Bundeskriminalamt

BKA

Wirtschaftskriminalität

Bundeslagebild 2017

Wirtschaftskriminalität 2017 in Zahlen

ALLGEMEINER ÜBERBLICK

74.070 ↑
Fälle (+28,7 %)

3.738 ↑
Mio. Euro Schaden (+25,9 %)

26.010 ↘
Tatverdächtige (-5,8 %)

94,6 % →
Aufklärungsquote (+0,6 %)

BEDEUTENDE ENTWICKLUNGEN

Virtuelle Währungen
- Initial Coin Offerings (IOCs) als Möglichkeit für Anlagebetrug
- Hochspekulativ mit Risiko für finanziellen Totalausfall

Binäre Optionen
- Investition in Fake-Angebote (z. B. Aktien, Indizes)
- Nutzung von Call-Centern

Social Bots
- Marktmanipulation von Aktienwerten
- Hohes Schadenspotenzial

CEO-Fraud
- Hohes Schadenspotenzial
- Imageschäden für betroffene Firmen

Inhaltsverzeichnis

1 Vorbemerkung

Das Bundeslagebild Wirtschaftskriminalität enthält in gestraffter Form die aktuellen Erkenntnisse zur Lage und Entwicklung im Bereich der Wirtschaftskriminalität. Grundlage für die Erstellung des Lagebilds sind die Daten aus der Polizeilichen Kriminalstatistik (PKS). Bei der PKS-Erfassung besteht die Möglichkeit der Mehrfachzuweisung einer Straftat. Daher können sich einzelne umfangreiche Ermittlungskomplexe mit einer Vielzahl einzelner Straftaten statistisch gleichzeitig auf verschiedene Einzelphänomene auswirken (z. B. auf Fallzahlen, Schäden, Tatverdächtige etc.).

Die polizeilichen Daten können das tatsächliche Ausmaß der Wirtschaftskriminalität nur eingeschränkt wiedergeben. Einerseits werden Wirtschaftsstraftaten, die von Staatsanwaltschaften und/oder von Finanzbehörden unmittelbar und ohne Beteiligung der Polizei bearbeitet werden (z. B. Wettbewerbsdelikte [insbesondere der Produkt- und Markenpiraterie], Gesundheitsdelikte, Arbeitsdelikte und Subventionsbetrug), nicht in den polizeilichen Statistiken erfasst. Änderungen der Rechtsgrundlagen zur Bekämpfung illegaler Ausländerbeschäftigung und illegaler Arbeitnehmerüberlassung haben zu einer Aufgabenzuweisung an die Zollverwaltung (Dienststellen der Finanzkontrolle Schwarzarbeit [FKS]) geführt. Die Arbeitsdelikte sind zwar noch Bestandteil des Bundeslagebilds Wirtschaftskriminalität, werden vor dem genannten Hintergrund allerdings keiner näheren Betrachtung mehr unterzogen.

Zum anderen ist im Hinblick auf die Interessenslage der Opfer von einem in Teilbereichen gering ausgeprägten Anzeigeverhalten und damit verbunden von einem großen Dunkelfeld auszugehen. Überdies lassen sich auf Grundlage der in der PKS erfassten polizeilichen Daten keine Aussagen zur Qualität von Ermittlungsverfahren treffen, da einzelne Aspekte, wie zum Beispiel eine lange Verfahrensdauer, in der statistischen Erfassung keine Berücksichtigung finden und jede Straftat gleich gewichtet wird.

Die Polizei orientiert sich bei der Zuordnung von Straftaten zur Wirtschaftskriminalität am Katalog des § 74 c Abs. 1 Nr. 1 bis 6 b Gerichtsverfassungsgesetz (GVG), der die Zuständigkeit der landgerichtlichen Wirtschaftsstrafkammern regelt. Eine Legaldefinition des Begriffs der Wirtschaftskriminalität besteht in Deutschland nicht. Nach kriminologischer Definition handelt es sich bei Wirtschaftskriminalität um die vertrauensmissbrauchende Begehung von Straftaten im Rahmen einer tatsächlichen oder vorgetäuschten wirtschaftlichen Betätigung, die unter Gewinnstreben die Abläufe des Wirtschaftslebens ausnutzt und zu einer Vermögensgefährdung oder einem Vermögensverlust großen Ausmaßes führt oder eine Vielzahl von Personen oder die Allgemeinheit schädigt.

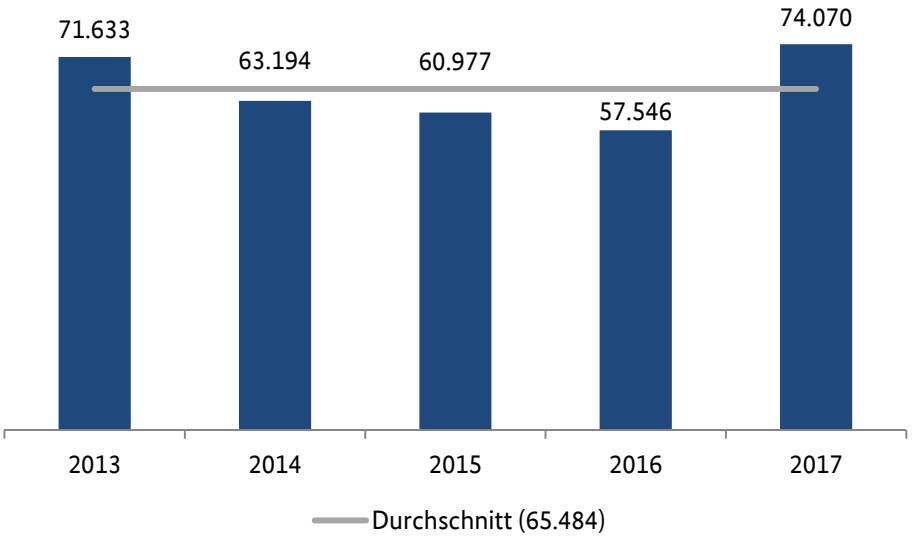
2 Darstellung und Bewertung der Kriminalitätslage

2.1 WIRTSCHAFTSKRIMINALITÄT[1] ALLGEMEIN

Starker Fallanstieg bei Wirtschaftskriminalität

Im Jahr 2017 wurden in der PKS insgesamt 74.070 Fälle der Wirtschaftskriminalität registriert, das entsprach einem Anstieg um 28,7 % im Vergleich zum Vorjahr (57.546 Fälle). Die Fallzahl lag deutlich über dem Durchschnitt der letzten fünf Jahre (65.484 Fälle). Der Anteil der Wirtschaftskriminalität an allen polizeilich bekannt gewordenen Straftaten betrug 1,3 % (2016: 0,9 %).

Fallentwicklung Wirtschaftskriminalität[2]



Einhergehend mit der Gesamtentwicklung sind die Fallzahlen in einigen Teilbereichen der Wirtschaftskriminalität beträchtlich angestiegen. Besonders hervorzuheben sind die Bereiche Betrug/Untreue i. Z. m. Kapitalanlagen (+252,7 %), Anlage- und Finanzierungsdelikte (+229,9 %), Abrechnungsbetrug im Gesundheitswesen (+126,7 %) sowie Wirtschaftskriminalität bei Betrug (+65,0 %).

Diesen starken Fallanstiegen standen leicht rückläufige Tendenzen bei den Wettbewerbsdelikten (-7,1 %), den Insolvenzdelikten (-5,7 %) und den Arbeitsdelikten (-3,0 %) gegenüber.

Ein umfangreicher Verfahrenskomplex aus Sachsen[3], in welchem wenige Tatverdächtige zahlreiche Anlagebetrugsdelikte begangen haben, wirkt sich aufgrund der Vielzahl an aufgeklärten Fällen erheblich auf bestimmte Bereiche der nachfolgenden Statistik aus. Darauf dürfte u. a. der Anstieg der Fallzahlen bei gleichzeitigem Rückgang der Tatverdächtigen zurückzuführen sein.

[1] Betrachtet werden die PKS-Summenschlüssel 893000 und der PKS-Schlüssel 518110.
[2] Polizeiliche Kriminalstatistik.
[3] Nähere Erläuterungen dazu erfolgen im Kapitel 2.2.2.

Entwicklung in den einzelnen Bereichen der Wirtschaftskriminalität[4]

Deliktsbereich	Fallzahlen 2017 (2016)	Tendenz	Tatverdächtige 2017 (2016)	Tendenz	Schaden in Mio. Euro 2017 (2016)	Tendenz
Wirtschaftskriminalität gesamt	**74.070** (57.546)	↑	**26.010** (27.615)	↘	**3.738** (2.970)	↑
Wirtschaftskriminalität bei Betrug	**48.103** (29.160)	↑	**9.099** (9.824)	↘	**2.065** (772)	↑
Insolvenzdelikte	**10.640** (11.283)	↘	**9.490** (9.940)	↘	**1.157** (1.566)	↓
Anlage- und Finanzierungsdelikte	**28.255** (8.566)	↑	**1.391** (1.744)	↓	**1.558** (466)	↑
Wettbewerbsdelikte	**1.614** (1.737)	↘	**1.496** (1.579)	↘	**8** (7)	↑
Arbeitsdelikte	**7.467** (7.699)	↘	**4.215** (4.320)	↘	**45** (47)	↘
Betrug/Untreue i. Z. m. Kapitalanlagen	**27.564** (7.815)	↑	**778** (967)	↓	**1.617** (356)	↑
Abrechnungsbetrug im Gesundheitswesen	**5.588** (2.465)	↑	**1.455** (1.577)	↘	**120** (29)	↑

Anzahl der Tatverdächtigen gesunken

Die Anzahl der Tatverdächtigen bei Wirtschaftsstraftaten sank im Jahr 2017 um 5,8 % auf insgesamt 26.010 Personen (2016: 27.615). Somit setzte sich der bereits im Vorjahr verzeichnete rückläufige Trend auch im Berichtsjahr fort. Der Anteil nichtdeutscher Tatverdächtiger in diesem Kriminalitätsbereich betrug 23,1 % (2016: 21,1 %) und war damit niedriger als deren Anteil in Bezug auf alle in der PKS erfassten Straftaten (30,4 %)[5].

