Lehr- und Studienbriefe Kriminalistik / Kriminologie

Herausgegeben von

Horst Clages, Leitender Kriminaldirektor a.D.,
Wolfgang Gatzke, Direktor LKA NRW a.D.

Band 26
Cybercrime

von

Christoph Keller, Polizeidirektor
Prof. Dr. Frank Braun
Prof. Dr. Jan Dirk Roggenkamp

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Buchvertrieb

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime“, 1. Auflage 2020
ISBN 978-3-8011-0880-9

Vorwort

Unter dem schillernden Begriff Cybercrime wird eine Vielzahl unterschiedlichster Straftaten verstanden, deren kleinster gemeinsamer Nenner die kriminelle Nutzung von Informationstechnologie und IT-Strukturen, namentlich des Internets ist. Cybercrime-Phänomene reichen vom Hacking über den betrügerisch-destruktiven Einsatz von Malware und Botnetzen, Angriffe auf den Zahlungs- und Warenverkehr mittels Phishing- und Skimming-Methoden oder das Bereitstellen und die Nutzung krimineller Infrastruktur im sog. Darknet.

Diese Einführung orientiert sich an den unterschiedlichen Erscheinungsformen von Cybercrime. Die Identifizierung der typischen kriminellen Handlungsmuster (Teil A.) ist demnach Ausgangspunkt der Darstellung, wobei auf die einschlägigen Straftatbestände hingewiesen wird. Daran schließt sich ein knapper Überblick über die wichtigsten strafrechtlichen Fragestellungen an (Teil B.). In den nachfolgenden Kapiteln stehen die Ermittlungsmöglichkeiten der Strafverfolgungsbehörden im Fokus (Teil C. Computerforensik und Teil D. Informationsgewinnung in Netzwerken), gefolgt von Handlungsanweisungen zur Kriminalitätsbekämpfung im sog. Ersten Angriff (Teil E. Polizeiliche Bekämpfung der Internetkriminalität). In einem Ausblick wird zudem auf den ermittlungstechnischen Einsatz von Big-Data-Technologie (Teil F.) aufmerksam gemacht.

Als Einführungswerk richtet sich die Schrift in erster Linie an Praktiker, die einen „Neueinstieg“ in die Materie suchen, sowie an Polizeibeamte in Ausbildung und Studium. Für eine Vertiefung der gewonnenen Erkenntnisse sei insbesondere auf das Handbuch von Dieter Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018, und dessen Internetauftritt (http://www.cyberfahnder.de) hingewiesen.

Zu danken gilt es Herrn EKHK Ulli Bahlo und Herrn EKHK Peter Niehoff für die kritische Durchsicht des Manuskripts und ihre wertvollen Hinweise, die vor allem bei der Erstellung von Checklisten Eingang in die Darstellung gefunden haben.

Berlin, Hofkirchen und Mettingen im Sommer 2020

Die Autoren

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime“, 1. Auflage 2020
ISBN 978-3-8011-0880-9

A. Phänomenologie

I. Unrechtskultur im digitalen Raum

Die Digitalisierung in allen Bereichen bietet umfassende Möglichkeiten für Straftäter

Viele „klassische" Deliktsfelder werden zu einem nicht unerheblichen Teil in der „digitalen Welt" abgewickelt. So wird im Internet illegal Handel mit Betäubungsmitteln, Waffen, Darstellungen des sexuellen Missbrauchs von Kindern sowie urheberrechtlich geschütztem Material betrieben. Die Betrugsfälle im Netz – von „Abo-Fallen" bis zum millionenschweren Anlagebetrug bei Kryptowährungen[1)] – sind seit jeher Legion. Höchstes Schadenspotential bergen Angriffe auf die Vertraulichkeit und Integrität informationstechnischer Systeme[2)]. Gerade durch die Manipulation von IT-Systemen bzw. deren Sabotage (etwa durch Bot-Netze, Einsatz von Ransomware, Hacking) können die Funktionsfähigkeit von Wirtschaft und Staat gefährdet werden.

Der Begriff **Cybercrime** bezeichnet als Sammelbegriff alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.[3)] Es handelt sich um einen äußerst dynamischen Deliktsbereich, dem im Zuge der umfassenden Digitalisierung neue Kriminalitätserscheinungen hinzutreten. Das Spektrum ist nahezu unbegrenzt und reicht u.a. von Hacking-Attacken, Verbreitung und Einsatz von Schadsoftware, über Kreditkartenbetrug, Urheberrechtsverletzungen, bis hin zu Identitätsdiebstahl und Cyber-Terrorismus bzw. Cyber-War.[4)]

Die Kreativität der Delinquenten kennt dabei kaum Grenzen. Auf technische Entwicklungen wird flexibel, schnell und professionell reagiert, etwa bei der Verbreitung von Malware[5)]. Befeuert wird dies durch eine kriminelle Wissenscommunity, die sich in der „Underground economy" (dt. „Schwarzmarkt" – bezogen auf entsprechende Foren und Plattformen im sog. Darknet)[6)] etabliert hat. Dort werden Themen wie das Programmieren von Malware diskutiert oder Anleitungen zum Hacken von Webservern und Hinweise zum Anmieten von Bot-Netzen gegeben. Technisch weniger Begabte können „gephishte" Zugangsdaten zu Bank-, eBay- oder PayPal-Konten oder „geskimmte" oder sonst entwendete Kreditkarten-Daten (sog. „credit card dumps") usw. käuflich erwerben.[7)]

Die Tätertypen sind, wie ihre Motive und ihr technisches Können, äußerst different.[8)] Vom „Einsteiger bis zum Profi" ist alles vertreten: jugendliche Hacker, die ihr Potenzial testen wollen, Gelegenheitstäter, Extremisten, Erpresser, Terroristen, lose kriminelle Zusammenschlüsse und international organisierte Banden, Nachrichtendienste anderer Staaten, usw. Im Bereich des Hacking werden vom BKA grob folgende Typen unterschieden:[9)]

7) Seidl, Deutsche Polizei 7/2013, 4 (9).

8) Ausf. zur Perspektive der Täter Huber 2019, S. 32 ff.

