



Bundeskriminalamt

BKA



Angriffe auf Geldautomaten

Bundeslagebild 2021

Angriffe auf Geldautomaten 2021

PHYSISCHE ANGRIFFE AUF GELDAUTOMATEN



579 physische Angriffe, (-17,8 %) ↘

davon Sprengungen von Geldautomaten



392 Fälle (Versuchsanteil: 51,8 %) (-5,3 %) ↘

darunter 250 Fälle mit festen Explosivstoffen (+125,2 %) ↑



124 Tatverdächtige (-26,2 %) ↘



ca. 19,5 Mio. Euro Beuteschaden (+14,0 %) ↗

ENTWICKLUNGEN

- Trotz Rückgangs der Gesamtfallzahl neuer Höchststand vollendeter Taten
- Vermehrte Verwendung fester Explosivstoffe mit hohem Gefahrenpotenzial setzt sich fort

TECHNISCHE MANIPULATIONEN VON GELDAUTOMATEN



Skimming



137 Fälle (-9,9 %) ↘



ca. 0,57 Mio. Euro Beuteschaden (-46,2 %) ↘



Logische (digitale) Systemangriffe



21 Fälle (+40,0 %) ↗



ca. 0,09 Mio. Euro Beuteschaden (-78,8 %) ↘

ENTWICKLUNGEN

- Sämtliche Skimming-Angriffe an Geldautomaten nur eines Finanzinstituts
- Nahezu alle logischen Systemangriffe Teil einer europaweiten Tatserie

Inhaltsverzeichnis

1	Vorbemerkung.....	4
2	Darstellung und Bewertung der Kriminalitätslage	4
2.1	Physische Angriffe auf Geldautomaten	4
2.1.1	Physische Angriffe auf Geldautomaten im Allgemeinen.....	4
2.1.2	Sprenkung von Geldautomaten im Speziellen.....	5
2.2	Technische Manipulationen von Geldautomaten.....	10
2.2.1	Skimming.....	10
2.2.2	Logische Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke	12
3	Gesamtbewertung.....	15

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 auf Informationen aus dem polizeilichen Nachrichtenaustausch sowie aus 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 Verwertungsstätten im Ausland betrachtet. Darüber hinaus beinhaltet dieser Teil des Lagebilds die dem Bundeskriminalamt vorliegenden Erkenntnisse zu verschiedenen Modi Operandi logischer (digitaler) Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke.

2 Darstellung und Bewertung der Kriminalitätslage

2.1 PHYSISCHE ANGRIFFE AUF GELDAUTOMATEN

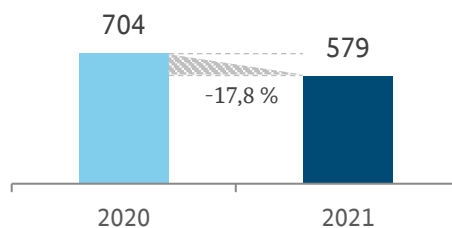
2.1.1 Physische Angriffe auf Geldautomaten im Allgemeinen

Die Anzahl der im Jahr 2021 bundesweit festgestellten physischen Angriffe auf Geldautomaten nahm im Vergleich zum Vorjahr ab (-17,8 %).

Folgende Modi Operandi wurden bei diesen Taten angewandt:

- 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)

Zahl der festgestellten physischen Angriffe auf Geldautomaten



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.

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

2.1.2 Sprengung von Geldautomaten im Speziellen

Modus Operandi

Geldautomaten werden inzwischen überwiegend mithilfe fester Explosivstoffe gesprengt. Dabei kommen insbesondere pyrotechnische Sätze und Selbstlaborate zum Einsatz.



Daneben ist weiterhin die Sprengung durch Einleitung eines Gases bzw. Gasgemischs und dessen anschließender Zündung gängiger Modus Operandi. Die Tatbegehung unterscheidet sich in diesen Fällen insbesondere in Bezug auf die Art des verwendeten Gases, die eingeleitete Menge und den Ort der Einleitung sowie die Zündquelle und die Zündleitung.

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 Unbeteiligter aus.

Insbesondere Trümmerteile und Splitter bergen hohe Risiken, die von den Tätern nicht abgeschätzt werden können. Der verstärkte Einsatz fester Explosivstoffe stellt für Anwohnerinnen und Anwohner in unmittelbarer Umgebung von Geldautomaten eine erhöhte Gefährdung dar, da die Täter häufig nicht in der Lage sind, diese vollständig zu kontrollieren. Zudem sind Einsatzkräfte bei versuchten Sprengungen – aufgrund einer möglicherweise weiterhin bestehenden Explosionsgefahr – einer erheblichen Gefährdung ausgesetzt.