Gleichbleibend hohe Aufklärungsquote

Im Jahr 2017 betrug die Aufklärungsquote 94,6 % (2016: 94,0 %) und lag somit deutlich über der Gesamtaufklärungsquote aller in der PKS erfassten Straftaten (57,1 %). Ursächlich dafür ist der Umstand, dass es sich bei Straftaten der Wirtschaftskriminalität überwiegend um Anzeigedelikte handelt, bei denen die Täter den Geschädigten in vielen Fällen bekannt sind.

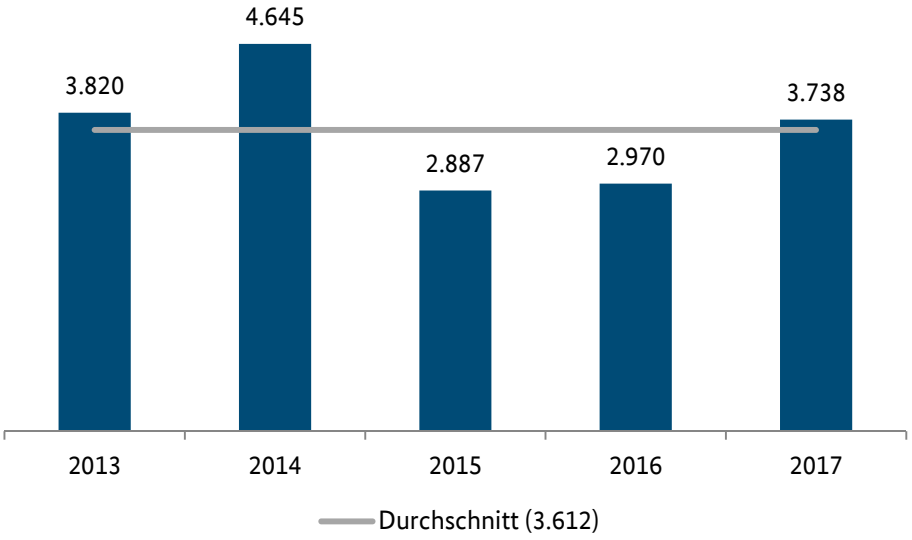
[4] Polizeiliche Kriminalstatistik.
[5] Beim Anteil der nichtdeutschen Tatverdächtigen an den Gesamtstraftaten in der PKS werden Tatverdächtige, die ausschließlich wegen ausländerrechtlicher Verstöße in Erscheinung getreten sind, nicht berücksichtigt.

Starker Schadensanstieg

Nachdem die Gesamtschadenssumme durch Wirtschaftskriminalität im Vorjahr nur gering angestiegen war, entstand im Jahr 2017 ein Schaden in Höhe von 3.738 Mio. Euro (2016: 2.970 Mio. Euro), was einem Anstieg um 25,9 % entspricht. Damit lag die Gesamtschadenssumme knapp über dem Durchschnitt der letzten fünf Jahre (3.612 Mio. Euro). In etwa 93 % der Fälle von Wirtschaftskriminalität konnte die Schadenssumme beziffert werden[6].

Die Schäden bei Wirtschaftskriminalitätsdelikten zeichneten im Jahr 2017 für einen Anteil von 50,5 % (2016: 43,1 %) am in der PKS ausgewiesenen Gesamtschaden (2017: 7.400 Mio. Euro) verantwortlich. Die Gesamtsumme der Schäden verdeutlicht einmal mehr die erheblichen Auswirkungen der Wirtschaftskriminalität.

Schadensentwicklung Wirtschaftskriminalität in Mio. Euro[7]



In nahezu allen Teilbereichen der Wirtschaftskriminalität sind die erfassten Schäden erheblich angestiegen. Dabei verursachte die Wirtschaftskriminalität bei Betrug mit 2.065 Mio. Euro die höchste Schadenssumme (2016: 772 Mio. Euro; +167,5 %). Ein ebenfalls hoher finanzieller Schaden in Höhe von 1.617 Mio. Euro entstand bei Betrug/Untreue i. Z. m. Kapitalanlagedelikten (2016: 356 Mio. Euro; +354,2 %), gefolgt von Anlage- und Finanzierungsdelikten mit 1.558 Mio. Euro Schaden (2016: 466 Mio. Euro; +234,3 %). Der Schaden beim Abrechnungsbetrug im Gesundheitswesen fiel mit 120 Mio. Euro (2016: 29 Mio. Euro) im Verhältnis zwar relativ gering aus, jedoch wurde in diesem Bereich mit 313,8 % ein hoher Anstieg verzeichnet.

Obwohl die Entwicklung bei den Insolvenzdelikten mit 1.157 Mio. Euro rückläufig war (2016: 1.566 Mio. Euro; -26,1 %), entstand auch in diesem Bereich ein Schaden in Milliardenhöhe. Gleichwohl wurde prozentual hier der stärkste Rückgang verzeichnet.

[6] Bei Fällen mit unbekannter Schadenshöhe wird ein symbolischer Schaden von einem Euro erfasst.
[7] Polizeiliche Kriminalstatistik.

Teilweise schwerwiegende immaterielle Schäden

Die in der PKS erfassten Schadenssummen können den durch die Wirtschaftskriminalität tatsächlich verursachten Gesamtschaden nur in Teilen abbilden. Neben den monetär darstellbaren Schäden müssen auch die durch das kriminelle Handeln verursachten immateriellen Schäden betrachtet werden. Diese sind nicht quantifizierbar, aber dennoch wesentliche Faktoren für die Bewertung des Schadenspotenzials der Wirtschaftskriminalität.

Beispiele sind etwa:

- Wettbewerbsverzerrungen durch Wettbewerbsvorsprünge des mit unlauteren Mitteln arbeitenden Wirtschaftsstraftäters,
- Gefahr, dass infolge finanzieller Abhängigkeiten und Verflechtungen bei einem wirtschaftlichen Zusammenbruch auch jene Geschäftspartner betroffen sein können, die an den kriminellen Handlungen der Täter nicht beteiligt waren,
- Reputationsverluste von einzelnen Unternehmen oder auch ganzen Wirtschaftszweigen,
- mögliche Vertrauensverluste in die Funktionsfähigkeit der bestehenden Wirtschaftsordnung.

Nutzung des Internets als Tatmittel nahezu halbiert

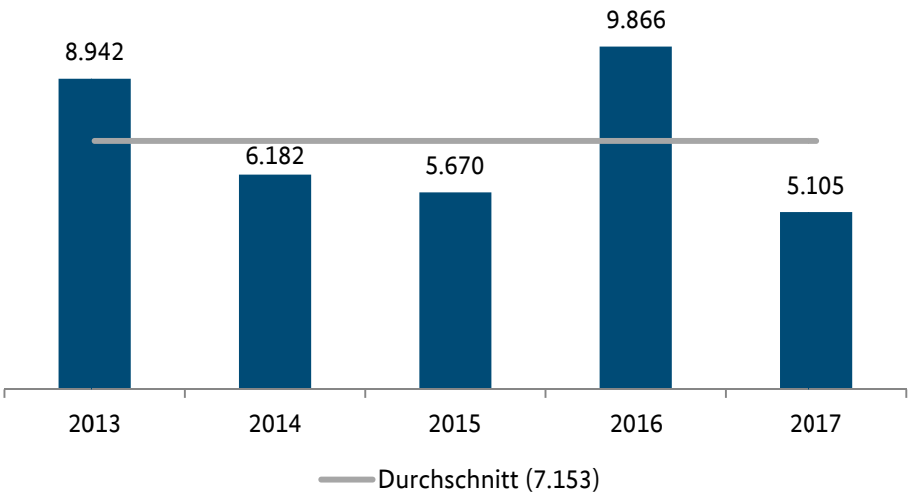
In 5.105 Fällen wurde im Jahr 2017 das Internet genutzt, um Wirtschaftsstraftaten zu begehen (6,9 % aller Fälle von Wirtschaftskriminalität). Im Vergleich zum Vorjahr ist die Anzahl der Wirtschaftsdelikte unter Nutzung dieses Tatmittels somit um fast die Hälfte zurückgegangen (2016: 9.866 Fälle; -48,3 %) und lag deutlich unter dem Durchschnitt der letzten fünf Jahre (7.153 Fälle). Der Hauptanteil entfiel wie bereits in den Vorjahren mit 3.912 Fällen (2016: 8.425 Fälle) auf den Bereich der Wirtschaftskriminalität bei Betrug.

Seit 2013 hat sich die Anzahl der Fälle, in denen das Internet für die Begehung von Wirtschaftsdelikten genutzt wurde, kontinuierlich verringert. Lediglich im Jahr 2016 hatte sich die Fallzahl etwa verdoppelt.

Die rückläufige Entwicklung im Berichtsjahr lässt sich wie folgt erklären: Im Jahr 2016 flossen umfangreiche Verfahren unter Nutzung des Internets als Tatmittel in die PKS ein.[8] Da diese Verfahren im Jahr 2016 abgeschlossen wurden, fanden sie folglich auch keinen Eingang mehr in die statistische Erfassung im Jahr 2017.

[8] Zu diesen Verfahren gehörten u. a. ein Umfangsverfahren aus Niedersachsen aus dem Deliktsbereich des Leistungsbetrugs, dem mehr als 3.400 Einzelfälle zugeordnet werden konnten, 736 Fälle des Waren- und Warenkreditbetrugs in Hessen sowie ein umfangreiches Ermittlungsverfahren des Anlagebetrugs in Baden-Württemberg, in welchem 510 Fälle zusammengeführt wurden.

Fallentwicklung Wirtschaftskriminalität mit Tatmittel Internet[9]



Social Bots

Social Bots sind geeignet, das Kunden- und Kaufverhalten über das sog. „Influencer Marketing" zu manipulieren. Beim Influencer Marketing handelt es sich um gezielte Marketingmaßnahmen kommerzieller Agenturen, um Nutzer in ihren Kaufentscheidungen zu beeinflussen und für ein Produkt oder eine Marke einzunehmen. Der Einsatz Sozialer Medien in Form von Kommentaren, sog. „Postings", „Likes" und „Shares" ist dabei essenziell.