9) Ziercke, Tagungsband BKA, Herbsttagung v. 12./13.11.2013, S. 62 ff.

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

Einsteiger	Kriminelle mit IT-Grundkenntnissen. Z.B. sog. Script Kids, die sich mittels Software-Toolkits überwiegend mit Phishing im Bereich Social Engineering und oder Defacement beschäftigen, also dem Verändern von Webseiten.
Hacker (Fortgeschrittene)	Führen strukturierte Attacken durch, wie DDoS, Drive-by-exploits oder SQL-injections
Profis	Staatlich gelenkte Hacker, terroristische Gruppen oder auch „Hacktivisten"; Hacktivisten verstehen sich als Kämpfer gegen Ungerechtigkeit (Handeln als ziviler Ungehorsam gegen bestimmte politische Richtungen)

Bei der Bekämpfung dieser äußerst breit gefächerten IT-Kriminalität sind generalpräventive Aspekte als nachrangig zu bewerten. Zwar erfolgt in regelmäßigen Abständen reflexartig der Ruf nach dem Strafrecht („Strafrecht als politischer Reflex"[10]) kombiniert mit der Floskel, dass das „Internet kein rechtsfreier Raum"[11] sein oder werden dürfe. Übersehen wird hierbei, dass das Strafrecht bereits seit vielen Jahren einen weitgehend geeigneten Deliktskatalog mit angemessenen Strafrahmen zur Verfügung stellt (allgemeine Straftatbestände[12] und spezielle zur Bekämpfung der „Computerkriminalität", vgl. **B.**). Zudem zeigen Untersuchungen zur negativen Generalprävention, dass im Bereich Cybercrime die erwartete Schwere der Strafe bedeutungslos ist. Die Verschärfung des Rechts würde also kaum Auswirkungen haben. Es gibt keine Anhaltspunkte dafür, dass eine Verschärfung des Strafrechts das Normbewusstsein positiv beeinflussen würde[13]. Zu adressieren ist vielmehr das von (potentiellen) Tätern wahrgenommene Entdeckungsrisiko. Im digitalen Raum herrscht offenbar nur geringe Angst vor Strafverfolgung. Anders gewendet: Die bestehenden Straftatbestände kommen mangels adäquater Verfolgung nicht zur Anwendung. Strategisch muss deshalb die Erhöhung der Verfolgungswahrscheinlichkeit im Mittelpunkt stehen. Gerade den Sicherheitsbehörden kommt bei der Bekämpfung der Unrechtskultur im digitalen Raum eine wichtige Rolle zu.[14] Um dieser gerecht werden zu können, bedarf es zunächst auf breiter Basis phänomenologischer Kenntnisse. Nachfolgend werden daher die für die Praxis wichtigsten Phänomene des Cybercrime in ihren Grundzügen dargestellt.

II. Kriminalitätsbegriff und Kriminalitätserfassung

1. Cybercrime-Konvention

Das „Übereinkommen über Computerkriminalität" – besser bekannt als **„Convention on Cybercrime"** bzw. **Cybercrime-Konvention** – ist ein Übereinkommen des Europarats aus dem Jahr 2001.[15] Sie wurde ausgehandelt, um dem

10) Singelnstein, Zeitschrift für Rechtssoziologie 2014, 321 (325). Es wird demonstrativ vermittelt, dass etwas getan werde.

11) Die Phrase hat sogar einen eigenen Wikipedia-Eintrag, https://de.wikipedia.org/wiki/Rechtsfreier_Raum.

12) Hierzu Neubacher 2017, 26. Kapitel, Rn. 4.

13) Hierzu Singelnstein, Zeitschrift für Rechtssoziologie 2014, 321 ff. m.w.N.

14) Rüdiger, Kriminalistik 2019, 37 (41).

15) Convention on Cybercrime, Budapest, 23.11.2001 (CETS No. 185); Deutschland ratifizierte die EU-Konvention am 9.3.2009; näher dazu Hirsch, in: Clages/Ackermann 2019, S. 644 f.

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

grenzüberschreitenden Charakter der Kriminalität im Internet Rechnung zu tragen. Die Gesamtzahl der Ratifikationen bzw. Beitritte beläuft sich derzeit auf 64 Staaten.[16] Zweck des Abkommens ist eine wirksame internationale Zusammenarbeit bei der Bekämpfung der Datennetzkriminalität. Verbesserten Schutz vor IT-Kriminalität sollen dabei harmonisierte Straftatbestände schaffen. In dem Abkommen sind Vorgaben für konkrete Straftatbestände enthalten, die es auf nationaler Ebene zu schaffen gilt. Folgende Kategorien nennt die Cybercrime-Konvention:

(1) **Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen** (Kap. 1, Abschn. 1, Titel 1 Cybercrime-Konvention)

- Ausspähen und Abfangen von Daten, Datenveränderung, Computersabotage einschließlich Vorbereitungshandlungen, Infizierung von Computersystemen mit Schadsoftware, Datenspionage-Hacking, Phishing, Störung des Zugriffs auf Computersysteme, Herstellen, Verschaffen und Zugänglichmachen von Passwörtern, Sicherungscodes oder auf die Begehung von Straftaten abzielender Computerprogramme, hacking tools, crimeware

(2) **Computerbezogene Straftaten** (Kap. 1, Abschn. 1, Titel 2 Cybercrime-Konvention)

- betrügerische Angriffe auf das Vermögen, Betrug, Computerbetrug, bei denen im Einzelfall aber auch die missbräuchliche Verwendung der digitalen Identität eines anderen und damit der Tatbestand des Verfälschens und Gebrauchens beweiserheblicher Daten eine Rolle spielen kann. Außerdem geht es hier um Angriffe auf höchstpersönliche Rechtsgüter wie die Ehre, Cybermobbing, Cyberbullying.

(3) **Inhaltsbezogene Straftaten** (Kap. 1, Abschn. 1, Titel 3 Cybercrime-Konvention)

- Straftaten, bei denen über das Netz illegale Inhalte transportiert werden, also Informationen, mit denen der Umgang vom Gesetzgeber mit Strafe bedroht wird, z.B. Darstellung des sexuellen Missbrauchs von Kindern, Gewaltdarstellungen und Propagandadelikte

16) Stand: November 2019 – aktueller Stand abrufbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures – dort auch Überblick über die eventuellen nationale Vorbehalte.