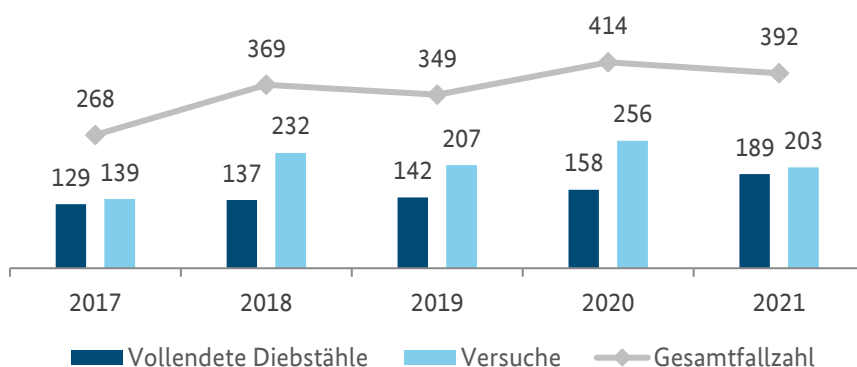
Die Taten sind häufig gekennzeichnet durch ein rücksichtsloses Fluchtverhalten mit hochmotorisierten Fahrzeugen. Auch hiervon geht eine erhebliche Gefährdung Dritter aus.

Große Risiken für Unbeteiligte

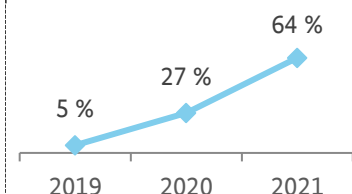
Fallzahlen

Im Jahr 2021 war ein leichter Rückgang der Fälle von Geldautomatensprengungen um 5,3 % gegenüber dem Vorjahr zu verzeichnen.

Sprengung von Geldautomaten – jährliche Fallentwicklung



Anteil Sprengungen mit Hilfe fester Explosivstoffe

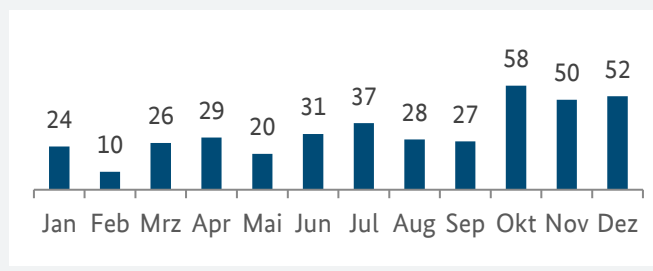


In 287 Fällen (2020: 268; +7,1 %) führten die Täter erfolgreich eine Explosion herbei, in lediglich 105 Fällen (2020: 146; -28,1 %) wurde die beabsichtigte Sprengung nicht ausgelöst.

Nach erfolgreicher Sprengung des Geldautomaten gelangten die Täter in 189 Fällen an Bargeld (2020: 158; +19,6 %). Bezogen auf die Gesamtfallzahl bedeutet dies einen Anteil vollendeter Fälle besonders schweren Diebstahls von 48,2 % (2020: 38,2 %).

Geldautomaten wurden im Jahr 2021 überwiegend mithilfe fester Explosivstoffe gesprengt (250 Fälle; 2020: 111). Damit setzt sich der bereits im Vorjahr registrierte signifikante Anstieg fort.

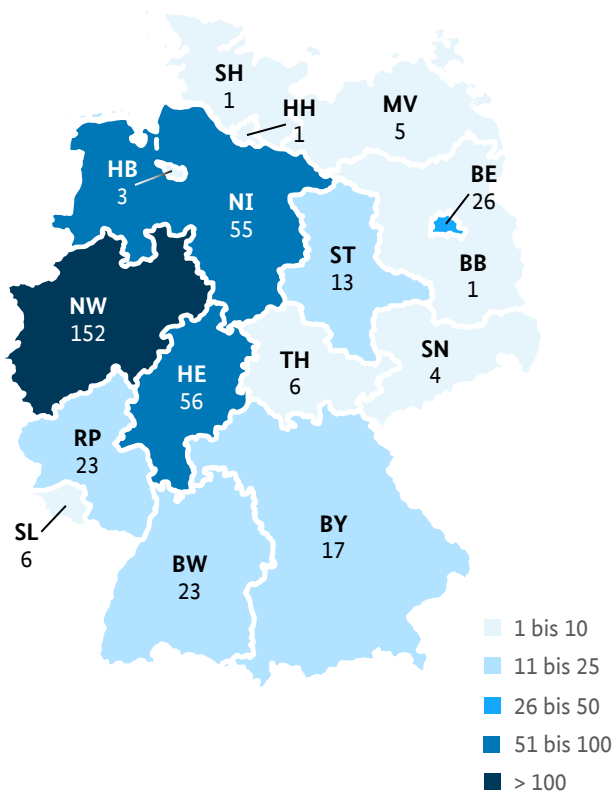
Sprengung von Geldautomaten (inkl. Versuche) – monatliche Fallentwicklung 2021



Vor dem Hintergrund der Tatsache, dass ein großer Teil der Tatverdächtigen aus den Niederlanden stammt und zu den Taten nach Deutschland einreist, ist der Rückgang der Gesamtfallzahl mit großer Wahrscheinlichkeit auch auf Maßnahmen im Zusammenhang mit der Corona-Pandemie zurückzuführen. In den Niederlanden wurden für den Zeitraum vom 23.01.2021 bis zum 28.04.2021 nächtliche Ausgangssperren angeordnet. Ab dem

24.04.2021 bis zum 30.06.2021 kam es auch in Deutschland regional zu entsprechenden Maßnahmen. Angesichts der vergleichsweise niedrigen Fallzahlen im ersten Halbjahr kann davon ausgegangen werden, dass sich die Maßnahmen zur Eindämmung der Pandemie auf die Fallzahlen ausgewirkt haben. Im Vergleich dazu nahmen diese im zweiten Halbjahr, insbesondere im letzten Quartal 2021, wieder deutlich zu.