Social Bots

Social Bots sind Computerprogramme, die eine menschliche Identität vortäuschen und zu manipulativen Zwecken eingesetzt werden, indem sie wie Menschen im Internet kommunizieren. Die Adressaten nehmen diese nicht als durch Algorithmen ausgelöste automatische Kommunikation, sondern als scheinbar real existierende Internet-User wahr. Die Adressaten sind sich daher der Manipulation nicht bewusst. Einfache Social Bots erkennen Schlüsselbegriffe und reagieren darauf. Komplexe Social Bots hingegen können Kommunikationsinhalte analysieren und Dialoge führen.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat mehrfach vor Marktmanipulationen mittels gefälschter oder unrichtiger Mitteilungen und Veröffentlichungen gewarnt. Social Bots könnten geeignet sein, derartige Falschmeldungen zu verbreiten und Manipulationen Vorschub zu leisten. Eine Störung der Finanzmärkte hätte vielfältige Auswirkungen auf unterschiedliche Bereiche der Wirtschaft, und das Vertrauen in die Integrität der Finanzmärkte wäre nachhaltig gestört.

[9] Polizeiliche Kriminalstatistik.

Die drei nachfolgenden Szenarien, denen eine Auswertung von Strafanzeigen der BaFin wegen Verstößen gegen das Wertpapierhandelsgesetz (WpHG) zugrunde liegt, sind für den Einsatz von Social Bots im Wirtschaftsleben denkbar:

1. Um Unternehmen in Misskredit zu bringen und ihren Aktienwert entsprechend sinken zu lassen, werden durch Social Bots gezielt Falschmeldungen verbreitet, auf Basis derer potenzielle Anleger ihre Investmententscheidungen treffen. Die Täter generieren ihre Einnahmen zum Beispiel dadurch, indem sie Optionen auf den Verlauf des Börsenkurses abschließen, welcher vorher durch den Einsatz von Social Bots in die gewünschte Richtung bewegt wurde.

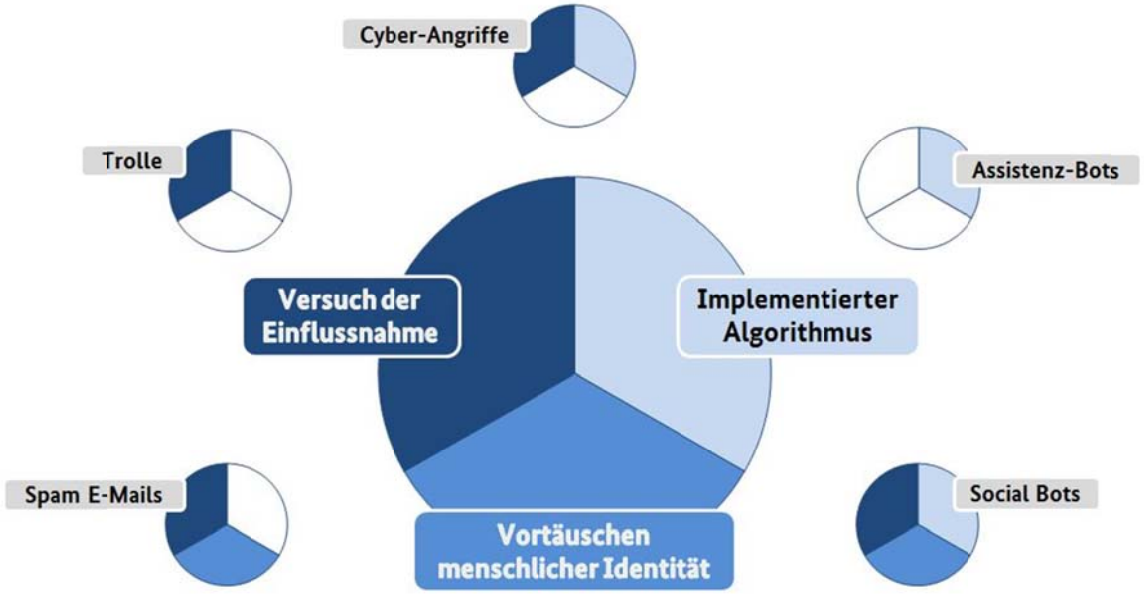
2. Künstliche, nichtexistente Märkte werden geschaffen, die dazu verleiten sollen, in nichtexistente Produkte zu investieren. Social Bots verbreiten Unmengen an Informationen im Internet, um interessierte Anleger von einem vermeintlich lukrativen Geschäft zu überzeugen. Diese Aktivitäten könnten für kriminelle Zwecke genutzt werden, indem Täter ein passendes Finanzprodukt schaffen, in welches die Anleger anschließend investieren.

3. Social Bots infiltrieren klassische Vertriebs- und Beratungsmodelle für Investments mit Falschnachrichten. Eine derartige Informationsverbreitung in Sozialen Netzwerken kann den Börsen- bzw. Marktpreis eines Finanzinstruments massiv beeinflussen, da potenziellen Anlegern ein reges Interesse des Kapitalmarkts am Finanzprodukt vorgetäuscht wird.

Derzeit führt die Hochschule Mittweida (Hochschule für angewandte Wissenschaften) in Zusammenarbeit mit der BaFin und dem BKA eine Vorstudie zur „Marktmanipulation mittels Social Bots“ durch. Es wird die Hypothese vertreten, dass hybride Bot-Netze bei der informationsgestützten Marktmanipulation von Aktienwerten in entsprechenden Foren eingesetzt werden können. Bei hybriden Bots handelt es sich um hochentwickelte Computerprogramme, die mit menschlichen Forennutzern eine starke Interaktion eingehen können.

Die nachfolgende Grafik verdeutlicht, wie sich Social Bots von anderen Internetphänomenen abgrenzen. Zudem ist erkennbar, dass Social Bots Charakteristiken anderer Phänomene in sich vereinigen. So unterscheiden sie sich auf technischer Ebene nicht grundlegend von Assistenz-Bots, die dem Anwender die Nutzung eines technischen Endgeräts erleichtern können (z. B. Siri), verfolgen dabei allerdings eine andere Zielsetzung. Da Social Bots für manipulative Zwecke eingesetzt werden können, kommen in ihnen auch die Eigenschaften von sog. „Trollen“ zum Tragen. Dabei handelt es sich um reale Personen, die vorrangig Diskussionen in Internetforen bewusst emotional aufladen, um sie in eine bestimmte Richtung zu lenken.

Abgrenzung von Social Bots zu anderen Internetphänomenen[10] [11]



2.2 DETAILBETRACHTUNGEN EINZELNER PHÄNOMENE

2.2.1 Betrug als Wirtschaftskriminalität[12]

Betrugsdelikte werden nicht per se der Wirtschaftskriminalität zugerechnet, sondern können bei massenhaft begangenen Betrugsstraftaten und bei festgestellten Tat- und Täterzusammenhängen hinzugezählt werden. Bei derartigen Konstellationen kann es sich auch um Fälle der Organisierten Kriminalität i. Z. m. dem Wirtschaftsleben handeln.

Organisierte Kriminalität

Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder

c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.

[10] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. Social Bots, 2017.
[11] Der große Kreis fungiert als Legende und benennt bestimmte Charakteristiken, die sich in den speziellen Internetphänomenen (kleine Kreise) widerspiegeln.
[12] Der PKS-Summenschlüssel 893100 setzt sich aus den PKS-Schlüsseln 511000, 513000, 514000, 516000 und 517000 zusammen.

Kriminalität i. Z. m. dem Wirtschaftsleben stellt seit Jahren einen relevanten Bereich der Organisierten Kriminalität in Deutschland dar. Dies zeigt sich anhand der Anzahl der jährlich geführten OK-Verfahren in diesem Bereich.

Im Jahr 2017 wurden 63 OK-Verfahren i. Z. m. dem Wirtschaftsleben (2016: 53 OK-Verfahren) geführt. Lediglich im Bereich der Rauschgift- und Eigentumsdelikte wurde im Berichtsjahr in mehr OK-Verfahren ermittelt. Gegenstand in über der Hälfte aller OK-Wirtschaftsverfahren waren Betrugsdelikte. Bei OK-Verfahren i. Z. m. dem Wirtschaftsleben ist regelmäßig ein hoher finanzieller Schaden festzustellen.

CEO-Fraud

Ein Beispiel für organisiert begangenen Betrug ist der sog. „CEO-Fraud“. Hierbei geben sich Täter u. a. als Geschäftsführer (engl. Chief Executive Officer [CEO]) eines Unternehmens aus und veranlassen einen Mitarbeiter des Unternehmens zum Transfer eines größeren Geldbetrags ins Ausland. Dabei werden häufig missbräuchlich erlangte personen- und unternehmensspezifische Daten zur Begehung der Betrugsstraftaten genutzt (sog. „Social Engineering“).

Social Engineering

Beim Social Engineering (Social Hacking) handelt es sich um eine Methode, um unberechtigten Zugang zu Informationen durch „Aushorchen“ zu erlangen. Dazu spionieren die Täter das persönliche Umfeld aus und nutzen dieses Wissen über das Opfer, um dessen Vertrauen zu gewinnen. Dabei werden die „Schwachstelle Mensch“ und menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität gezielt ausgenutzt. Die Opfer handeln meist aus Unwissenheit, aus einer Stresssituation heraus oder aus Höflichkeit und werden so zu einem Werkzeug des Angreifers. Ein typischer Angriff ist das Manipulieren von Mitarbeitern per Telefonanruf.