ISBN 978-3-8011-0880-9

(4) **Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte** (Kap. 1, Abschn. 1, Titel 4 Cybercrime-Konvention)

- unerlaubte Verwertung urheberrechtlich geschützter Werke, unerlaubtes Verbreiten von Bildnissen, z.B. unbefugtes Herunterladen und Verbreiten von Musik, Filmen, Software mittels Filesharing-Systemen oder Peer to Peer-Netzwerken wie eMule oder BitTorrent

(5) Mittels Computersystemen begangene **Handlungen rassistischer und fremdenfeindlicher Art** (Zusatzprotokoll zur Cybercrime-Konvention v. 28.1.2003, sog. Antirassismus-Abkommen)[17)]

Derzeit wird ein weiteres Zusatzprotokoll zur Cybercrime-Konvention beraten, das den grenzüberschreitenden Zugriff der Strafverfolgungsbehörden auf Daten zum Gegenstand hat. Ein entsprechender Entwurf wird in Kürze erwartet.

Insbesondere Brasilien, China und Russland stehen dem Übereinkommen aus unterschiedlichen Gründen ablehnend gegenüber, was bedeutet, dass mehr als 50 Prozent des internationalen Internetverkehrs nicht erfasst werden.[18)]

2. Cybercrime

Vor dem Hintergrund internationaler sicherheitspolitischer Entwicklungen wurden der phänomenbezogene Sprachgebrauch harmonisiert und die Sachverhalte, die bislang unter den Terminus „IuK-Kriminalität" gefasst wurden, durch den Begriff „Cybercrime" ersetzt. Im **Bundeslagebild Cybercrime** des BKA (2017) wird dieser Deliktsbereich allgemein wie folgt definiert:

„Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden."[19)]

Es wird weiter zwischen **Cybercrime im engeren und im weiteren Sinne** differenziert: Neben spezifischen Angriffen auf informationstechnische Systeme (Angriffsobjekt = Daten), die mittels hierfür geschaffener Datendelikte sanktioniert werden (Cybercrime im engeren Sinne), wird auch die Nutzung derartiger Systeme zur Tatbegehung – sowohl als Tatmittel, wie auch als Angriffsmedium – erfasst (Cybercrime im weiteren Sinne).[20)]

a) Cybercrime im engeren Sinne

Zentrale Schutzgüter der unter Cybercrime im engeren Sinne gefassten Straftatbestände sind die Integrität und die Vertraulichkeit informationstechnischer Systeme.[21)]

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

Erscheinungsformen von Cybercrime im engeren Sinne sind vor allem:[22]

- Einsatz von Schadprogrammen, z.B. „Malware“ und Trojaner, als Tatmittel zum Angriff auf informationstechnische Systeme (unten **III. 6.**)
- Kriminelle Nutzung sogenannter „Botnetze“ (unten **III. 1.**)
- Überlastung von Servern („DDoS-Angriffe“, unten **III. 2.**) und
- unberechtigtes Eindringen in Rechnersysteme („Hacking“ unten **III. 3.**).

Cybercrime im engeren Sinne umfasst im Wesentlichen folgende **Delikte**:[23]

- Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB)
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB)
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB)
- Computerbetrug (§ 263a StGB)

Die Zuordnung einzelner Delikte zur Gruppe Cybercrime im engeren Sinne ist zum Teil strittig. So wird der Computerbetrug nach § 263a StGB auch zur Cybercrime im weiteren Sinne gezählt.[24]

Bei den aufgeführten Straftatbeständen ist eine zweigliedrige Regelungsstruktur erkennbar. Die §§ 202a ff. StGB pönalisieren den **Zugriff auf fremde Daten**, begonnen mit dem zweckgerichteten Vorhalten von Spähsoftware, bis hin zum mit dem Tatbestand der Datenhehlerei (§ 202d StGB) pönalisierten Ankauf widerrechtlich erlangter Daten. Regelungstechnisch getrennt hiervon steht das **Verändern von Daten** in den §§ 303a f. StGB. Dabei nimmt der Gesetzgeber sowohl den Persönlichkeitsrechtsschutz in den Blick, als auch die vermögensrechtliche Bedeutung von Daten.[25]

b) Cybercrime im weiteren Sinne

Während die Begehung der vorgenannten Delikte eine gewisse Technikaffinität voraussetzt, beschreibt der Terminus **Cybercrime im weiteren Sinne** die (traditionellen) Deliktsbereiche, bei denen informationstechnische Systeme zur Tatbegehung genutzt werden[26], also Straftaten, die im oder mit Hilfe des Internets begangen werden.

Es handelt sich um Straftatbestände, die regelmäßig auch im realen Raum verwirklicht werden können, wie Betrugsstraftaten, verbotenes Glücksspiel oder Verbreitung von sog. Kinderpornografie (korrekt: Darstellung des sexuellen Missbrauchs von Kindern).[27] Insbesondere sind folgende Straftatbestände relevant: Volksverhetzung (§ 130 StGB), Anleitungen zu Straftaten (§ 130a StGB), Gewaltdarstellung (§ 131 StGB), Verbreitung pornographischer Schriften (§ 184 StGB), Verbreitung gewalt- oder tierpornographischer Schriften (§ 184a StGB), Verbreitung, Erwerb und Besitz „kinderpornographischer“ Schriften (§ 184b StGB), Verbreitung, Erwerb und Besitz jugendpornographischer Schriften (§ 184c StGB), Ehrverletzungsdelikte (§§ 185 ff. StGB), Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB), Betrug (§ 263 StGB), Uner-

22) Wernert 2017, S. 29 f.

27) Clages/Zeitner 2016, S. 364.

ISBN 978-3-8011-0880-9

laubte Veranstaltung eines Glückspiels (§ 284 StGB) und die Beteiligung daran (§ 285 StGB).

