten, wobei die Verwertungstat teilweise bereits in Deutschland erfolgt.

Auch in Deutschland wird ein Kartenprodukt vermarktet, welches nicht mit einem EMV-Chip ausgestattet ist, sondern bei dem die Kartendaten auf Magnetstreifen gespeichert sind. Dubletten dieser Karten sind an Geldautomaten in Deutschland bzw. im SEPA-Raum einsetzbar.

Skimming-Angriffe auf Geldautomaten – Verteilung nach Ländern (2019)



6 SEPA: Single Euro Payments Area.

Tatverdächtige

Im Deliktsbereich Skimming werden im Rahmen des polizeilichen Informationsaustauschs bereits seit Jahren vorrangig rumänische und bulgarische Tatverdächtige bekannt.

Schaden

Da von Skimming betroffene Karteninhaber regelmäßig durch die Geldinstitute und Kreditkartengesellschaften entschädigt werden, wird ein Großteil der Straftaten nicht zur Anzeige gebracht. Darüber hinaus werden Daten zu Verlusten und Missbrauchsumsätzen von der Deutschen Kreditwirtschaft nicht zur Verfügung gestellt. Insofern können keine belastbaren Aussagen zum tatsächlichen bundesweiten Schadensausmaß getroffen werden.

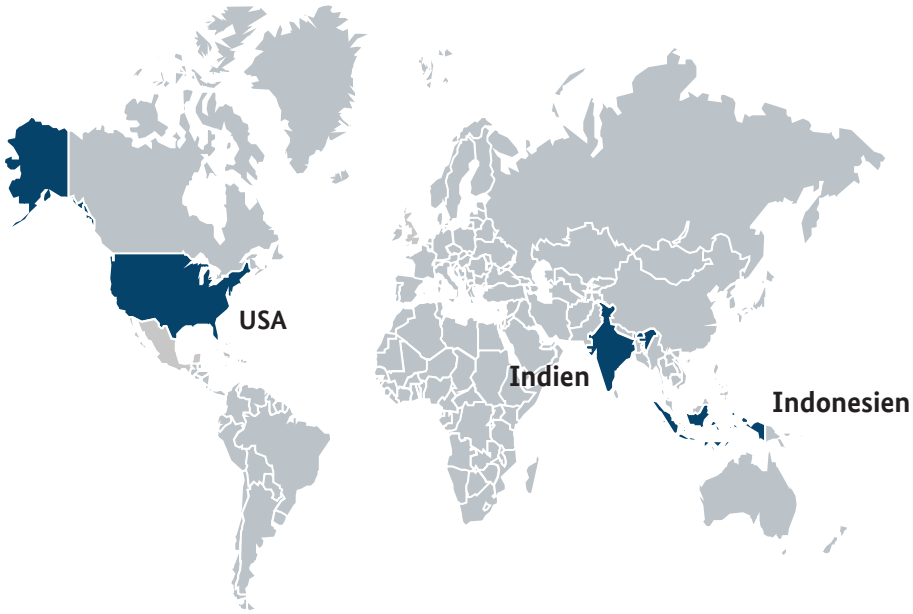
Nach Angaben der EURO Kartensysteme (EKS) betrug der Schaden aus Skimming-Fällen zum Nachteil deutscher Kreditinstitute im Jahr 2019 rund 1,4 Mio. Euro. Trotz des neuerlichen Rückgangs der Skimming-Fälle blieb die Schadenssumme somit nahezu unverändert (2018: ca. 1,4 Mio. Euro). Im Vergleich zum Jahr 2010 (bisher höchste Schadenssumme mit rund 55 Mio. Euro) ist das Schadensniveau indes gering. Auch im Vergleich mit der Schadenssumme von ca. 14,6 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, die mit einem EMV-Chip ausgestattet sind, im SEPA-Raum nicht mehr über den Magnetstreifen, sondern ausschließlich 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 zur Durchführung der Verwertungstaten in sog. „Nicht-Chip-Staaten“ außerhalb des SEPA-Raums, in denen noch auf Magnetstreifenbasis funktionierende „White Plastics“[7] eingesetzt werden können.

Schwerpunktstaaten hinsichtlich des Einsatzes gefälschter Zahlungskarten mit deutschen Kartendaten waren im Jahr 2019 Indien (61,2 %), Indonesien (21,2 %) und die USA (8,7 %). Weitere Verwertungstaten erfolgten hauptsächlich in Mittel- und Südamerika sowie in Südostasien.