Sprengung von Geldautomaten (inkl. Versuche) – Verteilung nach Ländern / Häufigkeitszahl²



Land	Fallzahlen			HZ 2021
	2020	2021	Trend	
BB	2	1	↘	0,04
BE	4	26	↑	0,71
BW	41	23	↘	0,21
BY	24	17	↘	0,13
HB	7	3	↘	0,44
HE	30	56	↑	0,89
HH	2	1	↘	0,05
MV	3	5	↗	0,31
NI	45	55	↗	0,69
NW	176	152	↘	0,85
RP	35	23	↘	0,56
SH	9	1	↘	0,03
SL	3	6	↗	0,61
SN	6	4	↘	0,10
ST	16	13	↘	0,60
TH	11	6	↘	0,28

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

Sprengungen von Geldautomaten waren auch in 2021 bundesweit zu verzeichnen, wobei weiterhin starke regionale Unterschiede festzustellen sind. Den regionalen Brennpunkt bildete auch in 2021

Steigende Fallzahlen vor allem in Berlin und Hessen

Nordrhein-Westfalen. Ein starker Anstieg der Fallzahl war zudem in Berlin und Hessen zu verzeichnen. Lediglich in Baden-Württemberg kam es zu einem nennenswerten Rückgang des Fallaufkommens.

Da die Anzahl der in einer Region aufgestellten Geldautomaten oftmals von der jeweiligen Bevölkerungsdichte abhängt, dient die Häufigkeitszahl als zusätzlicher wichtiger Indikator, um Entwicklungen erkennen zu können. Diesbezüglich fällt insbesondere die vergleichsweise starke Betroffenheit Hessens und Berlins auf. Gleichwohl bleibt festzuhalten, dass insbesondere die westdeutschen Länder mit Nähe zu den Niederlanden insgesamt deutlich stärker betroffen waren als das restliche Bundesgebiet.

Tatverdächtige

Mit dem Rückgang der Gesamtfallzahl ging auch ein Rückgang der Zahl der im Zusammenhang mit Sprengungen von Geldautomaten festgestellten Tatverdächtigen um 26,2 % einher.

In 2021 traten im Zusammenhang mit Sprengungen von Geldautomaten erneut überwiegend Tatverdächtige mit niederländischer (Anteil: 50,8 %) oder deutscher Staatsangehörigkeit (25,8 %) in Erscheinung.

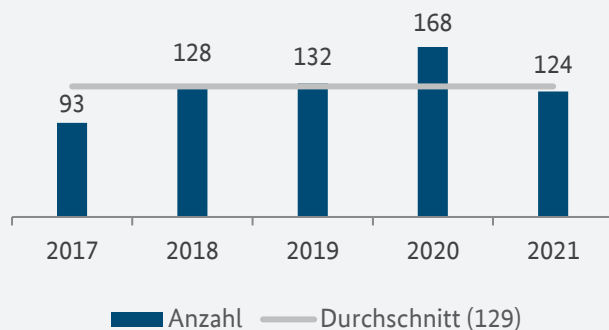
Sprengungen von Geldautomaten werden in der Regel arbeitsteilig durch Tätergruppierungen begangen. Nur in wenigen Fällen sind Einzeltäter aktiv.

Deutlich weniger reisende Tatverdächtige als 2020

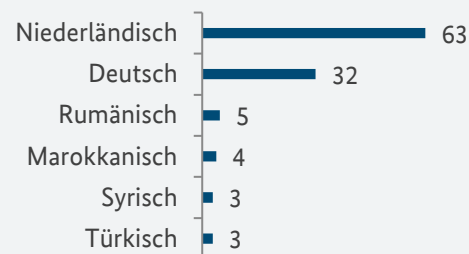
Im Rahmen von Ermittlungen konnten in 2021 sowohl reisende³ als auch regional agierende Tätergruppierungen festgestellt werden.

Die Zahl der regional agierenden Tatverdächtigen entsprach nahezu dem Vorjahresniveau (2020: 48). Hinsichtlich der Anzahl der Tatverdächtigen, welche als reisende Täter einzustufen sind, war ebenso

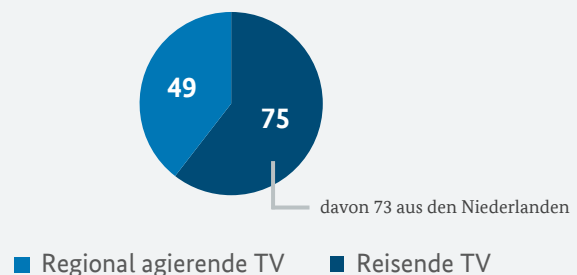
Entwicklung der Anzahl der Tatverdächtigen



Häufigste Staatsangehörigkeiten der Tatverdächtigen



Regional agierende / Reisende³ Tatverdächtige (TV)



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

ein starker Rückgang festzustellen (2020: 120) wie bei ihrem Anteil an allen Tatverdächtigen (60,5 %; 2020: 71,4 %). Der Rückgang dürfte im Zusammenhang mit der COVID-19-Pandemie und den damit einhergehenden Maßnahmen zur Eindämmung (z. B. Ausgangssperren) stehen.

