Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2018

Cybercrime in Zahlen 2018

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 Onlinebanking (-49 %)

60,7 Mio. Euro Schaden im Bereich Computerbetrug (2017: 71,4 Mio. Euro)

13 Gruppierungen und damit 2,4 % aller Verfahren der Organisierten Kriminalität im Kriminalitätsbereich Cybercrime (2017: 17)

Inhaltsverzeichnis

Gender-Hinweis:
Aus Gründen der besseren Lesbarkeit wird in diesem Lagebild das generische Maskulinum verwendet.

1 Vorbemerkung

Grundlage für den statistischen Teil des Bundeslagebilds Cybercrime sind die Daten der Polizeilichen Kriminalstatistik (PKS). Das polizeiliche Hellfeld umfasst alle Straftaten, einschließlich der mit Strafe bewehrten Versuche, die polizeilich bearbeitet und an eine Staatsanwaltschaft abgegeben wurden. Aus den zwischenzeitlich geänderten Erfassungsmodalitäten für das Delikt Computerbetrug resultiert eine eingeschränkte Vergleichbarkeit der Zahlen ab 2016 mit denen der Vorjahre. Die Aussagen im vorliegenden Lagebild beruhen darüber hinaus auf Erkenntnissen aus dem kriminalpolizeilichen Informationsaustausch.

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

So wurde die Kooperation des Bundeskriminalamts (BKA) mit dem „German Competence Centre against Cyber Crime e. V.“ (G4C)[1] bei der diesjährigen Lagebilderstellung noch intensiver genutzt.

Die auf diesem Weg gewonnenen Informationen ergänzen das polizeiliche Hellfeld und ermöglichen eine quantitativ und qualitativ verbesserte Lagebewertung.

[1] G4C-Mitglieder: Commerzbank, ING-DiBa, HypoVereinsbank, Kreditanstalt für Wiederaufbau, Schufa, Bank-Verlag, R+V, Symantec, Diebold Nixdorf, Link11, G-Data; G4C-Kooperationspartner: BKA und BSI.

2 Darstellung und Bewertung der Kriminalitätslage

2.1 ERFASSUNGSMODALITÄTEN DER POLIZEILICHEN KRIMINALSTATISTIK

Cybercrime als Phänomen unterscheidet die Bereiche Cybercrime im engeren Sinne (CCieS) und im weiteren Sinne (CCiwS). Eine derartige Unterscheidung erfolgte bereits im Jahr 2000 auf dem 10. Kongress der UN zum Thema „Prevention of Crime and the Treatment of Offenders“ und wird seitdem international mit individuellen Abwandlungen insbesondere auf juristischer und polizeilicher Ebene genutzt.[2]

Der Deliktsbereich CCieS umfasst die Straftaten, die sich gegen das Internet[3], weitere Datennetze[4], informationstechnische Systeme[5] oder deren Daten richten. Im Einzelnen fallen hierunter folgende Tatbestände des Strafgesetzbuches:

- **Computerbetrug als Cybercrime im engeren Sinne** (§ 263a StGB)
  Dieses Delikt wird seit 01.01.2016 in der PKS in folgende Betrugsarten aufgeschlüsselt:
  - Betrügerisches Erlangen von Kraftfahrzeugen gem. § 263a StGB,
  - weitere Arten des Kreditbetruges gem. § 263a StGB,
  - Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB,
  - Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB,
  - Leistungskreditbetrug gem. § 263a StGB,
  - Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB,
  - Überweisungsbetrug gem. § 263a StGB.
- **Sonstiger Computerbetrug** (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB, soweit nicht unter die nachfolgenden Betrugsarten bzw. die „Missbräuchliche Nutzung von Telekommunikationsdiensten“ gefasst).

