Bundeskriminalamt

BKA

Angriffe auf Geldautomaten

Bundeslagebild 2020

Angriffe auf Geldautomaten 2020

PHYSISCHE ANGRIFFE AUF GELDAUTOMATEN

704 Fälle, davon (+28,2 %) ↑

Sprengungen von Geldautomaten

- 414 Fälle (Versuchsanteil: 61,8 %) (+18,6 %) ↑
- 168 Tatverdächtige (+27,3 %) ↑
- ca. 17,1 Mio. Euro Beuteschaden (+12,5 %) ↗

ENTWICKLUNGEN

- Sprunghafter Anstieg von Sprengungen mit festen Explosivstoffen
- ca. 2/3 aller Tatverdächtigen sind reisende Täter aus den Niederlanden

TECHNISCHE MANIPULATIONEN VON GELDAUTOMATEN

Skimming

- 152 Fälle (-38,0 %) ↓
- ca. 1,05 Mio. Euro Beuteschaden (-25,0 %) ↓

Logische (digitale) Systemangriffe

- 15 Fälle (-77,6 %) ↓
- ca. 0,42 Mio. Euro Beuteschaden (-60,9 %) ↓

ENTWICKLUNGEN

- Erneut starker Rückgang der Skimming-Fälle
- Starker Rückgang der Fälle logischer Systemangriffe

Inhaltsverzeichnis

1 Vorbemerkung

Das Bundeslagebild „Angriffe auf Geldautomaten“[1] enthält die aktuellen Erkenntnisse des Bundeskriminalamts zu physischen Angriffen auf und technischen Manipulationen von Geldautomaten mit dem Ziel der Erlangung von Bargeld.

Sprengungen von Geldautomaten sind seit mehreren Jahren ein Auswerteschwerpunkt des Bundeskriminalamts. Die in diesem Zusammenhang vorliegenden Informationen und Daten stammen hauptsächlich aus dem Informationsaustausch mit den Polizeibehörden der Länder. Erkenntnisse zu anderen physischen Angriffen auf Geldautomaten basieren neben Informationen aus dem polizeilichen Nachrichtenaustausch auch auf frei zugänglichen Quellen.

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.

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

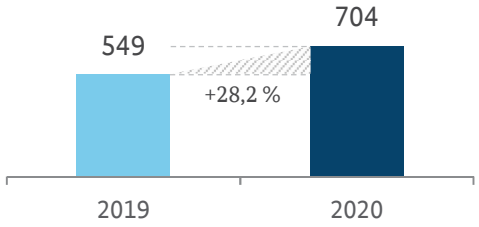
2 Darstellung und Bewertung der Kriminalitätslage

2.1 PHYSISCHE ANGRIFFE AUF GELDAUTOMATEN

2.1.1 Physische Angriffe auf Geldautomaten im Allgemeinen

Gemäß der dem Bundeskriminalamt vorliegenden polizeilichen Erkenntnisse nahm die Zahl der im Jahr 2020 bundesweit festgestellten physischen Angriffe auf Geldautomaten im Vergleich zum Vorjahr zu (+28,2%).

Zahl der festgestellten physischen Angriffe auf Geldautomaten



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)

Sprengungen von Geldautomaten erfüllen strafrechtlich den Verbrechenstatbestand des Herbeiführens einer Sprengstoffexplosion (§ 308 StGB) in Tateinheit mit dem besonders schweren Fall des Diebstahls (§ 243 StGB). Bei allen anderen Angriffsformen handelt es sich um besonders schwere Fälle des Diebstahls, u. a. in Tateinheit mit der Sachbeschädigung gemäß § 303 StGB.

Modus Operandi
Sprengung von Geldautomaten

Geldautomaten werden häufig durch Einleitung eines Gases bzw. Gasgemischs und dessen anschließender Zündung gesprengt. Ausgehend von diesem Grundprinzip unterscheiden sich die Tatbegehungen insbesondere in Bezug auf die Art der verwendeten Gase, die eingeleitete Menge und den Ort der Einleitung sowie die Zündquelle und die Zündleitung.

Daneben werden dem Bundeskriminalamt zunehmend Sprengungen von Geldautomaten bekannt, die nicht mit Gas bzw. Gasgemischen, sondern mit festen Explosivstoffen (insbesondere pyrotechnische Sätze und Selbstlaborate) verübt werden.