Mit 73 Personen hatte erneut der weit überwiegende Teil der reisenden Tatverdächtigen seinen Lebensmittelpunkt in den Niederlanden (2020: 111). Daneben wurden zwei reisende Tatverdächtige mit Lebensmittelpunkt in Rumänien festgestellt.

Bei den reisenden Tatverdächtigen 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. Aus den Niederlanden stammende Tatverdächtige führen Sprengungen deutlich häufiger mit festen Explosivstoffen herbei als andere Tätergruppierungen.

Intensivierung der internationalen Zusammenarbeit

Da ein verstärkter Strafverfolgungsdruck durch die niederländischen Strafverfolgungsbehörden und vor allem verstärkte Präventionsmaßnahmen seitens niederländischer Finanzinstitute mitunter zu Verdrängungseffekten nach Deutschland geführt haben, wurde

die Zusammenarbeit von deutschen und niederländischen Strafverfolgungsbehörden im Phänomenbereich Geldautomatensprengung intensiviert. Um das Kriminalitätsgeschehens einzudämmen, finden regelmäßige Arbeitstreffen sowie koordinierte, gemeinsame Einsatzmaßnahmen – auch unter Einbeziehung europäischer Partner – statt. Gleichzeitig gibt es auf Bundes- und Landesebene verschiedene Initiativen, die gemeinsam mit den Geldautomatenbetreibern auf verstärkte Präventionsmaßnahmen in Deutschland hinwirken.

Deutsch-niederländischer Ermittlungserfolg

Im September 2021 gelang deutschen und niederländischen Strafverfolgungsbehörden mit dem Vollzug von Europäischen Haftbefehlen gegen drei Tatverdächtige und der Durchsuchung von Wohnungen in den Niederlanden ein großer Ermittlungserfolg.

Den Tatverdächtigen wird u. a. zur Last gelegt, einen Geldautomaten in Schüttorf/NI zur Explosion gebracht zu haben. Durch die Explosion war in dem betroffenen Wohn- und Geschäftshaus ein Feuer ausgebrochen, die Bewohner mussten von der Feuerwehr gerettet werden.

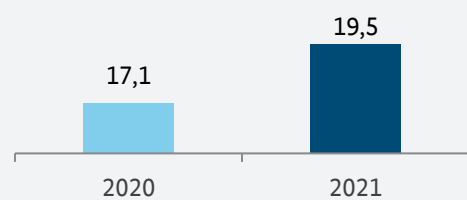
Im Laufe der Ermittlungen wurden Tatzusammenhänge zu sechs ähnlich gelagerten Fällen in weiteren vier Bundesländern festgestellt. Der ermittlungsführenden Dienststelle gelang es gemeinsam mit der niederländischen Polizei, einer Gruppierung aus Utrecht die Beteiligung an den Taten nachzuweisen.

Gemeinsame Ermittlungen führten zur Identifizierung weiterer Tatverdächtiger, zur Gewinnung von Strukturkenntnissen und zu der Feststellung, dass es im niederländischen Utrecht eine Art „Trainingszentrum“ für Geldautomatensprengungen gab, in dem ein Tatverdächtiger in Folge einer selbstverursachten Explosion zu Tode kam (vgl. Bundeslagebild 2020).

Schäden

Trotz des Rückgangs der Gesamtfallzahl stieg die in 2021 durch Sprengungen von Geldautomaten insgesamt erlangte Beutesumme im Vergleich zum Vorjahr um 14,0 % an. Diese Entwicklung ist insbesondere auf den Anstieg der Fälle zurückzuführen, bei denen die Täter nach erfolgreicher Sprengung des Geldautomaten an Bargeld gelangten (+11,3 %).

Beuteschäden (in Mio. Euro)⁴



Wie in den Vorjahren überstiegen die durch die Sprengungen von Geldautomaten verursachten Sachschäden die Beuteschäden in Teilen deutlich. Es muss auch für 2021 davon ausgegangen werden, dass durch die festgestellten Geldautomatensprengungen insgesamt Begleitschäden im mittleren zweistelligen Millionenbereich entstanden sind.

Filialschließung nach Geldautomatensprengung

Im Oktober 2021 wurde der Geldautomat im Selbstbedienungsbereich einer Bankfiliale im niedersächsischen Itterbeck, nahe der deutsch-niederländischen Grenze, mittels fester Explosivstoffe zur Explosion gebracht. Der Geldautomat war im Juli 2020 schon einmal gesprengt worden. Bei der neuerlichen Tat wurde das Gebäude der Bankfiliale schwer beschädigt und Trümmerteile verteilten sich über den Kundenparkplatz bis auf die angrenzende Hauptstraße. Schätzungen zufolge entstand ein Gebäudeschaden im sechststelligen Euro-Bereich. Im Dezember 2021 gab die betroffene Bank bekannt, die Filiale dauerhaft aufzugeben.



Bei der Sprengung eines Geldautomaten in einer Bankfiliale in Itterbeck entstand ein erheblicher Gebäudeschaden.

⁴ Die Angaben zur Gesamtsumme der Beuteschäden sind als Näherungswert zu betrachten, da nicht zu allen Sprengungen von Geldautomaten Angaben zur erlangten Beutesumme gemacht werden konnten.