3. Dokumentation von Cybercrime

In der **Polizeilichen Kriminalstatistik** (PKS) werden Cybercrime-Delikte in der Rubrik „Tatmittel" mit dem Schlagwort „Internet" erfasst:

Schlüsselzahl 516300	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN, § 263a StGB
Schlüsselzahl 517500	Computerbetrug, § 263a StGB
Schlüsselzahl 517902	Computerbetrug mit Zugangsberechtigungen zu Kommunikationsdiensten, §§ 263, 263a StGB
Schlüsselzahl 516502	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, §§ 253, 263a StGB
Schlüsselzahl 543000	Fälschung beweiserheblicher Daten, § 269 StGB
Schlüsselzahl 516502	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, §§ 253, 263a StGB
Schlüsselzahl 543000	Fälschung beweiserheblicher Daten, § 269 StGB
Schlüsselzahl 543001	Täuschung im Rechtsverkehr bei Datenverarbeitung, § 270 StGB
Schlüsselzahl 674200	Datenveränderung, Computersabotage, §§ 303a, 303b StGB
Schlüsselzahl 678000	Ausspähen von Daten, § 202a StGB
Schlüsselzahl 678020	Abfangen von Daten, § 202b StGB
Schlüsselzahl 678030	Vorbereitungshandlungen zu §§ 202a, 202b, 202c StGB
Schlüsselzahl 674200	Datenveränderung, § 303a StGB
Schlüsselzahl 674201	Computersabotage, § 303b StGB
Schlüsselzahl 715100	Softwarepiraterie (private Anwendung z.B. Computerspiele)
Schlüsselzahl 715200	Softwarepiraterie in Form gewerbsmäßigen Handelns.

Aus den Zahlen der PKS generiert das Bundeskriminalamt das „**Bundeslagebild Cybercrime**". Im Berichtszeitraum eines Jahres beschreibt das Lagebild das Gefahren- und Schadenspotenzial von Cybercrime und deren Bedeutung für die Kriminalitätslage in Deutschland.

Die Entwicklung der Cybercrime stellt sich 2018 danach wie folgt dar:[28)]

- 87.106 Fälle von Cybercrime im engeren Sinne (+1,3%)
- 271.864 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (4,9% aller in der PKS erfassten Straftaten)
- 723 Fälle von Phishing im Online-Banking (-49%)
- 60,7 Mio. Schaden im Bereich Computerbetrug (2017: 71,4 € Mio. Schaden)

28) Bundeskriminalamt (Hrsg.), Bundeslagebild Cybercrime 2018.

ISBN 978-3-8011-0880-9

– 13 OK-Gruppierungen im Kriminalitätsbereich Cybercrime[29]; 2,4% aller OK-Verfahren (2017: 17).

Zur Optimierung des Informationsaustauschs wurde 2011 das **Nationale Cyber-Abwehrzentrum** gegründet, das als Kooperationsplattform für staatliche und private Akteure fungiert und so die Bildung eines einheitlichen Lagebilds erleichtert. Der 2012 gegründete private **Cyber-Sicherheitsrat e.V.** versteht sich als Wissensplattform für private und staatliche Akteure; er berät auch das Nationale Cyber-Abwehrzentrum.[30]

Um aktuelle Erscheinungsformen der Internetkriminalität zu erkennen, wurden dem **Bundesamt für Sicherheit in der Informationstechnik (BSI)** weitgehende Aufgaben und Befugnisse eingeräumt. Als zentrale Meldestelle für die Sicherheit der Informationstechnik sammelt und analysiert das BSI Sicherheitslücken und neue Angriffsmuster auf die IT-Sicherheit. Dadurch können ein verlässliches Lagebild erstellt, kriminelle Angriffe frühzeitig festgestellt und wirksame Gegenmaßnahmen ergriffen werden.[31]

Die in München ansässige und dem Geschäftsbereich des BMI zugeordnete **Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)** soll ebenfalls einen Beitrag zur Bewältigung von Cybercrime leisten, indem sie die Sicherheitsbehörden des Bundes in diesen Bereichen unterstützt. ZITiS ist lediglich Forschungs- und Entwicklungsstelle und soll Expertisen in technischen Fragestellungen mit Cyberbezug für die Sicherheitsbehörden des BMI abdecken; die Behörde selbst hat keine Eingriffsbefugnisse. Die Aufgaben von ZITiS orientieren sich eng am Aufgabenspektrum der Sicherheitsbehörden, insbesondere in den Bereichen der digitalen Forensik, der Telekommunikationsüberwachung, der Kryptoanalyse (Dekryptierung), der Massendatenauswertung sowie der technischen Fragen von Kriminalitätsbekämpfung, Gefahrenabwehr und Spionageabwehr[32].

Wegen des hohen Gefahrenpotenzials von Angriffen auf die Sicherheit von Datensystemen bilden diese Kriminalitätsformen ein eigenes Themenfeld des **Programms Innere Sicherheit**.[33]

4. Dunkelfeldproblematik

Eine Einschätzung des Phänomens Cybercrime allein auf Basis statistischer Zahlen der PKS wird dessen Dimension nicht gerecht. So werden einzelne Deliktstypen, wie die vielfältigen Ausprägungen digitaler Erpressung, in der PKS nicht unter dem Begriff „Cybercrime“, sondern unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst (z.B. „Erpressung“, wenn es um Ransomware geht).[34]

29) Dazu insbesondere Goertz, Der Kriminalist 4/2018, 15 ff.

30) Dreimann, Die Polizei 2017, 135 (141).

31) Hierzu Wirth, in: Wirth 2013, S. 313 f. (IuK-Kriminalität).

32) https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/01/zitis-vorstellung.html.

33) Das Programm Innere Sicherheit ist ein Grundsatzdokument für die Gewährleistung der inneren Sicherheit in der Bundesrepublik Deutschland mit strategischen Aufgaben für die Polizei und andere Sicherheitsbehörden. Es wurde 1972 von der Innenministerkonferenz mit der Zielsetzung einer Stärkung und bundesweiten Angleichung der Polizeiarbeit verabschiedet.

34) Seidl, in: Albrecht 2018, Rn. 835.