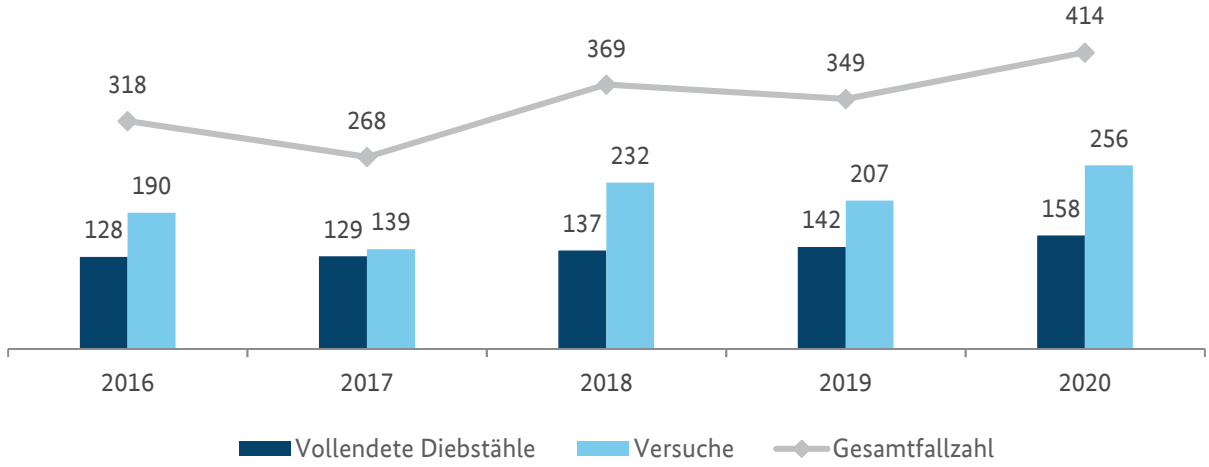
2.1.2 Sprengung von Geldautomaten im Speziellen

Fallzahlen

Im Jahr 2020 wurde ein Anstieg der Fälle von Geldautomatensprengungen um 18,6 % gegenüber dem Vorjahr registriert. In 268 Fällen (2019: 218; +22,9 %) führten die Täter erfolgreich eine Explosion herbei, in 146 Fällen (2019: 131; +11,5 %) wurde die beabsichtigte Sprengung nicht ausgelöst.

Nach erfolgreicher Sprengung des Geldautomaten gelangten die Täter in 158 Fällen an Bargeld (+11,3 %). Bezogen auf die Gesamtfallzahl bedeutet dies einen Anteil vollendeter Fälle besonders schweren Diebstahls von 38,2 % (2019: 40,7 %).

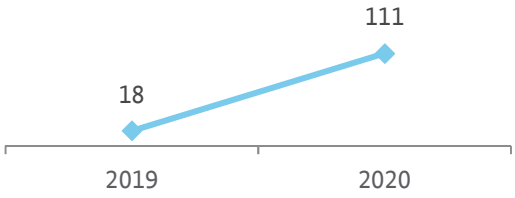
Sprengung von Geldautomaten (inkl. Versuche) – Fallentwicklung



In 2020 stieg die Zahl der Sprengungen von Geldautomaten unter Verwendung von festen Explosivstoffen sprunghaft an. Hier war ein Anstieg um 516,7 % zu verzeichnen.

Anzahl der Sprengungen von Geldautomaten mit festen Explosivstoffen in 2020 sprunghaft angestiegen

Fallentwicklung der Sprengungen mithilfe von festen Explosivstoffen



Die Entwicklung der Taten mit festen Explosivstoffen im Jahr 2020 lässt sich mit großer Wahrscheinlichkeit auf Präventionsmaßnahmen der Betreiber von Geldautomaten in Deutschland (z. B. Gasneutralisationssysteme) sowie verstärkte Präventionsmaßnahmen in den Niederlanden zurückführen. Insbesondere der nächtliche Verschluss bzw. die technische Abschaltung von Geldautomaten in den Niederlanden dürfte zu Verdrängungseffekten nach Deutschland geführt haben. Dabei kommt zum Tragen, dass aus den Niederlanden stammende Tatverdächtigen Sprengungen deutlich häufiger mit festen Explosivstoffen herbeiführen als andere Tätergruppierungen.

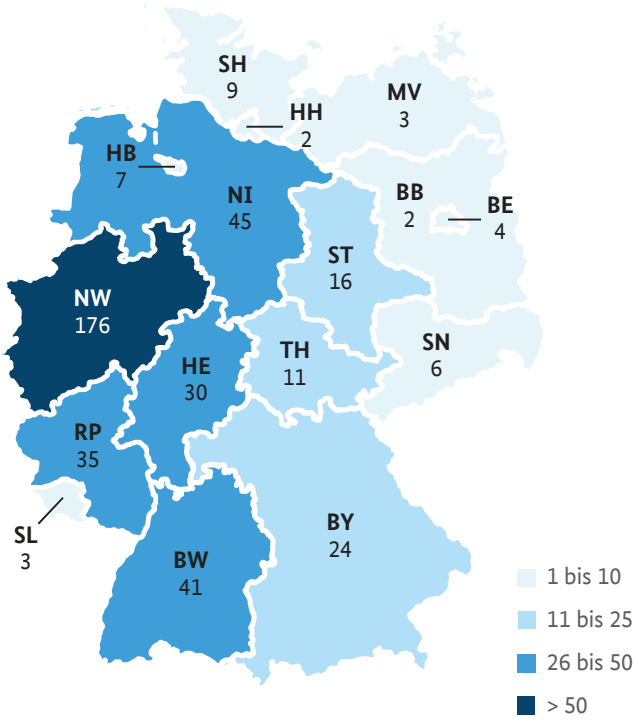
Starke regionale Unterschiede mit Schwerpunkt im Westen Deutschlands