2.2 TECHNISCHE MANIPULATIONEN VON GELDAUTOMATEN

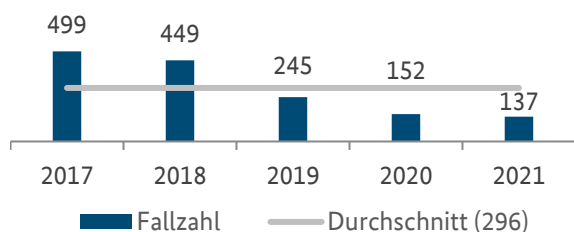
2.2.1 Skimming

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 stellen die nachfolgend dargestellten polizeilichen Erkenntnisse nur einen Näherungswert des tatsächlichen Kriminalitätsgeschehens dar.

Fallzahlen

Die Anzahl der Skimming-Angriffe⁶ war auch im Jahr 2021 rückläufig (-9,9 %) und erreichte einen neuerlichen Tiefstwert. Insgesamt waren 80 Geldautomaten (2020: 87; -8,0 %) betroffen. Verschiedene Geräte wurden mehrfach, im Höchstfall fünf Mal, angegriffen.

Skimming-Angriffe – Fallentwicklung



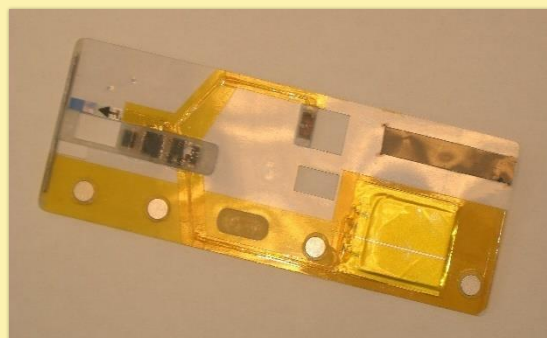
Die anhaltend rückläufigen Fallzahlen deuten darauf hin, dass die in den letzten Jahren eingeführten Sicherheitsmaßnahmen, insbesondere die Umstellung auf Zahlungskarten mit dem EMV⁷-Chip, nachhaltige Wirkung entfalten. Zudem dürfte die Ausstattung der Geldautomaten mit wirksamen Anti-Skimming-Modulen, die ein Auslesen von Kartendaten (Magnetstreifendaten) erschweren, zu der Entwicklung beigetragen haben.

Dennoch bleibt festzuhalten, dass die Täter weiterhin verbesserte Skimming-Geräte einsetzen und sich dabei auch technisch den neuen Sicherheitsvorkehrungen anpassen. So wurden zum Beispiel schmalere Kartenschlitze als physische Sicherheitsvorkehrungen an Geldautomaten durch schmalere Skimmer umgangen.

Modus Operandi



Beim sog. Skimming greifen die Täter durch den Einsatz technisch manipulierter Lesegeräte (sog. Skimmer) die Magnetstreifendaten von Zahlungskarten ab. Mithilfe versteckter Mini-Kameras oder unmittelbar auf der Originaltastatur (PIN-Pad) angebrachter Tastaturattrappen wird zudem die eingegebene PIN ausgespäht. Mit den abgegriffenen Kartendaten erstellen die Täter mithilfe von „White Plastics“⁵ eine Kopie der Zahlungskarte (sog. Kartendublette). Anschließend nehmen die Täter mit dieser Kartendublette und der ausgespähten Geheimzahl (PIN) unberechtigte Bargeldabhebungen an Geldautomaten vor.



Sehr flacher, in Frankreich sichergestellter Deep-Insert-Skimmer, der auch in Deutschland zum Einsatz kommt.

⁵ „White Plastics“ sind die Kartenrohlinge, auf welche die durch die Täter erlangten Kartendaten übertragen werden.

⁶ Ein Angriff bezeichnet jeden (Einzel-)Fall, in dem Täter Skimming-Equipment an einem Geldautomaten installieren.

⁷ EMV: Europay International, Mastercard und Visa. Durch den EMV-Chip lassen sich Kartendaten schwerer auslesen als bei Zahlungskarten, die lediglich über einen Magnetstreifen verfügen.

Skimming-Angriffe ausschließlich an Geldautomaten eines einzigen Finanzinstituts

Im Jahr 2021 fanden alle polizeilich bekannt gewordenen Skimming-Angriffe an Geldautomaten nur eines einzigen Finanzinstituts statt, welches ein Zahlungskartenprodukt ohne EMV-Chip anbietet. Die Täter fokussierten sich offenbar auf Geldautomaten dieses Finanzinstituts, 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. Daneben gelangen die Täter an diesen Geldautomaten ebenfalls an die Magnetstreifendaten von Zahlungskarten mit EMV-Chip. Die Magnetstreifendaten dieser EMV-Chip-Zahlungskarten werden nach wie vor auf Dubletten im außereuropäischen Ausland missbräuchlich verwendet, da dort teilweise noch auf Magnetstreifenbasis funktionierende Dubletten eingesetzt werden können.

Die Manipulationen der Geldautomaten erfolgten im Jahr 2021 in zehn Ländern. Die meisten Skimming-Angriffe wurden in Baden-Württemberg, Bayern und Hamburg verübt. In allen drei Ländern, wie auch im Saarland, stieg die Fallzahl deutlich an.⁸ Hingegen brach das Fallaufkommen in Nordrhein-Westfalen in 2021 nahezu vollständig ein (2020: 44).