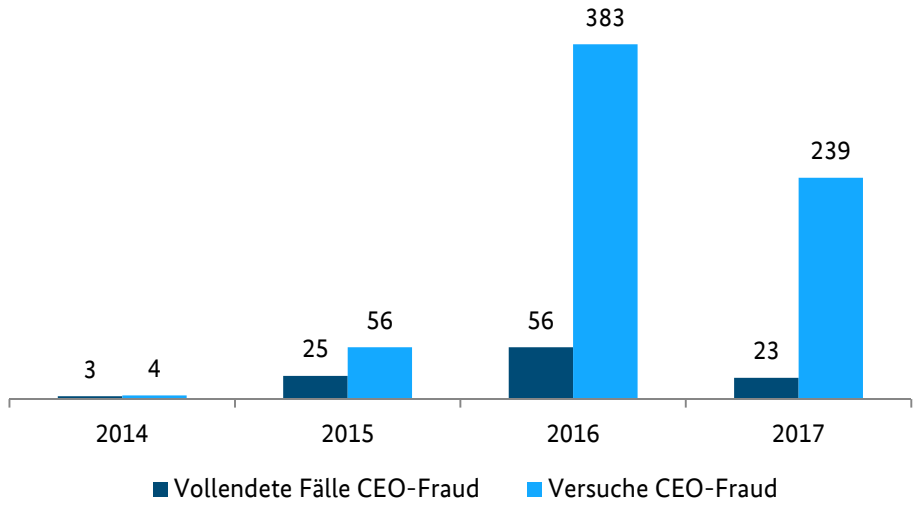
Um glaubwürdig aufzutreten, nutzen die Täter hierfür Informationen, welche die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Homepage oder in Werbebroschüren veröffentlichen. Die Täter legen ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments. Für die Täter sind beispielsweise E-Mail-Adressen von Interesse, da sie daraus die Systematik von Erreichbarkeiten herleiten können. Soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, stellen ebenfalls eine wichtige Informationsquelle dar. Auf diese Weise verschaffen sich die Täter die für den Betrug notwendigen internen Kenntnisse über das betreffende Unternehmen.

Die Täter nehmen mit dem „ausgeforschten“ Mitarbeiter Kontakt auf und geben sich als leitende Angestellte, Geschäftsführer oder Handelspartner aus. Dabei fordern sie, z. B. unter Hinweis auf eine angebliche Unternehmensübernahme oder angeblich geänderte Kontoverbindungen, den Transfer eines größeren Geldbetrages vorwiegend auf Konten in China (insb. Hongkong) oder osteuropäischen Staaten. Die Kontaktaufnahme erfolgt in der Regel per E-Mail oder Telefon, wobei E-Mail-Adressen verfälscht und Telefonnummern verschleiert werden.

Da im Jahr 2016 vermehrt Fälle des CEO-Fraud zum Nachteil deutscher Unternehmen verzeichnet wurden, haben sich die Polizeibehörden der Problematik verstärkt angenommen und umfangreiche Auswertungen, Ermittlungen und Präventionsmaßnahmen durchgeführt. In diesem Zusammenhang traten häufig israelische bzw. aus Israel heraus agierende Tätergruppierungen in Erscheinung. Aus diesem Grund hat das BKA diesbezüglich eine Sondererhebung mit diesem Schwerpunkt durchgeführt. Die nachfolgenden Fallzahlen geben somit ausschließlich die Ergebnisse dieser Sonderauswertung wider. Da vergleichbare Taten und Modi Operandi aber auch von polnischen und nigerianischen Tätergruppierungen begangen bzw. angewendet werden, ist von einem nicht unerheblichen Dunkelfeld beim CEO-Fraud auszugehen.

Seit dem Jahr 2014 hat das Phänomen CEO-Fraud zum Nachteil deutscher Unternehmen kontinuierlich an Bedeutung gewonnen. Gleichwohl hat sich die Zahl der vollendeten CEO-Fraud-Fälle im Jahr 2017 im Vergleich zum Vorjahr mehr als halbiert und sank auf 23 Fälle (2016: 56 vollendet Fälle).

Fallentwicklung CEO-Fraud[13]

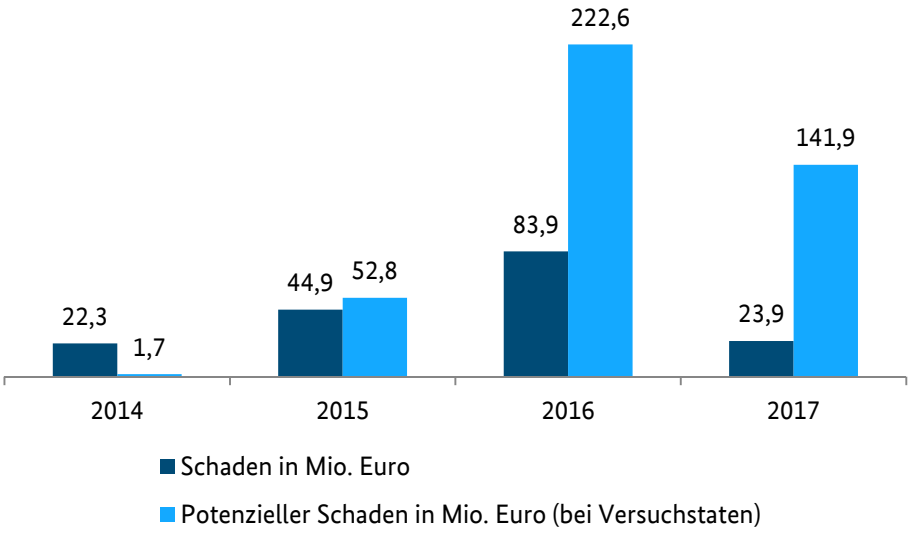


Im Jahr 2015 entfielen auf jeden vollendeten Fall des CEO-Fraud mehr als doppelt so viele Versuche. Bereits im Folgejahr hatte sich die Diskrepanz zwischen vollendeten Fällen und Versuchen deutlich erhöht (2016: 56 vollendete Fälle, 383 Versuche). Im Berichtsjahr 2017 standen einem erfolgreich durchgeführten CEO-Fraud sogar zehn Versuche gegenüber, wobei die Anzahl der Versuchstaten allerdings um ein Drittel auf 239 Fälle sank.

Eine sehr ähnliche Entwicklung ließ sich bei den Schadenssummen beobachten. Im Jahr 2015 waren der tatsächlich entstandene Schaden und der potenzielle Schaden bei versuchten Fällen des CEO-Fraud etwa gleich hoch. Im Jahr darauf hatte sich der Schaden nahezu verdoppelt (83,9 Mio. Euro) und der potenzielle Schaden mehr als vervierfacht (222,6 Mio. Euro). Analog zu den sinkenden Fallzahlen sind auch die Schadenszahlen im Jahr 2017 zurückgegangen. Der tatsächliche Schaden fiel um mehr als zwei Drittel auf 23,9 Mio. Euro, der potenzielle Schaden um mehr als ein Drittel auf 141,9 Mio. Euro.

[13] Sondererhebung des BKA. Aufgrund von Nacherfassungen und Datenbereinigungen können die Fallzahlen von denen im Bundeslagebild Wirtschaftskriminalität 2016 abweichen.

Schadensentwicklung CEO-Fraud[14]



Die dargestellten rückläufigen Entwicklungen bei Fall- und Schadenszahlen lassen sich unter anderem auf breit angelegte polizeiliche Sensibilisierungsmaßnahmen bei einer Vielzahl betroffener Wirtschaftsunternehmen zurückführen. Dabei wurden die Firmen über das Phänomen CEO-Fraud intensiv aufgeklärt und den Mitarbeitern Handlungsoptionen vermittelt, wie sie sich im konkreten Verdachtsfall verhalten sollen.

Die Tatsache, dass sich das Gros der registrierten Fälle auf Versuchstaten bezieht, könnte ein Indiz für die Wirksamkeit der Präventionsmaßnahmen und das daraus resultierende gesteigerte Bewusstsein für das Phänomen sein. Auch die polizeilichen Ermittlungserfolge dürften dazu beigetragen haben, ermittelte Täterstrukturen zumindest teilweise zu zerschlagen. Zudem kann davon ausgegangen werden, dass sich das Anzeigeverhalten bei den Unternehmen verändert hat und daher mehr Fälle gemeldet wurden.

Jeder CEO-Fraud ist zunächst als einzelne Betrugsstraftat zu betrachten. Erst die Zusammenführung vieler Einzelsachverhalte unter Berücksichtigung der konkreten Umstände der strukturierten Begehungsweise sowie der Tat- und Täterzusammenhänge erlaubt die Zuordnung dieses Phänomens zur Wirtschaftskriminalität. Zudem sind im Hinblick auf die erfassten Täterstrukturen einige OK-Indikatoren erfüllt, so dass bei den betrachteten Tätergruppierungen auch eine OK-Relevanz zum Tragen kommt.

Neben der gewerbs- und bandenmäßigen Tatausführung agieren die Täter in netzwerkartigen Strukturen, die für die verschiedenen Ausführungsschritte genutzt werden. Die jeweiligen Unterstützungshandlungen, z. B. Anrufe, Kontoerstellung, Bereitstellung von Ressourcen, Geldwäsche, erfolgen arbeitsteilig, unabhängig und ohne Kenntnis voneinander. Weiterhin verwenden diese Täterstrukturen zahlreiche Verschleierungsmechanismen (Fälschen von Telefonnummern und IP-Adressen, Nutzung von Proxy-Servern und Konten im Ausland), die ihnen ein hohes Maß an Abschottung gewähren sollen. Nicht zuletzt werden durch Fälle des CEO-Fraud hohe Geldbeträge kriminell erwirtschaftet, die entweder der persönlichen Bereicherung dienen oder in anderen kriminellen Bereichen investiert werden.