Sprengungen von Geldautomaten waren auch in 2020 bundesweit zu verzeichnen. Hinsichtlich der Verteilung der Fälle auf die Länder waren erneut starke regionale Unterschiede festzustellen. Nach einer erneut deutlichen Zunahme der Anzahl von Geldautomatensprengungen lag der regionale Brennpunkt wie im Vorjahr in Nordrhein-Westfalen (176 Fälle). In den meisten anderen Ländern wurden ebenfalls ansteigende Fallzahlen registriert, lediglich in Hessen kam es zu einem nennenswerten Rückgang des Fallaufkommens (2019: 53 Fälle).

Da die Anzahl der in einer Region aufgestellten Geldautomaten oftmals von der jeweiligen Bevölkerungsdichte abhängt, dient die Häufigkeitszahl[2] als zusätzlicher wichtiger Indikator, um Entwicklungen erkennen zu können. Diesbezüglich fällt – neben den Ländern mit ohnehin erhöhten Fallzahlen – insbesondere auch die starke Betroffenheit Bremens (1,00) und Sachsen-Anhalts (0,73) auf, wenngleich diese verhältnismäßig niedrige absolute Fallzahlen aufweisen.

Gleichwohl bleibt festzuhalten, dass insbesondere die westdeutschen Länder mit Nähe zu den Benelux-Staaten insgesamt deutlich stärker betroffen waren als das restliche Bundesgebiet. Dies dürfte auch auf die bereits beschriebenen Präventionsmaßnahmen in den Niederlanden zurückzuführen sein.

Sprengung von Geldautomaten (inkl. Versuche) – Verteilung nach Ländern



Bundesland	Fallzahlen			HZ
	2019	2020	Trend	2020
Baden-Württemb.	34	41	↗	0,37
Bayern	27	24	↘	0,18
Berlin	10	4	↘	0,11
Brandenburg	5	2	↘	0,08
Bremen	1	7	↗	1,00
Hamburg	1	2	↗	0,06
Hessen	53	30	↓	0,48
Mecklenburg-Vorp.	1	3	↗	0,19
Niedersachsen	45	45	→	0,56
Nordrhein-Westf.	105	176	↑	0,98
Rheinland-Pfalz	22	35	↑	0,85
Saarland	6	3	↘	0,30
Sachsen	14	6	↘	0,15
Sachsen-Anhalt	13	16	↗	0,73
Schleswig-Holstein	5	9	↗	0,31
Thüringen	7	11	↗	0,50

2 Die Häufigkeitszahl gibt die Zahl der Sprengungen von Geldautomaten pro 100.000 Einwohner an.

Tatverdächtige

Mit dem Anstieg der Gesamtfallzahl ging auch ein Anstieg der Zahl registrierter Tatverdächtiger um 27,3 % einher.

Im Zusammenhang mit Sprengungen von Geldautomaten traten in 2020 überwiegend Tatverdächtige mit niederländischer (Anteil: 51,2 %) oder deutscher Staatsangehörigkeit (19,6 %) in Erscheinung.

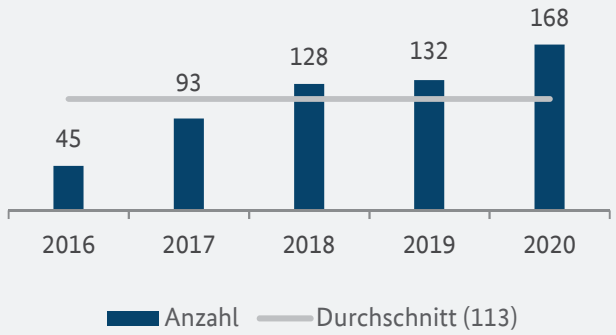
Sprengungen von Geldautomaten werden in der Regel arbeitsteilig durch Tätergruppierungen begangen. Nur in wenigen Fällen sind Einzeltäter aktiv.

Im Rahmen von Ermittlungen konnten im Berichtsjahr sowohl reisende[3] als auch regional agierende Tätergruppierungen festgestellt werden.