In Berlin, welches bis 2019 stets das Bundesland mit den höchsten Fallzahlen war, wurden erstmalig keine Angriffe verzeichnet. Hierbei könnte u. a. eine Rolle spielen, dass Täter in der Vergangenheit insbesondere Geldautomaten an Orten angegriffen haben, an denen sie mit einer hohen Anzahl an ausländischen, insbesondere außereuropäischen Touristen rechnen konnten, deren Zahlungskarten teilweise nicht mit dem EMV-Chip ausgestattet waren. Mit den Auswirkungen der COVID-19-Pandemie auf den internationalen

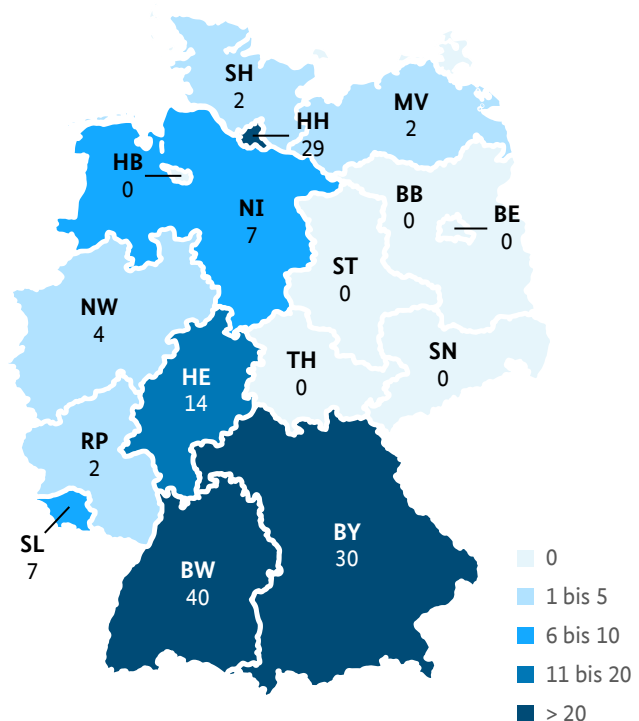
Tourismus (insbesondere in Form von zeitweiligen Reisebeschränkungen) hatten sich die Rahmenbedingungen in den Jahren 2020 und 2021 geändert.

Überwiegend rumänische und bulgarische Tatverdächtige

Schäden

Nach Angaben der Euro Kartensysteme GmbH (EKS) fiel der Schaden aus Skimming-Fällen zum Nachteil deutscher Kreditinstitute im Jahr 2021 deutlich geringer als im Vorjahr aus (-46,2 %). Die

Skimming-Angriffe – Verteilung nach Ländern

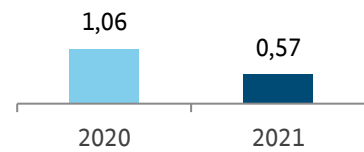


Im Deliktsbereich Skimming werden seit Jahren vorrangig rumänische und bulgarische Tatverdächtige polizeilich bekannt.

⁸ In 2020 wurden in Baden-Württemberg vier Fälle verzeichnet, in Bayern zwölf, in Hamburg fünf und im Saarland kein Fall.

Schadenssumme bezieht sich allein auf die betroffenen EMV-Chip-Zahlungskarten (meistens girocards), deren Magnetstreifendaten auf Dubletten im außereuropäischen Ausland missbräuchlich verwendet wurden. Zu den Schadenszahlen des Kartenprodukts des besonders betroffenen Finanzinstituts liegen keine Erkenntnisse vor.

Beuteschäden (in Mio. Euro)⁹



Im Vergleich zum historischen Höchststand von Skimming-Attacken im Jahr 2010 und dem durch diese Angriffe verursachten Gesamtschaden (rd. 55 Mio. Euro bei 3.183 Skimming-Angriffen) ist das Schadensniveau im Berichtsjahr gering. Auch in Bezug auf die Schadenssumme von rd. 18,2 Mio. Euro im Bereich der verlorenen und gestohlenen Zahlungskarten fällt die Schadenssumme bei gefälschten Zahlungskarten vergleichsweise niedrig aus.

Verwertungstaten im Ausland¹⁰

Im SEPA¹¹-Raum werden Geldautomatentransaktionen bei mit EMV-Chip ausgestatteten Zahlungskarten 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“ eingesetzt werden können. So wurden gefälschte Zahlungskarten mit deutschen Kartendaten in 2021 vor allem in den USA (46 %), Brasilien (41 %) und Indien (6 %) eingesetzt.

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:

Modi Operandi

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 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.



⁹ Die Summe der Beuteschäden für 2020 stimmt aufgrund einer nachträglich notwendig gewordenen Anpassung nicht mit den im Bundeslagebild 2020 ausgewiesenen Beuteschäden (1,05 Mio. Euro) überein.

¹⁰ Basierend auf Erkenntnissen der EURO Kartensysteme GmbH (EKS).

¹¹ Single Euro Payments Area.