Haupteinsatzstaaten gefälschter Zahlungskarten mit deutschen Kartendaten (2019)

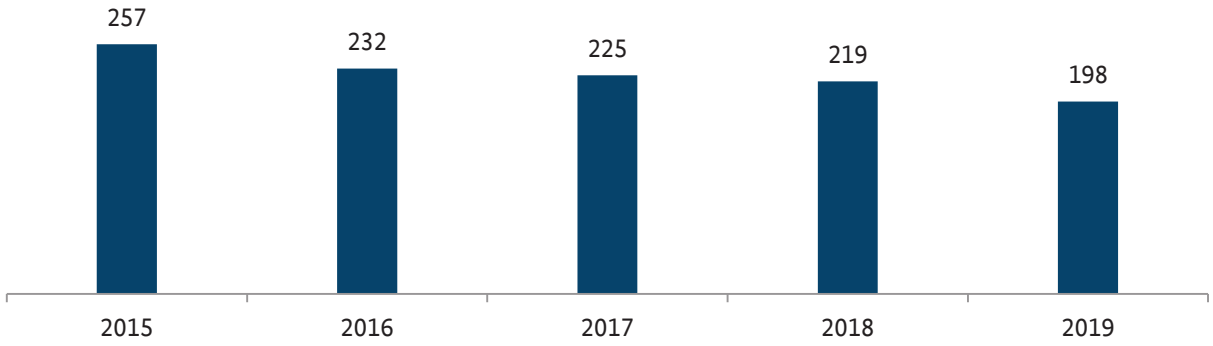


7 „White Plastics” sind die Kartenrohlinge, auf welche die durch die Täter erlangten Kartendaten übertragen werden.

Abgriffe deutscher Kartendaten im Ausland

Im Jahr 2019 wurde der Abgriff von deutschen Kartendaten und PIN durch Manipulationen von insgesamt 198 Geldautomaten und POS-Terminals[8] im Ausland bekannt. Gegenüber dem Vorjahr bedeutet dies einen Rückgang um 10 % (2018: 219 Fälle). Die Fallzahl ist allerdings nur als Näherungswert zu verstehen, da in vielen Auslandsfällen der „Point of Compromise“ (PoC)[9] nicht eindeutig identifiziert werden konnte und diese Fälle somit nicht statistisch berücksichtigt werden konnten.

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



Am häufigsten erfolgten die Datenabgriffe in Großbritannien (54), Italien (31), Mexiko (28) und Indonesien (23). Indonesien trat wiederholt nicht nur als Verwertungs-, sondern auch als Datenerlangungsstaat in Erscheinung.

Stand der Technik bei Skimming-Geräten

Der Trend des Einsatzes von sog. „Deep-Insert-Skimmern“[10] setzte sich auch im Jahr 2019 fort. Seitens der Automatenhersteller wurden technische Maßnahmen getroffen, um „Deep-Insert-Skimmer“ zu detektieren und somit solche Angriffe auf Geldautomaten erfolgreich abzuwehren. Weiterhin wurden seitens der Täter auch im Jahr 2019 herkömmliche, außen am Kartenleser des Geldautomaten angebrachte Vorsatz-Skimmer erfolgreich eingesetzt.

Skimming-Angriffe auf sog. „Tresormat-Anlagen“

In den vergangenen Jahren wurden Fälle bekannt, in denen Schließfächer über sog. „Tresormat-Anlagen“ angegangen wurden. Hierbei handelt es sich um automatisierte Schließfachanlagen, mit deren Hilfe die Schließfachkassetten nach erfolgter Legitimierung durch den Kunden über einen Fördermechanismus aus einem Tresorraum im Keller der Bank zum Bedienautomaten bewegt und dort herausgegeben werden.

Mit ausgespähten Kartendaten wurden Dubletten-Karten erzeugt, mit denen sich die Täter Zugang zu den Tresormat-Anlagen verschafften und mitsamt zugehöriger PIN die Selbstbedienungsautomaten nutzen konnten. Das Ausspähen der Kartendaten erfolgte regelmäßig durch Manipulationen am Kartenlesegerät der Tresormaten.

---

8 Ein „Point-of-Sale-Terminal“ (POS-Terminal) ist ein computergestütztes Gerät zum bargeldlosen Bezahlen an einem Verkaufsort.

9 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.