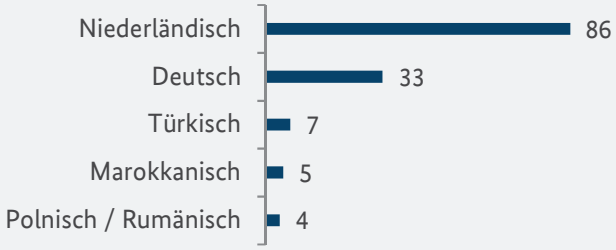
Rund zwei Drittel waren reisende Tatverdächtige aus den Niederlanden

Von den im Jahr 2020 festgestellten Tatverdächtigen sind 71,4 % als reisende Täter einzustufen. Mit 111 Personen hatte der größte Anteil der Tatverdächtigen seinen Lebensmittelpunkt in den Niederlanden. Die im Vergleich zum Vorjahr (2019: 68) deutlich erhöhte Zahl reisender Täter aus den Niederlanden dürfte auf denselben Verdrängungseffekt zurückzuführen sein, der sich auch im Anstieg der Fallzahlen widerspiegelte. Daneben wurden vereinzelt reisende Tatverdächtige mit Lebensmittelpunkt in Rumänien (4), Polen (2), Belgien, Spanien und Ungarn (je 1) festgestellt.

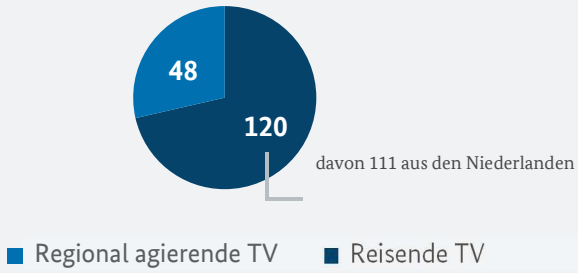
Entwicklung der Anzahl der Tatverdächtigen



Häufigste Staatsangehörigkeiten der Tatverdächtigen



Regional agierende / Reisende[3] Tatverdächtige (TV)

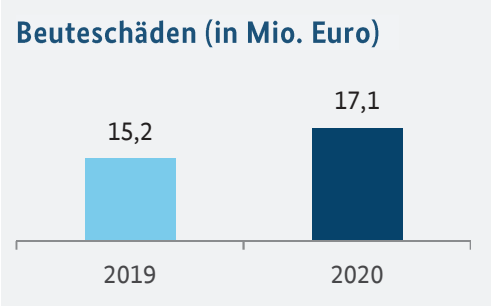


Bei den reisenden Tatverdächtigen aus den Niederlanden handelt es sich weiterhin überwiegend um Personen aus der Region Utrecht/Amsterdam, die häufig einen marokkanischen Migrationshintergrund aufweisen. Diese Personen agieren in Form eines kriminellen Netzwerks, dessen Mitglieder anlassbezogen in wechselnder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

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

Schäden

Die in 2020 durch Sprengungen von Geldautomaten insgesamt erlangte Beutesumme stieg im Vergleich zum Vorjahr um 12,5 % an. Dies entspricht weitestgehend dem Anstieg der Fälle, in denen die Täter nach erfolgreicher Sprengung des Geldautomaten an Bargeld gelangten (+11,3 %).

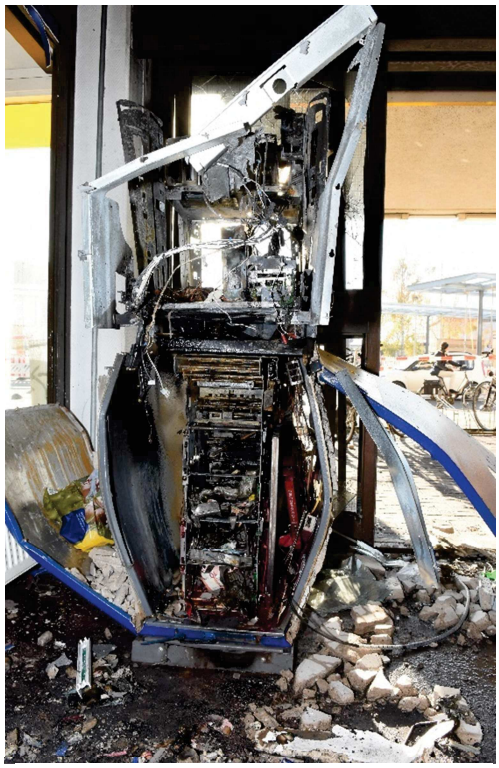


Die durch die Sprengungen von Geldautomaten verursachten Sachschäden überstiegen die Beuteschäden in Teilen deutlich. Wie in den Vorjahren muss davon ausgegangen werden, dass durch die festgestellten Geldautomatensprengungen im Berichtsjahr insgesamt Begleitschäden im mittleren zweistelligen Millionenbereich entstanden sind.