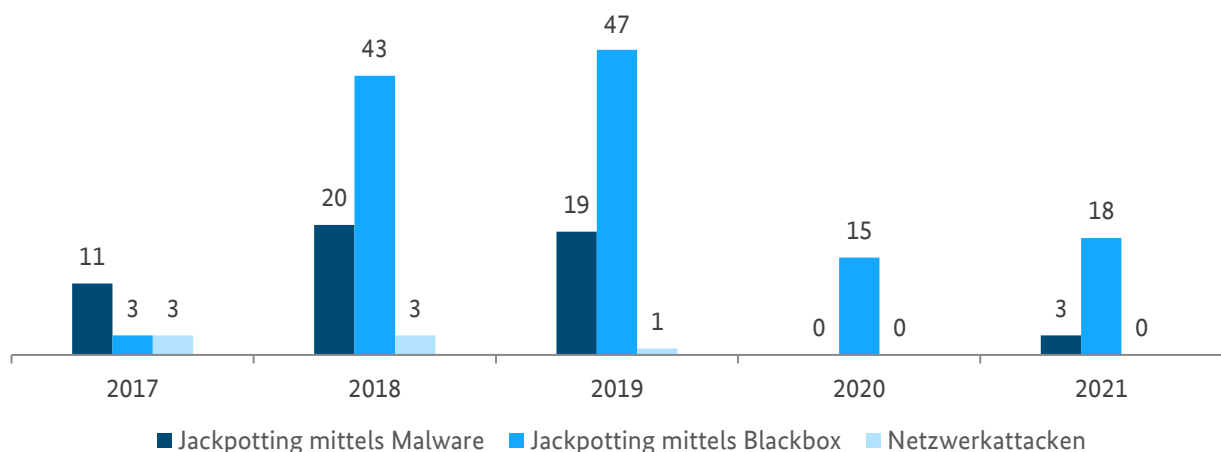
Netzwerkattacken

Bei Netzwerkattacken werden entweder die Geldautomaten-Netzwerke von Zahlungskarten-instituten oder Netzwerke von kartenausgebenden Banken bzw. deren Processinggesellschaften mit dem Ziel infiltriert, dort Schadsoftware zu installieren. Mithilfe dieser 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).

Fallzahlen

Im Jahr 2021 kam es zu einem leichten Anstieg der Fallzahlen beim Jackpotting mittels Malware und mittels Blackbox. Netzwerkattacken wurden nicht registriert.

Logische Angriffe auf Geldautomaten – Fallentwicklung¹²



Die Jackpotting-Angriffe mittels Blackbox erfolgten 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 bei zwei der 18 Jackpotting-Angriffe mittels Blackbox gelangten die Täter an Bargeld (Versuchsanteil: 88,9 %; 2020: 73,3 %). Die Jackpotting-Angriffe mit Malware verliefen ohne Erfolg.

Die Tatverdächtigen im Bereich Jackpotting stammen fast ausschließlich aus dem Ausland und reisen lediglich zur Tatbegehung nach Deutschland ein. Es kann daher nicht ausgeschlossen werden, dass die verhältnismäßig niedrigen Fallzahlen in 2020 und 2021 auch im Zusammenhang mit den Auswirkungen der COVID-19-Pandemie (z. B. zeitweilige Reisebeschränkungen, regionale Ausgangssperren) stehen.

Schäden

Bei den zwei erfolgreichen Jackpotting-Angriffen mittels Blackbox entstand ein Schaden von insgesamt rd. 88.500 Euro (2020: rd. 420.000 Euro bei vier erfolgreichen Angriffen, -78,9 %).

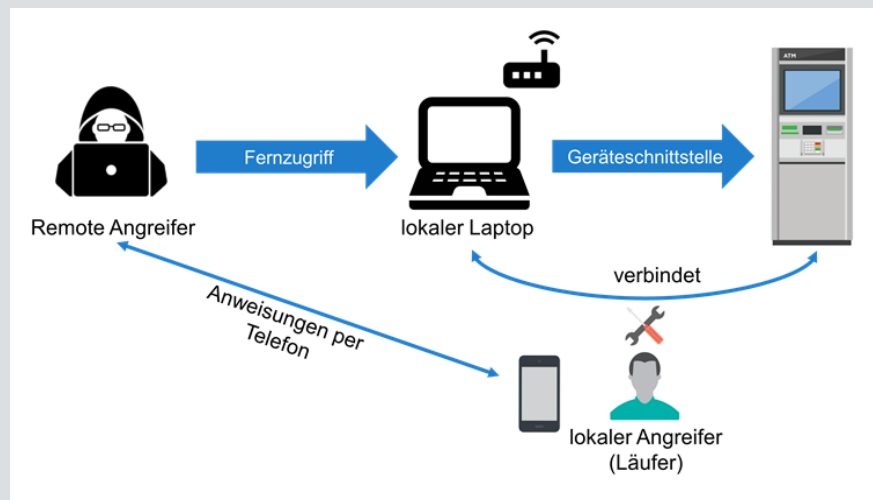
¹² Die Fallzahl für Jackpotting mittels Malware wurde für das Jahr 2019 nachträglich angepasst und stimmt somit nicht mit der Fallzahl im Bundeslagebild 2019 überein.