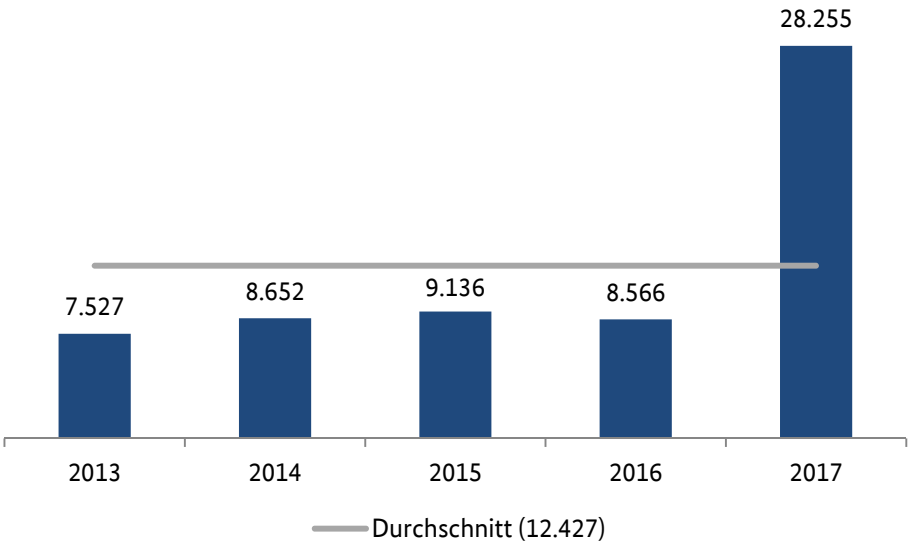
[14] Sondererhebung des BKA. Aufgrund von Nacherfassungen und Datenbereinigungen können die Schadenszahlen von denen im Bundeslagebild Wirtschaftskriminalität 2016 abweichen.

2.2.2 Anlage- und Finanzierungsdelikte[15]

Fall- und Schadenszahlen bei Anlage- und Finanzierungsdelikten verdreifacht

Im Jahr 2017 wurden in der PKS insgesamt 28.255 Anlage- und Finanzierungsdelikte registriert. Dies entspricht einem Anstieg um 229,9 % (2016: 8.566 Fälle). Die Fallzahl ist damit mehr als doppelt so hoch wie der Durchschnitt der vergangenen fünf Jahre (12.427 Fälle). Der registrierte Schaden nahm im Berichtsjahr ebenfalls zu und stieg auf 1.558 Mio. Euro (2016: 466 Mio. Euro; +234,3 %).

Fallentwicklung Anlage- und Finanzierungsdelikte[16]



Diese sprunghafte Entwicklung resultiert im Wesentlichen aus einem umfangreichen, im Jahr 2017 abgeschlossenen, Ermittlungskomplex in Sachsen. Dabei wurde nicht nur eine Vielzahl von Einzelfällen, sondern auch der verursachte hohe Gesamtschaden erfasst (siehe Fallbeispiel Anlagebetrug.)

[15] Der PKS-Summenschlüssel 893300 setzt sich aus den PKS-Schlüsseln 513000, 514100, 514300 und 714000 zusammen.
[16] Polizeiliche Kriminalstatistik.

Fallbeispiel: Anlagebetrug

Im Auftrag der StA Dresden ermittelte das LKA Sachsen seit dem Jahr 2012 in einem Verfahren gegen insgesamt zehn Beschuldigte wegen gewerbs- und bandenmäßigen Betrugs. Ihnen wurde vorgeworfen, über ein umfangreiches Konglomerat von 21 Firmen verschiedene Finanzprodukte wie Orderschuldverschreibungen, Genussscheine, Nachrangdarlehen, Fonds, Immobilien und Versicherungen vertrieben sowie mit Edelmetallen, insbesondere Gold, gehandelt zu haben. Dabei wurden die angelegten Gelder zum größten Teil nicht in die versprochenen Produkte gewinnbringend investiert, sondern in einem Geldkarussell eingesetzt und größtenteils zur Auszahlung fälliger Renditen sowie für den persönlichen Bedarf genutzt.

Im Rahmen dieses Umfangverfahrens wurden 23.626 Einzelfälle aufgeklärt. Bei über 40.000 verschiedenen Anlegern mit knapp 80.000 Einzahlungen entstand ein Gesamtschaden von über 1.300 Mio. Euro. Gegen die Beschuldigten und Firmen wurden vermögensabschöpfende Maßnahmen umgesetzt und Geldwerte von mehr als 150 Mio. Euro sichergestellt.

Kurzbewertung:

Das genannte Großverfahren aus dem Bereich Wirtschaftskriminalität setzte hinsichtlich Ermittlungsumfang, Schadenshöhe und Anzahl der Geschädigten neue Maßstäbe. Dieser Fall verdeutlicht einmal mehr das hohe Schadenspotenzial, das mit Wirtschaftskriminalität einhergeht.

Binäre Optionen

Beim Betrug i. Z. m. Binären Optionen handelt es sich um eine relativ neue Ausprägung der „klassischen“ Anlagedelikte. Er stellt nach Einschätzung von Europol ein europaweites Betrugsphänomen dar. Gemäß der BaFin sind Binäre Optionen Finanzinstrumente, deren Geschäftsmodelle unter Erlaubnisvorbehalt stehen. Der Handel mit Binären Optionen ist legal, sofern eine Aufsichtsbehörde in der EU diesen zugelassen hat und die Anbieter somit der Finanzaufsicht des jeweiligen Staates unterliegen. Ein lukrativer Markt für den illegalen Handel mit Binären Optionen besteht in Großbritannien, den USA, auf Zypern und Malta.

Binäre Optionen

Geschäfte mit Binären Optionen basieren auf dem „Alles-oder-Nichts-Prinzip“ und sind mit einem Wettgeschäft vergleichbar. In der Binären Logik gibt es nur zwei Möglichkeiten – „Ja“ oder „Nein“, „Gewinn“ oder „Verlust“. Der Anleger investiert bei dieser Anlageart einen festgelegten Geldbetrag auf einen Basiswert (z. B. Aktien oder Indizes) und „wettet“ auf eine bestimmte Kursentwicklung des Basiswerts. Tritt die entsprechende Entwicklung ein, realisiert der Anleger einen Anlagegewinn, ansonsten einen Anlageverlust.

Um am Handel mit Binären Optionen teilnehmen zu können, ist die Eröffnung eines Kundenkontos bei einer Online-Handelsplattform für Binäre Optionen notwendig. Nach Zahlung eines Fixbetrages kann der Anleger auf der Plattform seine Investitionen tätigen und seine (angeblichen) Gewinne/Verluste einsehen. Bei in betrügerischer Absicht gehandelten Binären Optionen werden dem Kunden durch teils aggressive Werbung verschiedene Anreize geboten, sich auf dieses „Wettgeschäft" einzulassen. Beispielsweise werden kurzfristige Gewinne, vermeintlich seriöse Renditen und die einfache Handhabung des Handels bei einer eigentlich risikobehafteten Anlageform beworben. Außerdem werden Anleger mit dem Versprechen gelockt, höhere Gewinne erzielen zu können, wenn sie bei höheren Einzahlungsbeträgen/Gebühren persönliche Beratungen, Premium-Kundenkonten oder Bonuszahlungen in Anspruch nehmen.

Entscheidend bei dieser Betrugsform ist die Diskrepanz zwischen der tatsächlichen Kursentwicklung und deren Bewertung durch die Betreiber der Handelsplattform. Diese berufen sich auf eigene, beliebig festgelegte Kurswerte, die von den Tageskursen der Basiswerte abweichen. Somit liegt die Realisierung eines Gewinnes, unabhängig von der tatsächlichen Kursentwicklung, im Ermessen des Anbieters. Fordert der Anleger die Auszahlung seines Guthabens, ist oftmals kein Zugriff auf das Kundenkonto mehr möglich oder die Kontaktperson bei der Handelsplattform nicht mehr erreichbar. In der Regel kommt es dabei zu einem Vermögensverlust bis hin zu einem Totalverlust beim Anleger.

Da der betrügerische Handel mit Binären Optionen ein relativ neues Phänomen ist, muss von einem erheblichen Dunkelfeld ausgegangen werden. Dennoch wurde im Zeitraum der Jahre 2016 bis 2017 in Deutschland bereits ein starker Anstieg der polizeirelevanten Sachverhalte mit einem Schadensvolumen im siebenstelligen Euro-Bereich festgestellt. Im Zuge dessen wurden bislang mindestens 65 Online-Anbieter für Binäre Optionen im deutschen Raum erfasst.

2.2.3 Betrug/Untreue i. Z. m. Kapitalanlagen[17]

Fallzahlen mehr als verdreifacht, Schäden mehr als vervierfacht

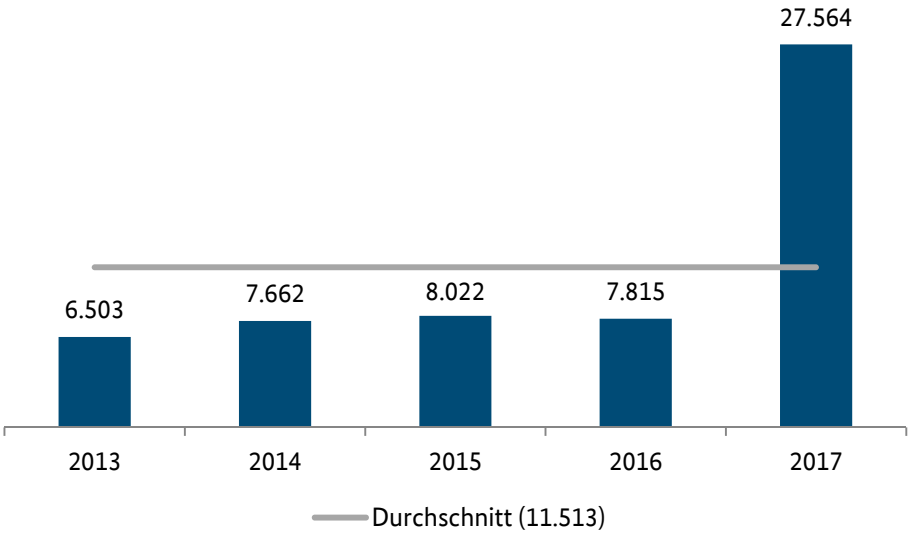
Die PKS subsumiert unter Betrugs- und Untreuehandlungen i. Z. m. Beteiligungen und Kapitalanlagen die Delikte Prospektbetrug (Kapitalanlagebetrug), Anlagebetrug und die Untreue bei Kapitalanlagegeschäften.