Risiken für unbeteiligte Dritte

Zur Begehung von Geldautomatensprengungen werden in der Regel Tatzeiten und Tatörtlichkeiten ausgewählt, in denen kein Kundenbetrieb zu erwarten ist. Dennoch geht von den Taten eine hohe Gefährdung für Leib und Leben von Passantinnen und Passanten sowie Anwohnerinnen und Anwohnern aus. Insbesondere Trümmerteile und Splitter bergen hohe Risiken, die von der Täterseite nicht abgeschätzt werden können. Zudem sind Einsatzkräfte bei versuchten Sprengungen – aufgrund einer möglicherweise weiterhin bestehenden Explosionsgefahr – einer erheblichen Gefährdung ausgesetzt.

Einsatz von Explosivstoffen birgt hohes Risiko für unbeteiligte Dritte



Gesprengter Geldautomat und umherliegende Trümmerteile

Tödlicher Unfall bei einer Testsprengung in den Niederlanden

Im September 2020 kam es in einer Lagerhalle in Utrecht/Niederlande bei der testweisen Sprengung mit einem selbstlaborierten Explosivstoff, der mutmaßlich zur Begehung von Geldautomatensprengungen bestimmt war, zu einer unkontrollierten Explosion. Dabei wurde eine Person tödlich verletzt, eine weitere Person musste sich in ärztliche Behandlung begeben. Bei dem Getöteten handelte es sich um eine Person, die als Geldautomatensprenger bereits mehrfach in Deutschland in Erscheinung getreten war und insofern über eine umfangreiche Expertise für die Vorbereitung und Ausführung solcher Taten verfügt haben dürfte. Der Unfall verdeutlicht, dass das Risiko im Umgang mit Explosivstoffen auch von solchen Tätern nicht gänzlich kontrolliert werden kann.

2.2 TECHNISCHE MANIPULATIONEN VON GELDAUTOMATEN

2.2.1 Skimming

Von Skimming betroffene Karteninhaber/-innen werden regelmäßig durch die Geldinstitute und Kreditkartengesellschaften entschädigt. Ein Großteil der Straftaten wird daher nicht zur Anzeige gebracht. Aufgrund dessen können auf Basis polizeilicher Erkenntnisse keine belastbaren Aussagen zu Skimming-Angriffen[4] getroffen werden. Die nachfolgenden Aussagen beruhen daher, soweit nicht anders gekennzeichnet, auf Angaben der Euro Kartensysteme GmbH (EKS)[5].

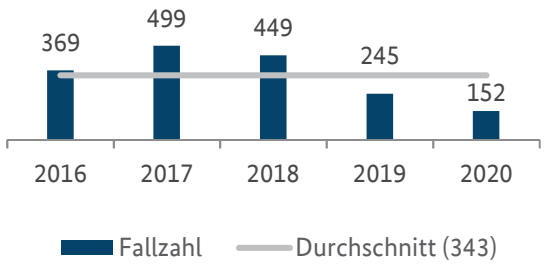
Modus Operandi
„Skimming“

Beim sog. Skimming greifen die Täter durch den Einsatz technisch manipulierter Lesegeräte (sog. Skimmer) die Magnetstreifendaten von Zahlungskarten ab, die sie selbst verwenden oder gewinnbringend an Dritte veräußern. Mithilfe versteckter Mini-Kameras oder unmittelbar auf der Originaltastatur (PIN-Pad) angebrachter Tastaturattrappen wird die eingegebene PIN ausgespäht. Mit einer Kopie der Karte und der ausgespähten Geheimzahl (PIN) nehmen die Täter anschließend unberechtigte Bargeldabhebungen an Geldautomaten vor.

Fallzahlen

Mit einem Rückgang um 38,0 % wurde 2020 in Deutschland ein neuerlicher Tiefstwert festgestellter Skimming-Angriffe im Verlauf der letzten Jahre erreicht. Insgesamt waren 87 Geldautomaten (2019: 130; -33,1 %)[7] betroffen. Verschiedene Geräte wurden mehrfach, im Höchstfall sieben Mal angegriffen.

Skimming-Angriffe – Fallentwicklung[6]



Der deutliche rückläufige Trend der Fallzahlen in den vergangenen beiden Jahren deutet darauf hin, dass die in den letzten Jahren eingeführten Sicherheitsmaßnahmen, insbesondere die immer weitere Verbreitung von Zahlungskarten mit dem EMV[8]-Chip, nachhaltig greifen. Zudem dürfte die Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen, die ein Auslesen von Kartendaten (Magnetstreifendaten) erschweren, zu der Entwicklung beigetragen haben.