Europaweite Tatserie logischer Systemangriffe

Bei einer europaweiten Serie von Jackpotting-Angriffen mittels Blackbox griffen Täter in 2021 gezielt bestimmte Geldautomatentypen an, in denen das gleiche Auszahlungsmodul verbaut ist. Der erste Angriff der rund 70 Fälle umfassenden Tatserie fand am 14. Mai 2021 in Nordrhein-Westfalen statt. Insgesamt wurden 18 Angriffe in Deutschland verübt. Zwei dieser Taten waren erfolgreich. Die Täter erbeuteten hierbei rd. 30.000 Euro bzw. 58.000 Euro. Die hohe Anzahl der gescheiterten Angriffe ist mit großer Wahrscheinlichkeit auf das frühzeitige Erkennen der Serie und die Bereitstellung eines Sicherheitsupdates des betroffenen Automatenherstellers zurückzuführen.

Die Täter, welche überwiegend aus dem osteuropäischen Raum stammen, führten die Angriffe per Fernsteuerung (Remote) durch.

Zum Beispiel griffen zwei Täter am 19. Mai 2021 einen Geldautomaten in Baden-Württemberg an. Das Gehäuse des Geldautoma-



ten wurde gewaltsam geöffnet und ein tätereigener Laptop, die sogenannte Blackbox, an das Auszahlungsmodul des Geldautomaten mit der Absicht angeschlossen, unautorisierte Bargeldausgaben durchzuführen. Der Angriff verlief erfolglos. Die Täter wurden in der darauffolgenden Nacht nur rund 25 km vom Tatort entfernt bei der Begehung einer weiteren Tat festgenommen. Eine Auswertung der im Rahmen der Festnahme sichergestellten Blackbox ergab Verbindungen zu Fällen in verschiedenen anderen europäischen Staaten.

3 Gesamtbewertung

Trotz eines leichten Rückgangs besonders schwerer Fälle des Diebstahls durch Sprengung von Geldautomaten ist die Bedrohungslage in Deutschland anhaltend hoch. Dies zeigt sich auch daran, dass der festgestellte Beuteschaden im Vergleich zum Vorjahr zunahm und in 2021 ein neuer Höchststand vollendeter Taten erreicht wurde. Letzteres könnte darauf hindeuten, dass die Präventionsmaßnahmen der Geldinstitute und der Geldautomatenhersteller in ihrer bisherigen Form nicht ausreichen.

Der Trend zur vermehrten Verwendung fester Explosivstoffe zur Sprengung von Geldautomaten setzte sich in 2021 fort. Der Einsatz dieser Stoffe birgt ein erhöhtes Risiko für Unbeteiligte, da die Täter häufig nicht in der Lage sind, die verwendeten Stoffe vollständig zu kontrollieren.

Kennzeichnend für den Phänomenbereich Sprengung von Geldautomaten ist weiterhin eine bundesweite Betroffenheit, wobei der Schwerpunkt – mit Ausnahme Berlins – im Westen Deutschlands lag. Wie in den Vorjahren kann eine Wechselwirkung in Form von Verdrängungseffekten aufgrund verstärkter Präventionsmaßnahmen in den Niederlanden, aber auch durch Maßnahmen zur Eindämmung der COVID-19-Pandemie nicht ausgeschlossen werden.

Der Phänomenbereich Sprengung von Geldautomaten bildet in Deutschland bereits seit mehreren Jahren einen Schwerpunkt der polizeilichen Kriminalitätsbekämpfung. Vor dem Hintergrund der vielfach grenzüberschreitenden Tatbegehung kommt der Kooperation mit internationalen Partnern eine große Bedeutung zu. Angesichts der großen Zahl reisender Tatverdächtiger aus den Niederlanden ist die Zusammenarbeit mit den niederländischen Strafverfolgungsbehörden von besonderer Bedeutung. Diese Kooperation wurde in 2021 noch einmal deutlich intensiviert.

Im Phänomenbereich Skimming wurde ein neuerlicher Tiefstwert der Skimming-Angriffe sowie des damit verursachten Gesamtschadens erreicht. Die anhaltend rückläufigen Fallzahlen sind ein Indiz dafür, dass die von den Geldinstituten eingeführten Sicherheitsmaßnahmen nachhaltig greifen. Das Bedrohungspotenzial durch Skimming-Angriffe ist vergleichsweise gering.

Im Bereich der logischen Systemangriffe auf Geldautomaten bzw. Geldautomaten-Netzwerke stieg die Fallzahl in 2021 – bei nach wie vor geringen absoluten Zahlen – leicht an. Dies ist insbesondere auf eine europaweite Serie von Jackpotting-Angriffen mittels Blackbox zurückzuführen. Trotz der im Berichtsjahr gesunkenen Schadenssumme bleibt die Entwicklung aufgrund der für die Täterseite weiterhin bestehenden Aussicht auf mitunter hohe kriminelle Erträge im Blick der Strafverfolgungsbehörden.

Inwieweit die seit 2020 vergleichsweise niedrigen Fallzahlen in den Bereichen Skimming und logische Systemangriffe auch auf Auswirkungen der COVID-19-Pandemie, insbesondere zeitweiliger Reise- und Ausgangsbeschränkungen, zurückzuführen sein könnten, kann noch nicht abschließend beurteilt werden.

Impressum

Herausgeber

Bundeskriminalamt, 65173 Wiesbaden

Stand

Juni 2022

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.

Nachdruck und sonstige Vervielfältigung, auch auszugsweise,
nur mit Quellenangabe des Bundeskriminalamtes
(Angriffe auf Geldautomaten, Bundeslagebild 2022, Seite X).