[2] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Crimes related to Computer networks, abrufbar unter: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf, S. 5.
[3] Technisch gesehen umfasst das Internet zum Beispiel folgende Dienste: WWW (Webseiten, Soziale Netzwerke, Online-Shops), E-Mail (elektronische Post), News („schwarze Bretter“ im Internet), Datenaustausch (FTP, File-Sharing, usw.), Chat (Echtzeitkommunikation über die Tastatur), Cloud Services.
[4] Hierunter fallen alle Netze, die nicht Teil des Internets sind, z. B. Intranet, Bluetooth, Cross-Connect-Verbindung zwischen zwei Endsystemen.
[5] Hierbei handelt es sich um ein in sich geschlossenes, keinem Netzwerk angehörendes IT-Gerät. Dies ist z. B. ein Stand-Alone-PC oder USB-Stick.

- **Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Daten-Hehlerei** (§§ 202a, 202b, 202c, 202d StGB) umfasst den Diebstahl und die Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden in der Regel als Handelsware auf digitalen Schwarzmärkten[6] zum Kauf angeboten und täterseitig missbräuchlich eingesetzt. Die Verwertung erfolgt damit in zwei Stufen: dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

- **Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr** (§§ 269, 270 StGB) – Diese Tatbestände beinhalten die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z. B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen. Unter Vortäuschung einer Legende soll der Geschädigte z. B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

- **Datenveränderung/Computersabotage** (§§ 303a, 303b StGB) – Hierbei handelt es sich um eine Art digitaler Sachbeschädigung. Es wird die Veränderung von Daten in einem Datenverarbeitungssystem bzw. das Verändern des Systems durch andere als den Dateninhaber unter Strafe gestellt. Die §§ 303a, 303b StGB umfassen typischerweise Denial of Service-Angriffe (DoS-/DDoS-Angriffe[7]), ebenso wie die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojaner, Viren, Würmer usw.).

- **Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB)** – Dies ist eine besondere, separat erfasste Form des Computerbetrugs gem. § 263a StGB. Unter Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen werden sowohl bei Firmen als auch Privathaushalten, z. B. durch den unberechtigten Zugriff auf Router, teure Auslandstelefonverbindungen angewählt oder gezielt Premium- bzw. Mehrwertdienste in Anspruch genommen.

Das Bundeslagebild Cybercrime 2018 informiert hauptsächlich über die polizeilich bekannt gewordenen Entwicklungen von CCieS.

Allerdings enthält das Bundeslagebild Cybercrime auch Ausführungen zum Bereich CCiwS, u. a. statistische Daten zum Tatmittel Internet (s. Kapitel 2.4) oder der detaillierten Beschreibung des Bereichs Digitale Marktplätze (s. Kapitel 3.8). Unter CCiwS werden jene Straftaten zusammengefasst, bei denen Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung genutzt wurde.

Bei der Betrachtung von polizeilich erfassten statistischen Daten müssen die besonderen Erfassungs- bzw. Zählmodalitäten in der PKS berücksichtigt werden. So ist bei der Interpretation der Statistik zu beachten, dass z. B. einzelne relevante Phänomene, wie Erpressungshandlungen

[6] Online-Schwarzmärkte, oft im Darknet, über die Anbieter und Käufer ihre kriminellen Geschäfte rund um die digitale Welt anbahnen und abwickeln können. Auch „Underground Economy-Plattformen", „Darknet-Markets" oder „Darknet-Märkte".

[7] Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. 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 häufig durch eine sehr große Anzahl von Computern oder Servern, die ein Botnetz bilden.

im Zusammenhang mit gezielten DDoS-Attacken oder auch mit Ransomware[8], in der PKS in der Regel nicht als Cybercrime-Delikt, sondern als schwerwiegendere bzw. speziellere Tat, in diesem Fall als Erpressung, erfasst werden.

Trotz der eingeschränkten Aussagekraft der PKS hinsichtlich der Gesamtheit der in Deutschland verübten Cybercrime-Straftaten ist festzuhalten, dass es sich um die einzige bundesweite statistische Datenquelle handelt, die auf polizeilichen Ermittlungen basiert. Sie liefert somit eine Datenbasis, auf deren Grundlage in diesem Phänomenbereich zumindest Trendaussagen getroffen werden können.