Im Jahr 2020 fanden 100 der 152 in Deutschland festgestellten Skimming-Angriffe (65,8 %) an Geldautomaten eines Finanzinstituts statt, welches ein Kartenprodukt ohne EMV-Chip anbietet. Die Täter fokussierten sich offenbar auf Geldautomaten

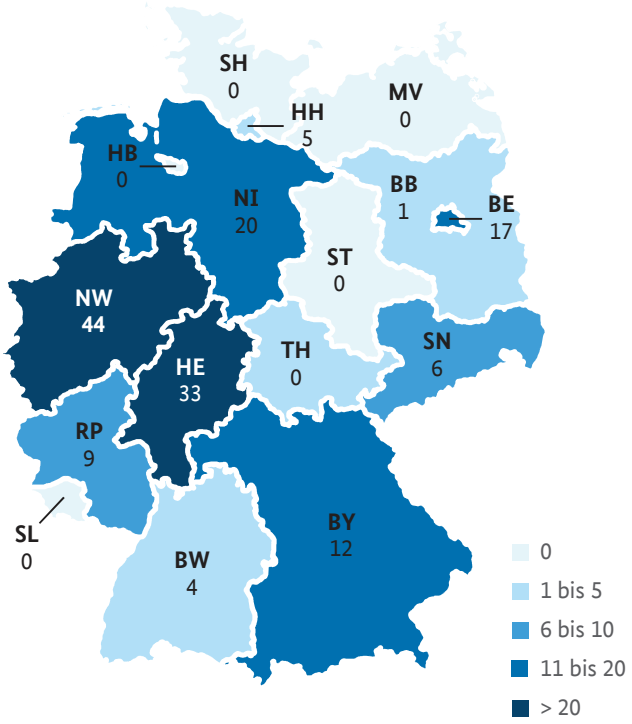
4 Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimming-Equipment an einem Geldautomaten installieren.
5 Die Euro Kartensysteme GmbH (EKS) ist ein Gemeinschaftsunternehmen der deutschen Banken und Sparkassen. Im Bereich des kartengestützten Zahlungsverkehrs erfasst sie u. a. auch Debitkartenschäden deutscher Banken und Sparkassen.
6 Die Fallzahl für 2019 stimmt aufgrund einer nachträglich notwendig gewordenen Anpassung nicht mit der im Bundeslagebild 2019 ausgewiesenen Fallzahl (244) überein.
7 Die Anzahl der betroffenen Geldautomaten in 2019 stimmt aufgrund einer nachträglich notwendig gewordenen Anpassung nicht mit der im Bundeslagebild 2019 ausgewiesenen Zahl (129) überein.
8 EMV: Europay International, Mastercard, Visa. Durch den EMV-Chip lassen sich Kartendaten schwerer auslesen als bei Zahlungskarten, die lediglich über einen Magnetstreifen verfügen.

dieses Instituts, um in den Besitz von Daten dieser Kartenart zu gelangen, bei denen Daten ausschließlich auf einem Magnetstreifen gespeichert werden. Dubletten mit Daten dieses Kartenprodukts lassen sich auch an Geldautomaten in Deutschland verwerten.

Starker Rückgang der Skimming-Angriffe in Berlin

Die Manipulationen der Geldautomaten erfolgten in elf Ländern. Die meisten Angriffe wurden in Nordrhein-Westfalen und Hessen verübt.

Skimming-Angriffe – Verteilung nach Ländern



Wurden in den Vorjahren stets die bundesweit mit Abstand höchsten Fallzahlen in Berlin registriert, nahm das Land in 2020 keine herausragende Stellung mehr ein. Als Grund ist u. a. die Aushebung mehrerer Skimming-Gruppierungen durch die Berliner Polizei im Jahr 2019 anzusehen. Daneben kann ein Verdrängungseffekt von Berlin in andere Städte bzw. Regionen nicht ausgeschlossen werden.

Weiter hatten die Täter in der Vergangenheit insbesondere Geldautomaten an Orten angegriffen, an denen sie mit einer hohen Anzahl an ausländischen, insbesondere außereuropäischen Touristen rechnen konnten, deren Zahlungskarten teilweise nicht mit dem EMV-Chip ausgestattet waren – dies trifft insbesondere auf Berlin zu. Mit den Auswirkungen der Covid-19-Pandemie (insbesondere in Form von zeitweiligen Reisebeschränkungen) auf den internationalen Tourismus hatten sich die diesbezüglichen Rahmenbedingungen im Jahr 2020 geändert.

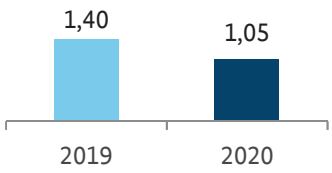
Tatverdächtige

Im Deliktsbereich Skimming werden seit Jahren vorrangig rumänische und bulgarische Tatverdächtige polizeilich bekannt.

Schäden

Nach Angaben der EKS ging der Schaden aus Skimming-Fällen zum Nachteil deutscher Kreditinstitute im Jahr 2020 um rund 25 % zurück. Das hierbei festgestellte Schadensniveau bewegt sich damit im Vergleich zu früheren Jahren (bisher höchste Schadenssumme in 2010 mit rd. 55 Mio. Euro bei 3.183 registrierten Skimming-Angriffen) weiterhin auf einem verhältnismäßig niedrigen Niveau.