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime“, 1. Auflage 2020
ISBN 978-3-8011-0880-9

Auch im Übrigen bildet die PKS die Realität nur unzureichend ab. So gehen Taten, die vom Ausland aus verübt werden oder bei denen Täter einen Server im Ausland nutzen, nicht in die Kriminalstatistik ein. Zudem wird durch die Erfassungsmodalitäten der PKS lediglich das **Hellfeld** von Inlandstaten abgebildet[35]. Das **Dunkelfeld** mit schätzungsweise 91 % ist aber so groß, dass basierend auf PKS-Erkenntnissen belastbare Aussagen zur Cybercrime-Entwicklung nicht möglich sind.[36] Dies bedeutet auf einzelne Deliktsbereiche bezogen, dass die vorliegenden statistischen Zahlen mit dem Faktor 11 multipliziert werden müssten, um ein annähernd realistisches Bild der Cybercrime in Deutschland zu beschreiben.[37]

In Anbetracht der überdurchschnittlich großen Anzahl von Cybercrime-Straftaten, die bei der Polizei nicht zur Anzeige gebracht werden, werden zur umfassenden Einschätzung des Gefahrenpotenzials von Cybercrime auch nichtpolizeiliche Informationsquellen einbezogen. Diese umfassen Studien von Forschungseinrichtungen oder von behördlichen Einrichtungen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch solche von privaten Verbänden und Firmen, wie z.B. Antivirensoftware-Herstellern und IT-Sicherheitsdienstleistern.[38]

Ein Teil des Hellfeldes klassischer Kriminalitätsformen ist in das Dunkelfeld moderner Computerkriminalitätsdelikte übergegangen.[39]

III. Phänomene

1. Botnetze und Cybercrime as a service

Botnetze[40] sind Verbünde von mit einer Schadsoftware infizierten („gekaperten") Rechnern, die von einem zentralen „Command & Control-Server" ferngesteuert werden.[41] Die eigentlichen Nutzer der infizierten Systeme bemerken die Manipulation regelmäßig nicht. Ziel des Aufbaus eines Botnetzes ist es, die Rechenleistung und Bandbreite einer Vielzahl von Rechnern und Internetzugängen kombiniert bzw. gebündelt zu nutzen.[42]

35) Zu Hell- und Dunkelfeld Kunz/Singelnstein 2016, § 15 Rn. 6.

36) Dreimann, Die Polizei 2017, 135 (140).

37) Clages/Zeitner 2016, S. 365.

38) Bundeskriminalamt (Hrsg.), Bundeslagebild 2017: Cybercrime, S. 2.

39) Zu dieser Schlussfolgerung kommt die Dunkelfelduntersuchung der Polizei des Landes Mecklenburg-Vorpommern im Rahmen des Forschungsberichts 2018. Dabei gehen die Autoren davon aus, dass diese Situation auch ein Grund für die sich seit Jahren positiv entwickelnden Hellfeldzahlen der polizeilichen Kriminalstatistiken sein könnte. Es ist in der Wissenschaft mittlerweile weitestgehend anerkannt, dass es bei allen digitalen Delikten eine wesentlich höhere Dunkelzifferrelation gibt als bei rein analogen Delikten, Rüdiger, Moderne Polizei 3/2019, 27.

40) Engl. robot = Roboter, wiederum von tschechisch Robota = Arbeit.

41) Eckert 2012, S. 77 ff.

42) Ähnlich funktioniert – jedoch mit Zustimmung des jeweiligen Computernutzers – das sog. „**Volunteer Computing**", bei dem durch das Herunterladen und Ausführen eines Computerprogramms die Rechenleistung des eigenen Computers anderen zur Verfügung gestellt wird. Ein Beispiel hierfür ist das Projekt „SETI@home" (Search for Extra-Terrestrial Intelligence at home) der Universität Berkeley, dass auf diese Weise bei der Suche nach außerirdischer Intelligenz unterstützt werden kann.

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

Beispiel:[43] Im Oktober 2016 kam es unter Beteiligung des Botnetzes „Mirai“ zu großangelegten DDoS-Angriffen. Das Botnetz „Mirai“ nutzte es aus, dass Alltagsgegenstände wie Router, Überwachungssysteme, Fernseher oder Kühlschränke mit dem Internet verbunden sind (**IoT = Internet of Things**). Die Software scannte über das Internet derartige Geräte auf Sicherheitslücken und infizierte diese dann mittels eines Schadcodes. Das ursprüngliche Botnetz „Mirai“ umfasste 2016 rund 500.000 kompromittierte „Internet of Things“-Geräte weltweit, zwischenzeitlich waren bis zu drei Millionen Geräte in das Botnetz eingebunden.

Botnetze stellen eine der wichtigsten Täterinfrastrukturen im Bereich der Cyberkriminalität dar. Neben der Durchführung von „Denial of Service“-Angriffen (dazu **2.**) ist eine Vielzahl anderer Einsatzmöglichkeiten denkbar. Botnetze können etwa zum massenhaften Versand von Spam- und Phishing-Mails oder zur Verschleierung des Standortes von Servern mit kriminellen Inhalten genutzt werden. In einem vom BGH entschiedenen Fall[44] wurde ein Botnetz verwendet, um mit Hilfe der kombinierten Rechenleistung der gekaperten Rechner Bitcoins zu erzeugen.

Die für die Fernsteuerung des Botnetzes erforderlichen Bot-Programme werden im Wesentlichen über folgende drei Wege verbreitet und auf die Zielrechner geschleust:

- mittels eines **Trojaners** (der durch Öffnen eines infizierten E-Mail-Anhangs installiert wird),
- mittels eines **Drive-by-Downloads** (unbeabsichtigtes Herunterladen von Schadsoftware durch das bloße Aufrufen einer dafür präparierten Webseite; dabei werden Sicherheitslücken eines Browsers ausgenutzt),
- mittels eines gezielten Angriffs auf den betroffenen Rechner (**Advanced Persistent Threat** – APT – dt. „fortgeschrittene andauernde Bedrohung“), wobei letztere aufgrund des wesentlich höheren Aufwands deutlich seltener zu beobachten ist.[45]

Die Möglichkeit, auch als nicht informationstechnisch versierte Person auf anonymen Marktplätzen im Internet die Bereitstellung von Botnetzen als „Dienstleistung“ (**crime as a service**) zu vereinbaren, soll in den vergangenen Jahren zu einer merklichen Erhöhung der Zahl der potenziellen Täter geführt haben.[46]

Die Installation von Bot-Programmen auf fremden IT-Systemen ist eine Datenveränderung im Sinne des § 303a StGB. Eine Strafbarkeit nach § 202a StGB (Ausspähen von Daten) scheitert in der Regel am Fehlen einer besonderen Zugangssicherung.[47] Eine Tatbestandsqualifikation besteht, wenn eine Variante des § 303b Abs. 4 StGB (Computersabotage) einschlägig ist: Herbeiführen eines Vermögensverlustes von großem Ausmaß (Abs. 4 Nr. 1), gewerbsmäßiges Handeln oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat (Nr. 2) oder Beeinträchtigung der Versorgung der

43) Bundeskriminalamt (Hrsg.), Bundeslagebild 2016: Cybercrime, S. 15.