Bei den Betrugsdelikten i. Z. m. Kapitalanlagen zeigte sich eine ähnliche Entwicklung wie bei den Anlage- und Finanzierungsdelikten. Die Anzahl der Fälle stieg auf 27.564 an (2016: 7.815 Fälle; +252,7 %). Demzufolge war die Fallzahl zweieinhalb Mal so hoch wie der Fünf-Jahres-Durchschnitt (11.513 Fälle). Dieser Teilbereich der Wirtschaftskriminalität speist sich zu über 99 % aus Fällen des Anlagebetrugs, wohingegen Prospektbetrug und Untreue bei Kapitalanlagen kaum ins Gewicht fallen. Die Schadenssumme hat sich angesichts des Fallanstiegs ebenfalls stark erhöht und lag im Berichtsjahr bei 1.617 Mio. Euro (2016: 356 Mio. Euro; +354,2 %).

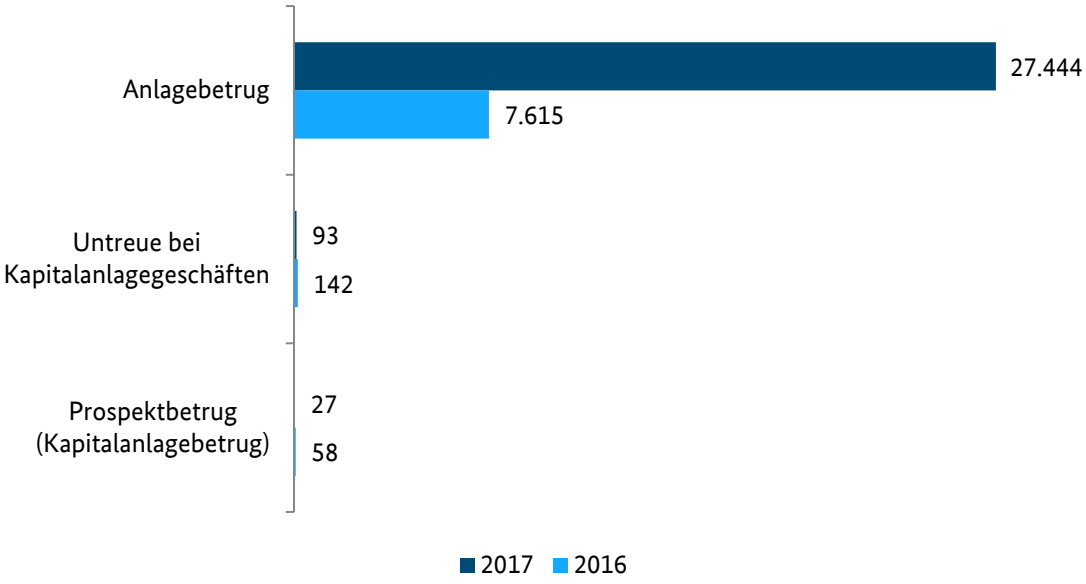
Fall- und Schadensanstieg lassen sich, wie bei den Anlage- und Finanzierungsdelikten (Kapitel 2.2.2), auf das bereits beschriebene, umfangreiche Verfahren aus Sachsen zurückführen. Da bei der PKS-Erfassung eine Straftat mehreren Einzelphänomenen zugeordnet werden kann, wirkt sich das Verfahren aus Sachsen statistisch sowohl auf die Anlage- und Finanzierungsdelikte als auch auf den Bereich Betrug/Untreue i. Z. m. Kapitalanlagen aus.

[17] Der PKS-Summenschlüssel 893600 setzt sich aus den PKS-Schlüsseln 513100, 513200 und 521100 zusammen

Fallentwicklung Betrug/Untreue i. Z. m. Kapitalanlagen[18]



Betrug i. Z. m. Kapitalanlagen im Einzelnen[19]



[18] Polizeiliche Kriminalstatistik.
[19] Polizeiliche Kriminalstatistik.

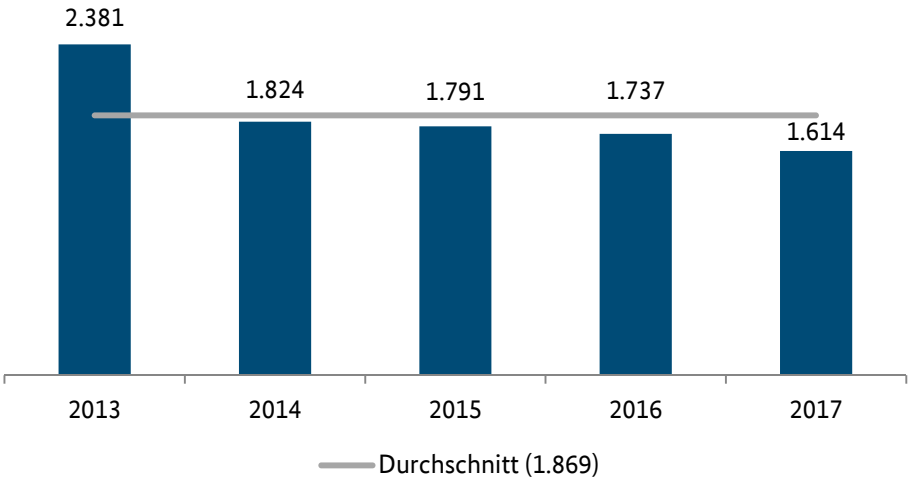
2.2.4 Wettbewerbsdelikte[20]

Kontinuierlicher Rückgang bei Wettbewerbsdelikten

Unter Wettbewerbsdelikten werden gemäß PKS alle Deliktsformen i. Z. m. Verstößen gegen das Gesetz gegen den unlauteren Wettbewerb (UWG), Urheberrechtsbestimmungen sowie nach dem Strafgesetzbuch (StGB) verstanden.

Im Jahr 2017 wurden in der PKS 1.614 Wettbewerbsdelikte (2016: 1.737; -7,1 %) erfasst. Im Berichtsjahr lag die Anzahl der Fälle erneut unter dem Durchschnitt der vergangenen fünf Jahre (1.869 Fälle). Im Gegensatz zur Entwicklung bei den Fallzahlen hat sich der Schaden leicht auf 8 Mio. Euro erhöht (2016: 7 Mio. Euro; +14,3 %).

Fallentwicklung Wettbewerbsdelikte[21]



Schneeballsysteme und Anlagebetrug bei Investitionen in virtuelle Währungen

Das von Europol im Jahr 2017 veröffentlichte „Serious and Organised Crime Threat Assessment“ (SOCTA) weist auf die grundsätzliche Bedeutung von Schneeballsystemen im Kontext kriminellen Handelns hin. Bei diesem Phänomen der Wirtschaftskriminalität können, wie Einzelfallbetrachtungen zeigen, illegale Profite in Milliardenhöhe erwirtschaftet werden.

Bei Investments in virtuelle Währungen kann es sich um Schneeballsysteme oder sonstige Anlagebetrugsmodelle handeln. Zu unterscheiden sind dabei zum einen Investitionen in sog. „Initial Coin Offerings“ (ICOs) oder Investitionen in bereits bestehende, alternative virtuelle Währungen (in Abgrenzung zum Bitcoin). Zum anderen gibt es die Möglichkeit, in sonstige i. Z. m. virtuellen Währungen stehende Anlagemodelle zu investieren, z. B. Handelsroboter für virtuelle Währungen oder das Cloud Mining. Bei letzterem legt der Investor Kapital in externe Rechenzentren zum Schürfen von Kryptowährungen an, ohne dass für ihn die Notwendigkeit besteht, eigene Hardware vorzuhalten.

Bei einem ICO handelt es sich laut BaFin um ein neues Mittel der Kapitalaufnahme zur Finanzierung unternehmerischer Vorhaben. Dabei werden neue digitale Einheiten erzeugt (Token Genera-

[20] Der PKS-Summenschlüssel 893400 setzt sich aus den PKS-Schlüsseln 656000, 715000 und 719200 zusammen.
[21] Polizeiliche Kriminalstatistik.

ting Event). Die generierten Token werden meist in einem unregulierten öffentlichen Bieterverfahren an interessierte Anleger verkauft (Token Sale). Eine Form des ICOs ist die Schaffung neuer virtueller Währungen basierend auf der Distributed Ledger bzw. Blockchain-Technologie. Ein ICO kann auch als Form des Crowdfunding bezeichnet werden.

Kryptowährungen[22]

Bei Kryptowährungen bzw. virtuellen Währungen handelt es sich um jegliche Form von Zahlungsmitteln, welche ausschließlich digital vorliegen und in der Regel von keiner zentralen oder regulierenden Instanz herausgegeben werden. Demgegenüber wird ein dezentrales Netzwerksystem zur Aufzeichnung von Transaktionen und zur Generierung neuer Währungseinheiten verwendet (Blockchain-Technologie). Zur Prävention von Fälschungen und betrügerischen Überweisungen wird Kryptografie eingesetzt. Eine Regulierung durch Banken oder Aufsichtsbehörden findet in der Regel nicht statt. Trotz öffentlich zugänglichem Transaktionsregister erfolgt die Zahlungsabwicklung anonymisiert bzw. pseudonymisiert.

Laut der Branchenseite Coinschedule.com gab es im Jahr 2017 weltweit mehr als 200 ICOs mit einer Gesamtinvestitionssumme von knapp 3,9 Mrd. US-Dollar.[23] Die Tendenz ist stark steigend und verdeutlicht das starke Interesse, in virtuelle Währungen zu investieren.

Merkmale und Zweck der Token und Coins können sich je nach Ausgestaltung des angebotenen Investitionssystems stark unterscheiden. Einige Coins oder Token ermöglichen die Nutzung oder den Kauf von Dienstleistungen oder Produkten, die der Anbieter mit dem Erlös aus dem ICO entwickelt. Mit anderen werden Stimmrechte oder Anteile an künftigen Einnahmen des Anbieters erworben. Nicht alle ICOs haben einen konkreten Mehrwert. Einige werden gehandelt und/oder lassen sich nach der Emission an spezialisierten Coin-Handelsplattformen gegen herkömmliche oder virtuelle Währungen eintauschen. Ziel von Anbietern und Anlegern ist hier oft auch die Idee des Aufbaus und der Nutzung eines neuen und möglicherweise besseren, neben den etablierten Kryptowährungen bestehenden kryptografischen Zahlungssystems.