Beuteschäden (in Mio. Euro)



Verwertungstaten im Ausland

Im SEPA[9]-Raum werden Geldautomatentransaktionen mit Zahlungskarten, die mit einem EMV-Chip ausgestattet sind, nicht mehr über den Magnetstreifen, sondern ausschließlich über den EMV-Chip autorisiert. Da die Täter jedoch ausschließlich mit Magnetstreifendaten ausgestattete Kartendubletten verwenden, sind sie zur Durchführung ihrer Verwertungstaten gezwungen, in „Nicht-Chip-Staaten" auszuweichen, in denen noch auf Magnetstreifenbasis funktionierende „White Plastics"[10] eingesetzt werden können. Gefälschte Zahlungskarten mit deutschen Kartendaten wurden in 2020 vor allem in Indien (35 %), den USA (27 %), Indonesien (15 %) und Israel (11 %) eingesetzt. Weitere Verwertungsstaaten finden sich in Mittelamerika, hier insbesondere in der Karibik.

Abgriffe deutscher Kartendaten im Ausland

Im Jahr 2020 sank die Fallzahl der im Ausland durch Manipulationen von Geldautomaten und POS-Terminals[11] abgegriffenen deutschen Kartendaten und PIN um 48,0 % auf 103 Fälle (2019: 198 Fälle). Die Fallzahl ist allerdings nur als Näherungswert zu verstehen, da der „Point of Compromise" (PoC)[12] in vielen Auslandsfällen nicht eindeutig identifiziert und diese Fälle somit nicht statistisch berücksichtigt werden konnten. Am häufigsten wurden Datenabgriffe in Großbritannien (39), Indonesien (14) und Italien (12) festgestellt. Wie in den Vorjahren trat Indonesien damit nicht nur als Verwertungs-, sondern auch als Datenerlangungsstaat in Erscheinung.

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

Beim sog. Blackboxing handelt es sich um eine 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

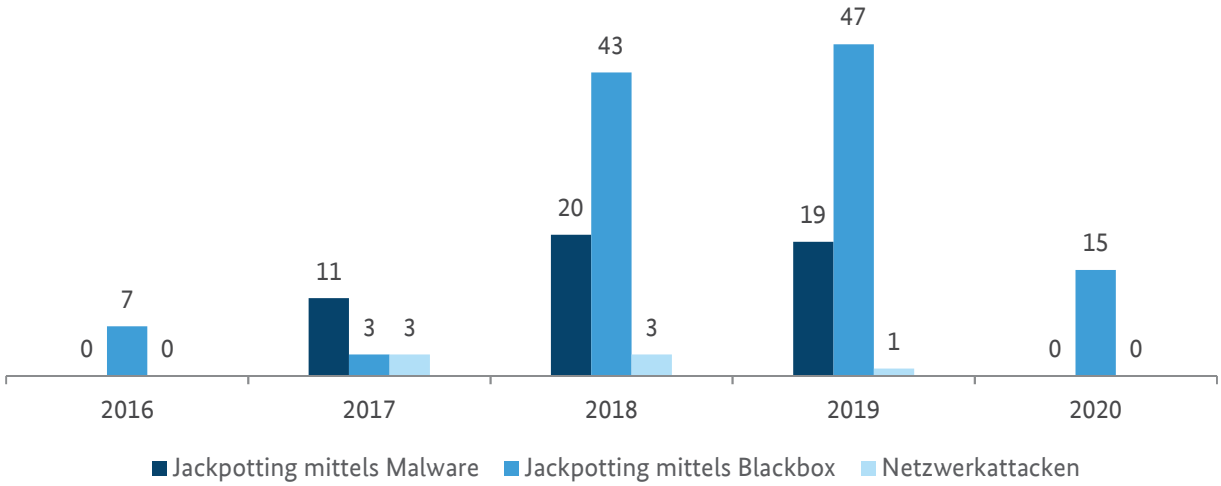
Bei Netzwerkattacken werden entweder die Geldautomaten-Netzwerke von Zahlungskarteninstituten oder Netzwerke von kartenausgebenden Banken bzw. deren Processinggesellschaften mit dem Ziel infiltriert, dort Schadsoftware zu installieren. Mithilfe der Malware werden u. a. die Zahlungslimits von Kreditkarten außer Kraft gesetzt, damit die Täter mit zuvor beschafften echten Kreditkarten an Geldautomaten sehr große Summen innerhalb kürzester Zeit abheben können (sog. Cash-Outs).

9 Single Euro Payments Area.
10 „White Plastics" sind die Kartenrohlinge, auf welche die durch die Täter erlangten Kartendaten übertragen werden.
11 Ein „Point-of-Sale"-Terminal" (POS-Terminal) ist ein computergestütztes Gerät zum bargeldlosen Bezahlen an einem Verkaufsort.
12 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.