10 Bei „Deep-Insert-Skimmern“ handelt es sich um Geräte, die innerhalb des Karteneinzugs installiert werden.

2.2.2 Logische Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke

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

Jackpotting mittels Malware

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

Jackpotting mittels Blackbox (sog. Blackboxing)

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

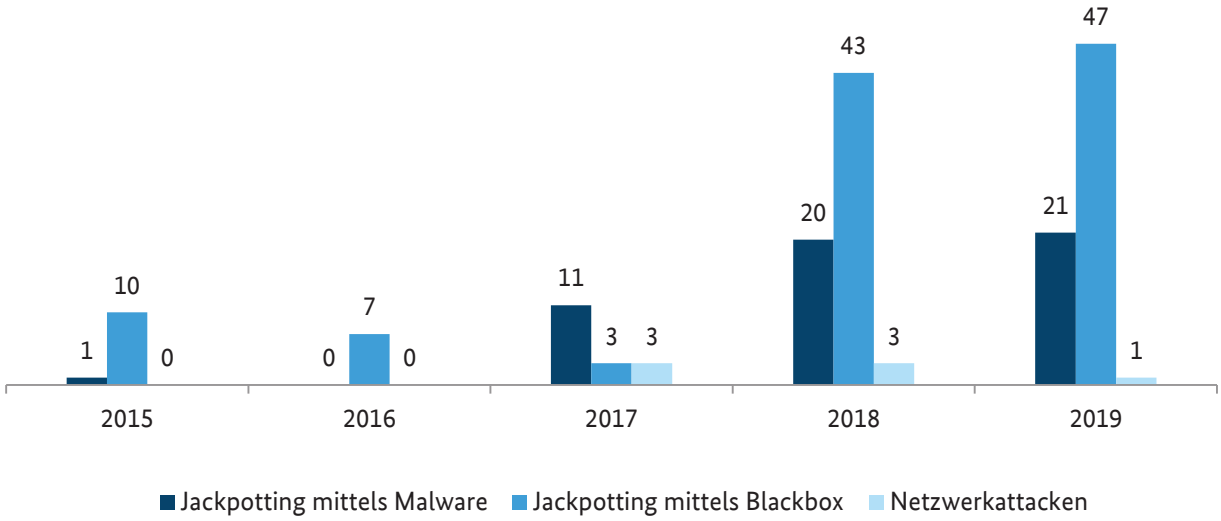
Netzwerkattacken

Bei Netzwerkattacken werden entweder die Geldautomaten-Netzwerke von Zahlungskarteninstituten oder Netzwerke von kartenausgebenden Banken bzw. deren Processinggesellschaften infiltriert und dort Schadsoftware installiert. So werden mit der Malware u. a. die verschiedenen Zahlungslimits von Kreditkarten außer Kraft gesetzt, woraufhin die Täter mit zuvor beschafften echten Kreditkarten an Geldautomaten sehr große Summen innerhalb kürzester Zeit abheben können. Derartige missbräuchliche Abhebungen (sog. „Cash-Outs“) fanden in der Vergangenheit u. a. auch in Deutschland statt, während die betroffenen Zahlungskarteninstitute/Banken ihre Stammsitze in Osteuropa, Süd-/Südostasien und Afrika hatten.

Fallzahlen

Nach einem signifikanten Anstieg von Jackpotting- und Blackboxing-Attacken im Vorjahr bewegten sich die Fallzahlen in Deutschland in 2019 auf einem vergleichbaren Niveau wie 2018.

Logische Angriffe auf Geldautomaten – Fallentwicklung



Die sog. Blackboxing-Attacken erfolgten stets auf denselben Automatentypen. Aufgrund der polizeilichen Ermittlungen konnten insbesondere russische und ukrainische Staatsangehörige als Tatverdächtige identifiziert und festgenommen werden, welche die Angriffe vermutlich serienmäßig begingen.

Die Vielzahl der im Jahr 2019 registrierten Attacken verlief erfolglos, da die getroffenen Sicherheitsvorkehrungen (z. B. Verschlüsselung der Festplatte beim Jackpotting bzw. Verschlüsselung der Kommunikation zwischen dem Geldautomaten-Computer und dem Auszahlungsmodul beim Blackboxing) Angriffe abwehrten. Beim Jackpotting mittels Malware gelangten die Täter in 4 von 21 Fällen an Bargeld (Versuchsanteil: 81 %), beim Jackpotting mittels Blackbox waren 16 der 47 registrierten Angriffe erfolgreich (Versuchsanteil: 66 %). Bei der einzigen, dem Bundeskriminalamt bekannt gewordenen Netzwerkattacke erfolgte der Malwareangriff auf ein Finanzinstitut in Asien. Die anschließenden Cash-Outs fanden weltweit, u. a. auch in Deutschland, statt.