Aussagen zur tatsächlichen Kriminalitätsbelastung lassen sich alleine auf Grundlage der PKS nicht treffen, da die Anzahl der tatsächlich begangenen, nicht polizeilich bekannt gewordenen bzw. erfassten Straftaten um ein Vielfaches höher liegen dürfte. Gründe hierfür liegen zum einen in den dargestellten Erfassungsmodalitäten, zum anderen weisen die nachfolgend aufgeführten – für das Deliktsfeld z. T. spezifischen – Punkte auf ein hohes Dunkelfeld im Bereich Cybercrime hin:

- Eine große Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinaus und wird von den Geschädigten nicht bemerkt,

- Die betroffenen Personen erkennen nicht, dass sie Geschädigte einer Cyber-Straftat geworden sind (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop) bzw. von ihnen eingesetzte technische Geräte unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht wurden (z. B. Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen oder Infektion mit Cryptomining-Malware),

- Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z. B. Versicherung) reguliert wird,

- Geschädigte, insbesondere Firmen, zeigen erkannte Straftaten nicht an, um bspw. die Reputation als „sicherer und zuverlässiger Partner“ im Kundenkreis nicht zu verlieren.

- Geschädigte erstatten z. B. in Erpressungsfällen oftmals nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.

Die Polizei weist immer wieder auf die Notwendigkeit der Anzeige entsprechender Cybercrime-Straftaten durch die Geschädigten hin, da sich hieraus nicht nur neue Ermittlungsansätze für eine effektivere Bekämpfung ergeben können (durch z. B. Analyse der Angriffsvektoren oder Feststellung von Tatzusammenhängen), sondern auch nur so eine Täterfeststellung und -verfolgung möglich ist. Ziel muss es sein, die Urheber für Cyber-Angriffe zu identifizieren und weitere Angriffe zu unterbinden. Die nur durch Bekanntwerden entsprechender Sachverhalte mögliche Sanktionierung kriminellen Verhaltens könnte hierbei auch abschreckende Wirkung auf potenzielle Täter haben.

[8] Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung einzelner Daten oder des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld („ransom“) zu erpressen.

2.2 FALLZAHLEN CYBERCRIME

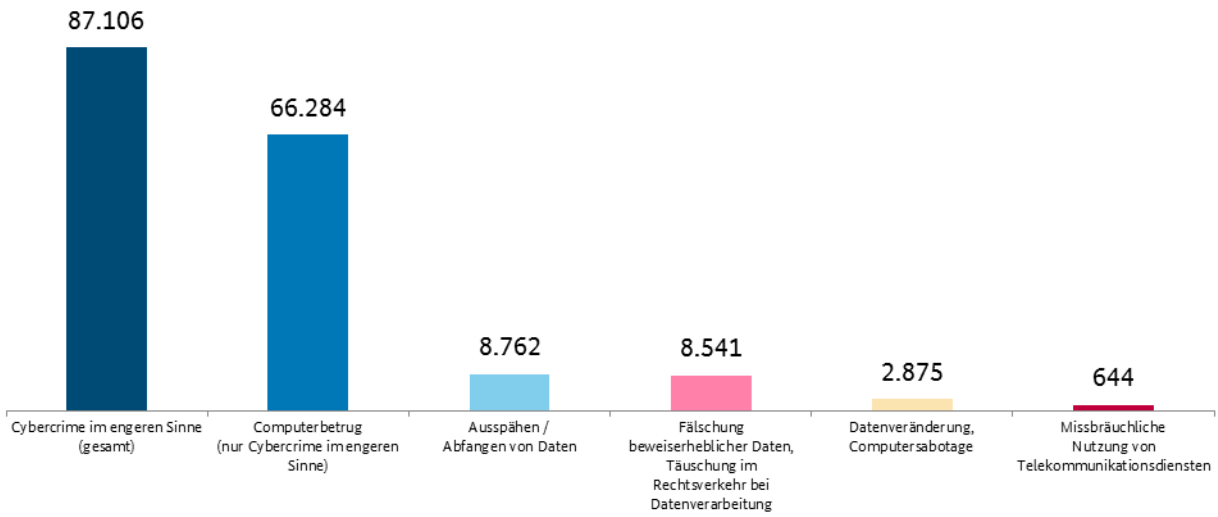
Im Jahr 2018 war ein erneuter Anstieg der Straftaten von CCieS zu verzeichnen. Die PKS wies insgesamt 87.106 Fälle aus. Dies bedeutet eine Steigerung gegenüber dem Vorjahr um 1,3 % (2017: 85.960 Fälle). Die Aufklärungsquote betrug 38,9 %, was einem Rückgang gegenüber dem Vorjahr um 1,4 Prozentpunkte entspricht.