Aufgrund der unterschiedlichen Ausgestaltungen können diese Geschäftsmodelle vielfältigen finanzaufsichtsrechtlichen Verpflichtungen unterliegen. Die BaFin und die europäische Finanzaufsichtsbehörde ESMA haben dazu bereits zahlreiche Erläuterungen und Warnmeldungen einschließlich des Verweises auf mögliche betrügerische Aktivitäten herausgegeben.

Die Bewerbung von ICOs und Investitionsmodellen in neue, alternative virtuelle Währungen findet häufig im Internet und in Sozialen Medien statt. Die Gewinnung weiterer Anleger erfolgt oft über das sog. „Multi-Level-Marketing“.

[22] Es handelt sich hierbei nicht um eine Legaldefinition des Begriffs „Kryptowährung“, sondern vielmehr um eine erläuternde Darstellung.
[23] Vgl. https://www.coinschedule.com/stats.html?year=2017.

Das gesellschaftliche und unternehmerische Interesse an virtuellen Währungen steigt beständig, nicht zuletzt aufgrund des starken Wertanstiegs des Bitcoin und der damit einhergehenden Medienaufmerksamkeit und Werbeaktivität vor allem in Sozialen Netzwerken. Daher ist nicht nur mit einem Wachstum in diesem Marktsegment zu rechnen, sondern auch mit verstärkten betrügerischen Handlungen im Bereich der Investitionen i. Z. m. virtuellen Währungen.

Modi Operandi bei Betrugsformen i. Z. m. Investitionen in virtuelle Währungen[24]

2.2.5 Insolvenzdelikte[25]

Anzahl der Insolvenzdelikte rückläufig, Schaden bleibt hoch

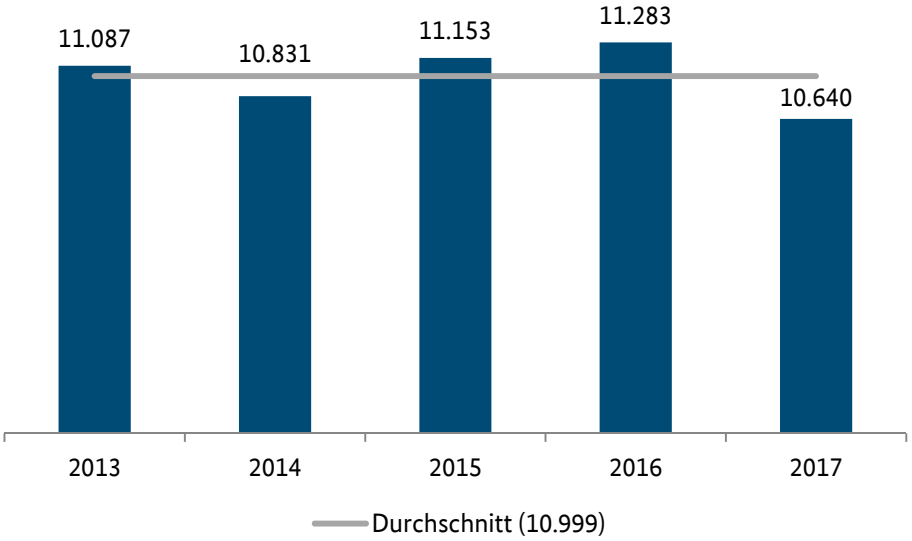
Zum Bereich der Insolvenzdelikte zählen gemäß Definition der PKS die Tatbestände

- Bankrott und besonders schwerer Fall des Bankrotts (§§ 283 und 283 a StGB),
- Verletzung der Buchführungspflicht (§ 283 b StGB),
- Gläubiger- und Schuldnerbegünstigung (§§ 283 c und 283 d StGB) sowie
- Insolvenzverschleppung (§ 84 GmbHG; §§ 130 b, 177 a HGB und § 15 a IV, V InSO).

Mit 10.640 registrierten Fällen sank die Anzahl der Insolvenzdelikte im Berichtsjahr um 5,7 %. Der durch Insolvenzdelikte verursachte Schaden verringerte sich im Jahr 2017 um ein Viertel auf 1.157 Mio. Euro (2016: 1.566 Mio. Euro; -26,1 %). Trotz des Schadensrückgangs bleibt das Schadenspotenzial in diesem Teilbereich der Wirtschaftskriminalität hoch. Da Insolvenzstraftaten oftmals mit weiteren Begleitdelikten einhergehen (z. B. Vorenthalten und Veruntreuen von Arbeitsentgelt gemäß § 266 a StGB), dürfte der tatsächlich verursachte Schaden in diesem Bereich über der genannten Schadenssumme liegen.

[24] Bundeskriminalamt.
[25] Der PKS-Summenschlüssel 893200 setzt sich aus den PKS-Schlüsseln 560000 und 712200 zusammen.

Fallentwicklung Insolvenzdelikte[26]



2.2.6 Abrechnungsbetrug im Gesundheitswesen[27]

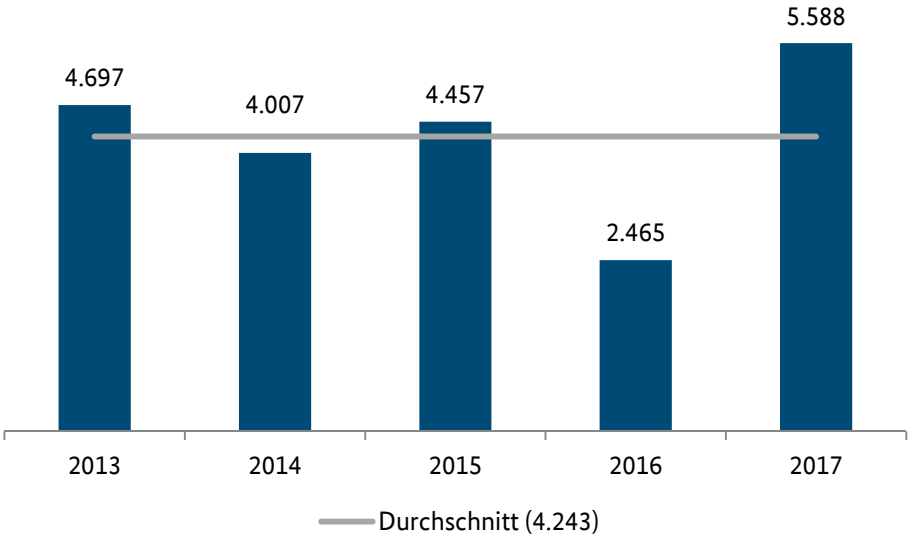
Abrechnungsbetrug im Gesundheitswesen auf Fünf-Jahres-Hoch

Gesundheitsdelikte im Sinne der Wirtschaftskriminalität umfassen nach Definition der PKS die Fälle des Abrechnungsbetrugs im Gesundheitswesen zur betrügerischen Erlangung von Geldleistungen von Selbstzahlern, Krankenkassen, Krankenversicherungen und Beihilfestellen durch Angehörige medizinischer oder pharmazeutischer Berufe sowie durch Krankenhäuser und Sanatorien.

Nach einem starken Rückgang im Vorjahr ist die Fallzahl beim Abrechnungsbetrug im Gesundheitswesen auf 5.588 Fälle im Jahr 2017 angestiegen und hat sich somit mehr als verdoppelt (2016: 2.465 Fälle; +126,7 %). Damit erreichte dieser Deliktsbereich den höchsten Wert der vergangenen fünf Jahre und lag deutlich über dem Fünf-Jahres-Durchschnitt (4.243 Fälle). Das verstärkte Fallaufkommen ist vor allem auf Berlin zurückzuführen, wo im Berichtsjahr 3.051 Fälle erfasst wurden (2016: 85). Diese Entwicklung wurde u. a. durch ein Großverfahren verursacht, in welchem zahlreiche Fälle der Falschabrechnung von Impfleistungen als privatärztliche Leistungen zusammengeführt wurden.

[26] Polizeiliche Kriminalstatistik.
[27] Fälle des Abrechnungsbetrugs im Gesundheitswesen unter werden unter dem PKS-Schlüssel 518110 erfasst.

Fallentwicklung Gesundheitsdelikte – Abrechnungsbetrug im Gesundheitswesen[28]



Analog zur Fallzahl stieg der erfasste Gesamtschaden im Vergleich zum Vorjahr auf etwa 120 Mio. Euro (2016: 29 Mio. Euro; +313,8 %). Die Entwicklung der Schadenssumme lässt sich auf Ermittlungsverfahren in Baden-Württemberg (2017: 37,1 Mio. Euro) und Nordrhein-Westfalen (2017: 59,2 Mio. Euro) zurückführen. Trotz des starken Anstiegs beim Schaden erfolgte in beiden Ländern ein wesentlich geringerer Anstieg der absoluten Fallzahlen als in Berlin.

Der markante Schadensanstieg in Nordrhein-Westfalen resultierte im Wesentlichen aus dem Abschluss eines Ermittlungsverfahrens, in dem über die Kassenärztliche Vereinigung nicht erbrachte Laborleistungen abgerechnet wurden. Die hohe Schadenssumme in Baden-Württemberg ergab sich aus einem Umfangsverfahren, dem 59 Einzelfälle zugrunde lagen.

Abrechnungsbetrug im Gesundheitswesen durch russischsprachige Pflegedienste

Eine spezielle Ausprägung des Abrechnungsbetrugs, vor allem vor dem Hintergrund einer OK-Relevanz, ist der Abrechnungsbetrug im Gesundheitswesen durch russischsprachige bzw. mehrheitlich von Personen aus den Staaten der ehemaligen Sowjetunion geführten Pflegediensten. Hierbei handelt es sich um ein bundesweites Phänomen, das insbesondere dort auftritt, wo sich durch Sprachgruppen geschlossene Systeme bilden.

Die Täter wählen beim Abrechnungsbetrug unterschiedliche Vorgehensweisen, indem sie beispielsweise

- nur zum Teil oder überhaupt nicht erbrachte Leistungen abrechnen,
- die Pflegebedürftigkeit von Patienten vortäuschen (Patienten simulieren bewusst),
- Ärzte und Pflegepersonal bestechen oder
- Urkunden i. Z. m. der Ausstellung von Ausbildungszertifikaten fälschen.