Fallzahlen

Im Jahr 2020 wurden erstmals seit 2016 keine Fälle von Jackpotting mittels Malware oder Netzwerkattacken festgestellt. Zudem kam es zu einem starken Rückgang der Fallzahl beim Jackpotting mittels Blackbox (-68,1 %).

Logische Angriffe auf Geldautomaten – Fallentwicklung[13]



Da die Tatverdächtigen fast ausschließlich aus dem Ausland stammen und lediglich zur Tatbegehung nach Deutschland einreisen, kann nicht ausgeschlossen werden, dass der Rückgang der Fallzahl auch im Zusammenhang mit den Auswirkungen der Covid-19-Pandemie (z. B. in Form von zeitweiligen Reisebeschränkungen) steht.

Auch in 2020 erfolgten die Jackpotting-Angriffe mittels Blackbox ausschließlich auf zwei Automatentypen eines Herstellers. Aufgrund von technischen Sicherheitsvorkehrungen, z. B. der Verschlüsselung der Kommunikation zwischen dem PC des Geldautomaten und dem Auszahlungsmodul, wurden die meisten logischen Angriffe auf Geldautomaten abgewehrt. Lediglich vier der 15 festgestellten Jackpotting-Attacken mittels Blackbox verliefen erfolgreich (Versuchsanteil: 73,3 %).

Schäden

Durch die vier erfolgreichen Jackpotting-Attacken mittels Blackbox im Jahr 2020 wurde ein Schaden in Höhe von ca. 420.000 Euro (2019: ca. 940.000 Euro, -55,3 %) verursacht.

13 Die Fallzahl für Jackpotting mittels Malware wurde für das Jahr 2019 nachträglich angepasst und stimmt somit nicht mit der Fallzahl im Bundeslagebild 2019 überein.

3 Gesamtbewertung

Die Bedrohungslage durch Sprengungen von Geldautomaten in Deutschland ist weiterhin hoch. Nach einem leichten Rückgang besonders schwerer Fälle des Diebstahls durch Sprengung von Geldautomaten im Vorjahr kam es in 2020 zu einem Höchstwert seit Beginn der statistischen Erfassung dieses Phänomenbereiches durch das Bundeskriminalamt im Jahr 2005. Zugleich nahmen im Berichtsjahr die Anzahl der Tatverdächtigen sowie der festgestellte Beuteschaden zu.

Auffallend war im Jahr 2020 insbesondere der sprunghafte Anstieg von Sprengungen von Geldautomaten unter Verwendung fester Explosivstoffe. Ebenso wie die noch immer am häufigsten angewandte Sprengweise durch Entzündung eines zuvor in den Geldautomaten eingeleiteten Gases bzw. Gasgemischs beinhalten solche Fälle ein hohes Risiko für Leib und Leben von unbeteiligten Dritten oder Einsatzkräften.

Kennzeichnend für den Phänomenbereich ist weiterhin eine bundesweite Betroffenheit, auch wenn sich im Berichtjahr ein sehr deutlicher Schwerpunkt im Westen Deutschlands zeigte. Ursächlich für die starke Zunahme der Straftaten im Westen Deutschlands können Verdrängungseffekte aufgrund verstärkter Präventionsmaßnahmen in den Niederlanden gewesen sein, zumal niederländische Staatsangehörige bei den Tatverdächtigen und reisende Tatverdächtige aus den Niederlanden deutlich überrepräsentiert sind.

Der Phänomenbereich Sprengungen von Geldautomaten bildet bereits seit längerem einen Schwerpunkt der polizeilichen Kriminalitätsbekämpfung. Vor dem Hintergrund der vielfach staatenübergreifenden Tatbegehung kommt der verstärkten Kooperation mit internationalen Partnern, insbesondere mit niederländischen Strafverfolgungsbehörden, eine große Bedeutung zu.

Im Phänomenbereich Skimming kam es im Jahr 2020 erneut zu einem starken Rückgang der Fallzahl und des durch Abgriffe von Kartendaten verursachten Gesamtschadens. Insbesondere im Vergleich mit dem Höchststand von Skimming-Angriffen im Jahr 2010 und des damaligen Gesamtschadens ist das Bedrohungspotenzial verhältnismäßig gering.

Auch im Bereich der logischen Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke ist die Fallzahl gesunken. Gleichwohl ist die Entwicklung aufgrund der für die Täterseite bestehenden Aussicht auf mitunter hohe kriminelle Erträge weiter im Blick zu behalten.

Ob und inwieweit sich auch die Covid-19-Pandemie auf die Fallzahlen ausgewirkt hat, lässt sich nicht abschließend bewerten. Teilentwicklungen, wie die rückläufige Anzahl der Skimming-Angriffe oder die der logischen Angriffe auf Geldautomaten, legen zumindest die Vermutung einer entsprechenden Einflussnahme durch die Covid-19-Pandemie und den damit einhergehenden Reisebeschränkungen nahe.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Juni 2021

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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