44) BGH, NStZ 2016, 339.

45) Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Die Lage der IT-Sicherheit in Deutschland 2016, 2016, S. 22 ff.

46) Goertz, Deutsche Polizei 5/2017, 5 (7); Henzler, Der Kriminalist 10/2015, 25 (26).

47) Stam, ZIS 2017, 547 (552).

ISBN 978-3-8011-0880-9

Bevölkerung mit lebenswichtigen Gütern/Dienstleistungen oder der Sicherheit der Bundesrepublik Deutschland (Nr. 3).[48]

2. DDoS-Angriffe

Denial-of-Service[49] (DoS)-Angriffe (dt. etwa „Dienstverweigerungsangriff") richten sich gegen die Verfügbarkeit von Internet-Diensten, Webseiten oder ganzen Netzen mit dem Ziel, diese zusammenbrechen oder zumindest unerreichbar werden zu lassen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen durch die soeben beschriebenen Botnetze.[50] Dabei werden die angegriffenen Systeme von den gekaperten Systemen des Bot-Netzwerkes mit Anfragen und riesigen Datenmengen regelrecht bombardiert. Das führt – vereinfacht ausgedrückt – zu einer Überlastung und damit zu einer Unerreichbarkeit für reguläre Nutzer. Auf diese Weise wurde z.B. das BKA-Hinweisportal zum Anschlag auf den Berliner Weihnachtsmarkt durch einen DDoS-Angriff lahmgelegt.[51] Hauptangriffsziele der Cyberkriminellen sind indes der Finanzsektor, der Einzelhandel und der Kommunikationssektor.[52]

Beispiel:[53] Eine international agierende Gruppe erpresste Unternehmen mit der Androhung und Durchführung von DDoS-Angriffen. Die DDoS-Angriffe dauerten jeweils bis zu 60 Minuten. Im Anschluss erhielten die Betroffenen ein Schreiben der Erpresser. Gefordert wurde jeweils ein Betrag (10.000 €) in der digitalen Währung Bitcoin. Bei Nichtzahlung wurde ein weiterer Angriff angedroht.

Der wirtschaftliche Schaden, der angegriffenen Unternehmen durch die verursachten Systemausfälle entstehen kann, ist enorm. Die Auswirkungen für die Bevölkerung können dramatisch sein, wenn erfolgreich mit dem Internet verbundene kritische Infrastrukturen betroffen sein sollten, wie große Industrieanlagen, Elektrizitätswerke, Telekommunikationsanlagen, Krankenhäuser oder Anlagen der Wasserversorgung.

Bei DoS-Attacken sind regelmäßig die Straftatbestände in § 303a (Datenveränderung) und 303b StGB (Computersabotage) einschlägig.[54]

Zu Zwecken der Bekämpfung von DDoS-Angriffen/Botnetzkriminalität kommen teils sog. **Honeypots** zum Einsatz. Als Honeypots werden absichtlich gelegte Fallen in Form von nicht abgesicherten Systemen bezeichnet, um Angreifer anzulocken.[55] Ein Honeypot kann dann zur Analyse des Angreifverhaltens, Angriffsmusters und der möglichen Motive beitragen. Da Honeypots jedoch selbst Bestandteil des Angriffs werden, stellt sich die Frage nach der Strafbarkeit des

48) Hirsch, in: Clages/Ackermann 2019, S. 673.

49) Denial of Service (DoS) bedeutet in etwa: „außer Betrieb setzen" bzw. „etwas unzugänglich machen".

50) Bundeskriminalamt (Hrsg.), Bundeslagebild 2016, S. 5.

51) Vogelgesang/Möllers/Potel, MMR 2017, 291.

52) Im November 2016 hat eine solche Attacke zu einer Großstörung bei der Telekom und zu einem Ausfall von 900.000 Anschlüssen geführt.

53) Meywirth, Die Polizei 2016, 185 (186); Münch, Kriminalistik 2019, 11 f.

54) Ausführlich zur strafrechtlichen Beurteilung von DDoS-Attacken Nemzov 2017, S. 65 ff.

55) Grützner/Jakob, „Honeypot".

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

Betreibers (Beihilfe zur Computersabotage, §§ 303b Abs. 1 Nr. 2, 27 StGB); teilweise wird eine solche bejaht.[56)]

3. Hacking

Unter dem Begriff des **Hacking** wird landläufig[57)] das unberechtigte Eindringen in ein fremdes informationstechnisches System bzw. ein Netzwerk solcher Systeme verstanden. Die Methoden des Hackings[58)] sind ebenso vielfältig wie die Ziele: täuschen, betrügen, sabotieren oder Informationsdiebstahl. Mitunter ist die Motivation des Hackers auch „lediglich" die Erkundung der Grenzen des Machbaren[59)].