In vielen dieser Fälle liegen Indizien für ein strukturiertes und organisiertes Vorgehen der Pflegedienste mit dem Ziel der illegalen Gewinnmaximierung vor. In Einzelfällen lassen sich i. Z. m. Inves-

[28] Polizeiliche Kriminalstatistik.

titionen in russischsprachige, ambulante Pflegedienste auch Hinweise auf eine OK-Relevanz erkennen. Beispielsweise ist das Vorgehen der Täter nicht nur banden- und gewerbsmäßig, sondern es werden zudem Scheinfirmen im In- und Ausland eingerichtet, hierarchische Strukturen innerhalb der Gruppierung kommen zum Tragen und es wird „Schutzgeld“ an die Hinterleute gezahlt. Mittlerweile konzentrieren sich die Täter auf das Geschäft mit Intensivpflegepatienten, da in diesem Bereich die höchsten Gewinne erzielt werden können. Krankenkassen zahlen für einen Intensivpflegepatienten monatlich etwa 22.000 Euro.

In Anbetracht der demografischen Entwicklung wird der Pflegemarkt in Deutschland weiter wachsen und somit der Abrechnungsbetrug im Gesundheitswesen auch zukünftig von Bedeutung sein. Aufgrund einer bundesweiten Kooperation der Polizeibehörden ist es gelungen, einen Teil des Phänomens aufzuhellen und zahlreiche polizeiliche Präventionsmaßnahmen umzusetzen. Auf diese Weise wurden die Kostenträger für diese spezielle Ausprägung des Abrechnungsbetrugs im Gesundheitswesen wirkungsvoll sensibilisiert.

Angesichts der Sensibilisierung wurde der Kontrolldruck auf Pflegedienste erhöht, was ebenfalls eine Erklärung für den bereits erläuterten Fallanstieg in Berlin sein könnte. Sobald Pflegedienste mit illegitimen Rechnungsansprüchen bei den Kostenträgern in Erscheinung treten, werden die Forderungen nicht ausgezahlt, bis ein Nachweis über die korrekte und geprüfte Rechnungsforderung vorliegt. Das eingesparte Geld setzen die Kostenträger für verstärkte Kontrollen ein, was im Falle der Anzeigenerstattung durch den Kostenträger zu einer erhöhten Aufdeckung betrügerisch abrechnender Pflegedienste führen kann.

Seitens der Politik erfolgte durch die Verabschiedung des Pflegestärkungsgesetzes III im Jahr 2017 ebenfalls eine entsprechende Reaktion, welches u. a. Maßnahmen zur Prävention, Aufdeckung und Bekämpfung von Abrechnungsbetrug im Gesundheitswesen vorsieht.

Fallbeispiel: Abrechnungsbetrug im Gesundheitswesen

Seit 2014 ermittelte das LKA Nordrhein-Westfalen in einem OK-Verfahren gegen eine deutsche Tätergruppierung mit russisch-ukrainischem Migrationshintergrund wegen gewerbsmäßigen Betrugs und Geldwäsche. Die Hauptbeschuldigten betrieben parallel bis zu drei Pflegedienste und rechneten nicht oder nur zum Teil erbrachte Pflegeleistungen betrügerisch bei den Kostenträgern (Kranken-/Pflegekassen und Kommunen) ab, um das deutsche Pflegesystem zur eigenen illegalen Gewinnmaximierung auszunutzen.

Zum Teil waren Ärzte und Patienten in das betrügerische System eingebunden. Die Ärzte attestierten gegen Bestechungsgeld die notwendige Pflegebedürftigkeit, welche für die Abrechnung erforderlich ist. Die Patienten täuschten vielfach ihre Pflegebedürftigkeit vor und erhielten anstelle der Pflegeleistungen kleinere monatliche Geldzahlungen bzw. Kompensationsleistungen in Form von Fahrten zu Ärzten, Putzen der Wohnung, Pediküre/Maniküre sowie Friseurleistungen, auf welche sie keinen Anspruch gehabt hätten. Zur Verschleierung der Betrugshandlungen führten die Mitarbeiter des Pflegedienstes die Pflegedokumentation gemäß den Vorgaben der Rahmenverträge nur unzureichend durch oder nutzten zwei unterschiedliche Dienst- bzw. Tourenpläne. Den ersten für Abrechnungszwecke, den zweiten für tatsächlich durchgeführte Leistungen.

Im Zuge der Exekutivmaßnahmen wurden 180 Wohn- und Geschäftsräume durchsucht, vier Tatverdächtige in Haft genommen und zahlreiche Geschäftsunterlagen sichergestellt. Das Landgericht Düsseldorf verurteilte im Februar 2018 fünf Männer und vier Frauen zu Freiheitsstrafen zwischen zwei und sieben Jahren. Der Hauptangeklagte wurde zu einer Gesamtfreiheitsstrafe von sieben Jahren und einer Zahlung in Höhe von 500.000 Euro verurteilt. Durch das betrügerische Handeln der Gruppierung entstand ein Gesamtschaden von mindestens 4,7 Mio. Euro.

Kurzbewertung:

Das Ermittlungsverfahren zeigt das hohe Schadenspotenzial, das vom Abrechnungsbetrug durch betrügerisch agierende Pflegedienste ausgeht. Nicht zuletzt durch diesen Fall ist die Thematik in den medialen Fokus gerückt, was die Politik zu entsprechenden Anpassungen in der Pflegegesetzgebung veranlasst hat.

3 Gesamtbewertung

Die Anzahl der Straftaten im Bereich der Wirtschaftskriminalität ist im Jahr 2017 stark gestiegen und befindet sich auf dem höchsten Stand der letzten fünf Jahre. Auch der durch Wirtschaftskriminalität registrierte Schaden lag deutlich über dem Vorjahreswert. Die Betrachtung der langfristigen Fall- und Schadensentwicklung zeigt die übliche Schwankungsbreite im Bereich der Wirtschaftskriminalität, die durch einzelne Umfangsverfahren hervorgerufen wird.

Von Bedeutung ist die Intensivierung polizeilicher Aufgabenwahrnehmung bei besonders schadensträchtigen und sozialschädlichen Wirtschaftsdelikten. So haben die Strafverfolgungsbehörden mit einer eng abgestimmten länderübergreifenden Zusammenarbeit bei der Bekämpfung des Betrugs auf den Abrechnungsbetrug im Gesundheitswesen durch russischsprachige Pflegedienste und organisiert begangene Massenkriminalität reagiert und die Öffentlichkeit sowie betroffene Institutionen hinsichtlich dieses Phänomens sensibilisiert. In diesem Zusammenhang haben die Präventionsmaßnahmen der Polizei nicht nur zu einer verstärkten Wahrnehmung in der Öffentlichkeit geführt, sondern gleichwohl zu umfangreichen Änderungen in der Pflegegesetzgebung. Ähnliche Erfolge durch Prävention wurden bei der Bekämpfung des CEO-Fraud erzielt: Eine bundesweite Präventionskampagne bei Wirtschaftsverbänden und -unternehmen, auch unter verstärktem Einsatz Sozialer Medien, dürfte zu einem deutlichen Rückgang der vollendeten Fälle des CEO-Fraud in Deutschland geführt haben.

Die erhöhte Sensibilisierung hat in einigen Bereichen einen verstärkten Kontrolldruck nach sich gezogen, der zur Aufdeckung krimineller Aktivitäten und somit auch zu einem Anstieg der Fallzahlen führte. Außerdem sollen Wirtschaftskriminelle durch Kontrollmaßnahmen von der Begehung entsprechender Wirtschaftsdelikte abgeschreckt werden.

Trotz eines Rückgangs bei der Nutzung des Tatmittels Internet i. Z. m. Wirtschaftsdelikten spielt die digitale Welt eine bedeutende Rolle. Das Internet schafft neue und vielfältige Tatgelegenheiten. So können mit Hilfe von Social Bots nicht nur Märkte sondern auch Meinungen von Kunden und Anlegern bewusst für betrügerische Zwecke manipuliert werden.

Die tatsächliche Bedeutung des organisiert begangenen Betrugs spiegelt sich bei ausschließlicher Betrachtung der polizeilichen Daten kaum wider. Vielmehr ist von einem hohen Dunkelfeld und darüber hinaus auch davon auszugehen, dass Kriminelle, die zuvor in den „klassischen“ Bereichen der Wirtschaftskriminalität (z. B. Wettbewerbs-, Anlagedelikte) aktiv waren, ihre Kenntnisse für organisiert begangene Betrugstaten (z. B. Telefonbetrug) nutzen.

Neue legale Anlageprodukte und Finanzierungsmöglichkeiten, wie der Handel mit Binären Optionen und Investitionen in virtuelle Währungen, können zur illegalen Gewinnmaximierung missbraucht werden. Dies stellt die Strafverfolgungsbehörden vor die Herausforderung, frühzeitig eine Lageeinschätzung mit dem Ziel der Verhinderung von Straftaten vorzunehmen. Gleiches gilt für Techniken, wie z. B. Social Bots, bei denen diskutiert wird, ob ihr Einsatz auf eine mögliche Beeinflussung der politischen Willensbildung abzielen könnte und ob dies auf einzelne Bereiche des Wirtschaftslebens übertragbar ist.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
2018

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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

Dateiname: 180612_BLB Wikri 2017.docx
Verzeichnis: Z:\12 Internet\01_bka.de\00_Aktualisierungen\2018\06_Juni\180611_Bundeslagebild-Wirtschaftskriminalität 2017
Vorlage: C:\Users\bk044165\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3705E060.dotm
Titel:
Thema:
Autor: Rossow, Marcus (BKA-SO51-3)
Stichwörter:
Kommentar:
Erstelldatum: 11.06.2018 14:17:00
Änderung Nummer: 2
Letztes Speicherdatum: 11.06.2018 14:17:00
Zuletzt gespeichert von: Müller, Marie (BKA-ZD12-4)
Letztes Druckdatum: 11.06.2018 17:08:00
Nach letztem vollständigen Druck
Anzahl Seiten: 27
Anzahl Wörter: 6.907 (ca.)
Anzahl Zeichen: 43.518 (ca.)