Trotz der in Deutschland von Seiten der Industrie eingeleiteten Präventionsmaßnahmen gegen logische Angriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke muss aufgrund der Aussicht auf hohe kriminelle Erträge für die Täter unverändert von einer hohen Bedrohungslage ausgegangen werden.

Schaden

Der dem Bundeskriminalamt bekannt gewordene Gesamtschaden durch Jackpotting-Angriffe im Jahr 2019 in Deutschland betrug ca. 125.000 Euro (2018: ca. 540.000 Euro). Die durch Blackboxing-Angriffe entstandene Schadenssumme belief sich auf ca. 940.000 Euro (2018: ca. 450.000 Euro).

Zudem wurden im Zusammenhang mit der einzigen, bekannt gewordenen Netzwerkattacke ca. 10.000 Euro bei den in Deutschland durchgeführten kartenbezogenen Cash-Outs durch die Täter erbeutet (2018: 37.000 Euro). Hierbei ist zu beachten, dass die tatsächliche Schadenssumme bedeutend höher gelegen hätte, wenn nicht die meisten Transaktionen abgelehnt worden wären.

3 Gesamtbewertung

Die Bedrohungslage im Bereich der besonders schweren Diebstähle durch Sprengungen von Geldautomaten scheint im Vergleich zum Vorjahr nahezu unverändert. Dies indiziert das ähnlich hohe Fallaufkommen wie im Jahr 2018, in dem ein vorläufiger Höchstwert erreicht wurde.

Bei Sprengungen von Geldautomaten gelangten die Täter auch im Jahr 2019 an teils beträchtliche Geldbeträge, wodurch den Geldinstituten hohe finanzielle Schäden entstanden. Gleichwohl schlug bei der Mehrzahl der Taten entweder bereits die Sprengung selbst fehl oder die Täter gelangten trotz erfolgreicher Sprengung nicht an Bargeld. Hierzu dürften auch verstärkte Sicherheitsvorkehrungen bei den Geldinstituten beigetragen haben.

Die generell im Rahmen der Straftaten verursachten Sach- und Gebäudeschäden sind teils erheblich und in der Gesamtschau zuweilen höher als die Beuteschäden. Hierbei ist zu berücksichtigen, dass von Geldautomatensprengungen im Einzelfall erhebliche Gefahren für unbeteiligte Dritte wie Anwohner, Passanten oder Einsatzkräfte von Feuerwehr und Polizei ausgehen.

Die polizeilichen Erkenntnisse weisen darauf hin, dass Sprengungen von Geldautomaten in Deutschland insbesondere durch reisende Täter begangen werden. Dabei dominieren Tätergruppierungen aus den Niederlanden, die mit einem hohen Professionalisierungsgrad agieren. Da auch in den Niederlanden, Frankreich und Belgien kontinuierlich Anpassungen der Präventionsmaßnahmen gegen Geldautomatensprengungen stattfinden, kommt es regelmäßig zu Verdrängungseffekten, die regionale Anstiege der Fallzahlen insbesondere in grenznahen Ländern wie Nordrhein-Westfalen, Rheinland-Pfalz oder Baden-Württemberg zur Folge haben können.

Dennoch bleibt festzuhalten, dass es sich bei den Sprengungen von Geldautomaten um ein bundesweites Phänomen handelt, welches weiterhin einen Schwerpunkt der polizeilichen Kriminalitätsbekämpfung darstellt. Sonstige Methoden zur Öffnung von Geldautomaten spielen ebenso wie Komplettentwendungen solcher Geräte eine – gegenüber Sprengungen – eher untergeordnete Rolle.

Im Bereich Skimming war im Jahr 2019 ein deutlicher Rückgang der Fallzahl zu verzeichnen. Der Trend bestätigt die Annahme, dass die in den letzten Jahren eingeführten Sicherheitsmaßnahmen, insbesondere die Umstellung auf die EMV-Chip-Technologie, greifen. Trotz verbesserter Skimming-Geräte auf Täterseite besteht in diesem Bereich daher, zumindest für Deutschland, derzeit ein verhältnismäßig geringes Bedrohungspotenzial.

Die Präventionsmaßnahmen im Bereich Skimming führen auf Täterseite dazu, Geldautomaten anderweitig anzugreifen. So nahmen bereits im Jahr 2018 die Zahlen der Jackpotting- und Blackboxing-Fälle deutlich zu. Dieser Trend hat sich im Jahr 2019 bestätigt.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Juli 2020

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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

Diese Publikation wird vom Bundeskriminalamt im Rahmen der Öffentlichkeitsarbeit herausgegeben.
Die Publikation wird kostenlos zur Verfügung gestellt und ist nicht zum Verkauf bestimmt.