Beispiel: Anfang Dezember 2018 wurden auf einem Twitter-Account Links zu gehackten Datensätzen mit privaten Informationen von Politikern, Prominenten und Journalisten veröffentlicht. Die Daten umfassten Kontaktdaten, Chatverläufe und private Bilder. Auf dem Twitter-Account „@_0rbit" wurden vom 1. bis 28.12.2018 täglich in Form eines Adventskalenders kurze Tweets mit Links zu den gestohlenen Daten der betroffenen Personen veröffentlicht. Die Links führten zu anonymen Portalen wie „PrivateBin" und von dort zu weiteren anonymen Seiten, auf denen die sensiblen Informationen abrufbar waren. Teilweise wurden die Daten auf bis zu sieben Servern parallel bereitgestellt, damit sie möglichst lange verfügbar bleiben. Die auf Twitter geteilten Links und die Daten blieben zunächst über Wochen von der breiten Öffentlichkeit unbemerkt. Erst als der Hacker Anfang Januar 2019 auch den Twitter-Account von dem deutschen YouTuber Simon Unge unter seine Kontrolle brachte und dort die Links mit den etwa 2 Mio. Followern erneut teilte, gelangte die Aktion in den Fokus der Öffentlichkeit.[60)]

Als Straftatbestände kommen beim Hacking in Betracht:[61)]

§ 202a StGB:	Ausspähen von Daten
§ 202b StGB:	Abfangen von Daten
§ 42 BDSG:[62)]	Datenschutzvergehen
§ 303a StGB:	Datenveränderung
§ 303b StGB:	Computersabotage (Abs. 1); schwere Computersabotage (Abs. 2)
§ 317 StGB:	Störung von Anlagen (Abs. 1); strafbare Fahrlässigkeit (Abs. 3)

Nach § 202c StGB sind auch Vorbereitungshandlungen zum Hacking strafbar. So ist das Herstellen, Verkaufen usw. von **„Hacker-Tools"** pönalisiert. Darunter fallen aber keine Programme, die auch zu legalen Zwecken genutzt werden können (sog. **Dual-Use-Tools**, dazu **B. III. 1.**)

4. Seitenkanalangriffe

Um vertrauliche Informationen aus PCs oder Smartphones zu gewinnen, muss deren Integrität nicht zwingend verletzt werden. Rückschlüsse auf verarbeitete

62) Die Vorschrift enthält in ihren ersten beiden Absätzen Strafvorschriften, durch die der nationale Gesetzgeber seinem Auftrag gerecht wird, der sich aus Art. 84 Abs. 1 DSGVO ergibt, Ehmann, in: Gola/Heckmann 2019, § 42 Rn. 1.

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9

Daten und sonstige Informationen können auch aus für sich genommen legitim verfügbaren Einblicken in Systemvorgänge – den sogenannten Seitenkanälen (deswegen auch „**Seitenkanalangriffe**“[63]) – gewonnen werden. So können aus dem Verhalten einer bestimmten (Hardware-/Software-)Implementierung (z.B. Stromverbrauch, akustische und mechanische Schwingungen, Zeitabstände usw.) weitreichende und treffgenaue spekulative Folgerungen auf die verarbeiteten Daten gezogen werden. Seitenkanalangriffe werden als ernsthaftes Sicherheitsproblem angesehen.[64]

Beispiel: Der Energieverbrauch eines Mikroprozessors während kryptographischer Berechnungen variiert abhängig von den jeweils ausgeführten Prozessen. Wird der Energieverbrauch im Wege eines „Seitenkanalangriffs“ aufgezeichnet, können Rückschlüsse auf die Rechenoperation und damit über den Schlüssel gezogen werden.

Nach § 202b Alt. 2 StGB ist nur das Abfangen von Daten mittels der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage strafbar. Das Ausnutzen anderer Seitenkanäle ist dagegen nicht explizit pönalisiert. In solchen Fällen wird aber eine Strafbarkeit nach §§ 202a Abs. 1, 303a Abs. 1 StGB in Erwägung gezogen.[65]

5. Strafbares Verhalten von Chatbots/Socialbots

a) Chatbots

Der Begriff „Chatbot“ ist eine Kombination aus dem englischen Verb to chat, plaudern, und der Kurzversion des Begriffs robot. Mit Chatbots soll sich der Nutzer wie mit einem Menschen "unterhalten" können. Dabei erfolgt die Kommunikation (derzeit) hauptsächlich über Texteingabe. Der Chatbot versucht zu erkennen, was und worüber das menschliche Gegenüber "chatten" möchte und gibt entsprechend "passende" Antworten.

Die automatisierte Übernahme von Kommunikationsaufgaben als Form „künstlicher Intelligenz“ basiert auf komplexen Algorithmen, die Routinen abarbeiten und setzt regelmäßig voraus, dass das eingesetzte System „selbstlernend“ konfiguriert wird, d.h. mit entsprechenden Informationen „gefüttert“ wird. Dies kann strafrechtliche Fragen aufwerfen. Etwa dann, wenn die vom Betreiber des Bots selektierte Zielgruppe strafbewährte Aussagen trifft und der selbstlernende Chatbot diese zur Inhaltsgenerierung nutzt.

63) Hierzu Brodowski, ZIS 2019, 49 ff.

64) FAZ v. 4.1.2018, „Computerchips sind doppelt unsicher“, http://www.faz.net/-ikh-95hyn.

65) Brodowski, ZIS 2019, 49 (61).

ISBN 978-3-8011-0880-9

Beispiel:[66] Der von Microsoft entwickelte Chatbot „Tay", sollte auf Twitter „lernen, wie junge Menschen reden". Auf die zuvor geführten Konversationen mit Nutzern aufbauend sendete der Chatbot binnen weniger Stunden volksverhetzende Inhalte und musste zwangsabgeschaltet werden.

In diesen Fällen kann die strafbare Äußerung nicht den Nutzern des Chatbots zugerechnet werden.[67] Wohl kommt aber eine Strafbarkeit des Betreibers in Betracht, der sich die strafbaren „fremden Inhalte" durch Betrieb des Chatbots erkennbar zu Eigen gemacht hat.[68]

b) Socialbots

Socialbots sind (autonom agierende) Computerprogramme, die in sozialen Netzwerken (vor allem bei Facebook und Twitter) menschliches Nutzerverhalten imitieren und mittels sog. Fake-Accounts vortäuschen, reale Menschen zu sein. Für Außenstehende sind sie kaum als Bots zu identifizieren.[69] Im Rahmen des US-Wahlkampfs im Jahr 2016 wurde erstmals das Phänomen des Einsatzes von Socialbots einer breiteren Öffentlichkeit bekannt; fast 20 Prozent aller Tweets im US-Präsidentschaftswahlkampf wurden durch diese verbreitet.[70]

Durch die Masse an (teils unzutreffenden) Inhalten, die von Socialbots erzeugt werden können, kann gezielt auf die öffentliche Meinungsbildung eingewirkt werden[71]. Nicht jeder Einsatz von Socialbots hat aber ideologische Hintergründe. Gerade auch wirtschaftliche Erwägungen spielen eine Rolle bei der künstlichen Generierung von „trending topic". Das Kauf- und Kundenverhalten und ganze Märkte (man denke an Falschmeldungen zur Manipulation von Aktienmärkten) können durch Socialbots beeinflusst werden.[72] In diesen Fällen greifen häufig Straftatbestände aus dem Wirtschaftsstrafrecht und dem UWG.

Von besonderer Relevanz ist die Verbreitung strafbarer Inhalte. So werden über Socialbots häufig auch Hasspostings, terroristische Ideologien und „Fake News"[73] gepostet[74].

So benutzt die Terrorgruppe Daesh (ISIS) Socialbots. Vermutungen nach handele es sich um ein paar tausend, die von Daesh bei Twitter eingesetzt werden. Untersuchungen zufolge liegt der Output der im Dienst von Daesh stehenden Bots bei ca. 26.000 Nachrichten am Tag.[75]

Der Einsatz von Socialbots ist nicht gesetzlich verboten, stellt aber stets einen Verstoß gegen die Allgemeinen Nutzungsbedingungen der führenden sozialen Netzwerke dar.[76]

Eine Strafbarkeit der Verwendung von Socialbots kommt im Hinblick auf § 303a Abs. 1 StGB und § 303b Abs. 1, Abs. 2 StGB in Betracht. Je nachdem, welchen Inhalt die einzelnen Posts haben und in welchem Kontext sie erfolgen, können eine Strafbarkeit im Zusammenhang mit Wahlen (§§ 107 ff. StGB) begründet sein oder Beleidigungsdelikte (§§ 185 ff. StGB) bzw. Volksverhetzung (§ 130 StGB) verwirklicht werden.[77]

66) https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch.

76) Zur verfassungsrechtlichen und einfachgesetzlichen Einordnung von Social Bots Dankert/Dreyer, K&R 2017, 73 ff.

77) Hierzu Libertus, ZUM 2018, 20 (21 ff.).

ISBN 978-3-8011-0880-9

6. Malware/Ransomware/Scareware

Schadsoftware (**Malware** – malicious software) ist eine vom Anwender unerwünschte und oft unbewusst installierte Software. Sie ermöglicht den „Diebstahl" und die Manipulation von Daten auf dem infiltrierten Zielsystem, etwa mittels **Keylogging** (Mitlesen jeglicher Tastatureingaben), **Sniffing** (Mitlesen der Kommunikation, z.B. E-Mails), **Man-in-the-Browser-Anwendungen** (Mitlesen und Manipulation der Ein- und Ausgaben eines Browsers) oder **Camfecting** (Webcam-Hack).[78] Gemeinsam ist allen Funktionalitäten, dass sie von einem Angreifer aus der Ferne gesteuert werden können.

Einen großen Teil der Schadsoftware machen Spionageprogramme aus (Sniffer, Keylogger usw.), die Zugriff auf kritische Informationen (z.B. Passwörter, andere sensitive Daten) ermöglichen.[79] Diese Schadprogramme werden häufig mittels sog. Trojaner auf den Zielsystemen installiert. Auch die heimliche Installation von sog. „Backdoor" (Hintertür)-Programmen ist nicht unüblich. Durch diese kann das Zielsystem unbemerkt über das Internet ferngesteuert werden und als Teil eines Botnetzwerkes für DDoS-Attacken missbraucht werden.

Beispiel „Rücküberweisungstrojaner"[80]: Ein solcher Trojaner manipuliert die dem Kunden via Online-Banking in seinem Browser angezeigten Umsätze und spiegelt ihm vor, er habe einen hohen Zahlungseingang erhalten. Gleichzeitig wird der Kunde darauf hingewiesen, dass es sich bei der fiktiven Überweisung um einen Irrläufer handeln würde und um Rücküberweisung gebeten. Auch nach erfolgter Rücküberweisung wird der Kontostand weiterhin manipuliert, sodass der Kunde über einen längeren Zeitraum keine Kenntnis von dem Betrug hat.

Unter der Bezeichnung **Ransomware** (dt. „Erpressungssoftware") werden Schadprogramme verstanden, die dem Nutzer den Zugriff auf sein System unmöglich machen. Der Nutzer wird zur Zahlung eines „Lösegeldes" aufgefordert, möchte er wieder auf seine Daten zugreifen. Ransomware ist häufig im Anhang einer Spammail versteckt und wird durch Anklicken des Anhangs durch den Nutzer installiert. Ebenfalls verbreitet ist die Installation im Rahmen so genannter „Drive-by-Downloads", also im Zusammenhang mit dem Aufruf einer entsprechenden, Sicherheitslücken des Zielsystems ausnutzenden Webseite.[81]

Ein prominentes Opfer des Krypto-Trojaners „Locky" war ein Krankenhaus in Neuss. Nach der Infektion mit dem Virus war das Krankenhaus nur eingeschränkt funktionsfähig. Geplante Operationen mussten verschoben werden. Nach Angaben der Krankenhausverwaltung entstand durch die notwendige Umorganisation im Krankenhaus sowie die Datenwiederherstellung ein Schaden von ca. 750.000 Euro.[82]

78) Rossow/Sorge, JM 2018, 7 (8).

79) Rossow/Sorge, JM 2018, 7 (8).

80) Schulte am Hülse/Kraus MMR 2016, 435 (436).

81) Hirsch, in: Clages/Ackermann 2019, S. 666.

82) http://www.spiegel.de/netzwelt/web/locky-teslacrypt-cryptolocker-co-zahlensie-nicht-a-1082315.html: „Flut von Erpresser-Viren – Zahlen Sie nicht!" [9.10.2019].

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime", 1. Auflage 2020
ISBN 978-3-8011-0880-9