Drei Viertel aller Straftaten wurden als Fälle von Computerbetrug registriert. Für das Jahr 2018 wurde in diesem Deliktsfeld ein Anstieg von 3,7 % verzeichnet. In den meisten Fällen wurden hierunter Sachverhalte erfasst, bei denen das Internet lediglich als Tatmittel fungierte.[9]
Sie stellen damit keine CCieS dar. Auch aus diesem Grund sind die Fallzahlen der PKS differenziert zu betrachten und zu bewerten.

Die Fallzahl zur missbräuchlichen Nutzung von Telekommunikationsdiensten gem. § 263a StGB stieg im Berichtsjahr um 36,2 % auf 644 Fälle (2017: 473 Fälle) an. Hauptursache ist ein komplexer Ermittlungsvorgang der Staatsanwaltschaft Oldenburg und der Polizeiinspektion Osnabrück[10] mit zahlreichen (aufgeklärten) Einzelfällen, der im Jahr 2018 in Niedersachsen abgeschlossen wurde.

Bei Datenveränderung/Computersabotage gem. § 303a, 303b StGB wurde ein starker Rückgang von 20,1 % verzeichnet. Diesbezüglich wurden 2.875 Fälle registriert (2017: 3.596 Fälle).

Fälle von Cybercrime im engeren Sinne (2018)



[9] Z. B. der Waren- oder Leistungskreditbetrug in folgender einfacher Form: Beim Versuch, eine Ware oder Dienstleitung über das Internet zu erlangen, erfolgt durch die Betrüger lediglich keine Bezahlung der Bestellung.

[10] Dabei erlangte der Beschuldigte über das Internet Zugriff auf sog. FRITZ! Boxen und programmierte Rufumleitungen zu nationalen und internationalen Mehrwertnummern. Anschließend wurden die Rufumleitungen automatisiert ausgelöst, so dass es zu kostenpflichtigen Verbindungen vom jeweils manipulierten Router/Telefonanschluss kam. Der Beschuldigte „mietete“ unter Verschleierung seiner Identität die zuvor programmierten nationalen und internationalen Mehrwert-rufnummern und erlangte einen Teil der angefallenen Telefongebühren. Es konnte ein Schaden von ca. 60.330 Euro nachgewiesen werden. Der tatsächliche Schaden dürfte deutlich höher sein.

Deutschland stellt aufgrund seines hohen Entwicklungsstands und Know-hows (insbesondere der Wirtschaft) weiterhin ein attraktives Ziel für Cyberkriminelle dar:

Laut einem Studienbericht des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (bitkom) aus 2018 zum Thema „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“ (Befragung von 503 nach Branchen und Größenklassen repräsentativ ausgewählten Industrieunternehmen mit mindestens zehn Beschäftigten) sollen 68 % der Industrieunternehmen in den vergangenen zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage gewesen sein. Weitere 19 % waren vermutlich betroffen – hier ließ sich nicht zweifelsfrei feststellen, ob tatsächlich Daten abgeflossen sind oder ein Angriff nicht entdeckt wurde.[11]

Bei einer Forsa-Befragung im Frühjahr 2018 zum Thema „Cyberrisiken und der deutsche Mittelstand“ (repräsentative Befragung von 300 Entscheidern bei kleinen und mittleren Unternehmen) gaben 30 % der Befragten an, durch Attacken von Cyberkriminellen bereits wirtschaftliche Schäden erlitten zu haben. Bei rund drei Viertel der Befragten sollen sich diese Angriffe in den letzten zwei Jahren ereignet haben.[12]

Bei der Erstellung des „Allianz-Risiko-Barometers 2019“ wurden über 2.000 Personen aus verschiedenen Industrie- und Wirtschaftsbereichen in 86 Staaten befragt. „Cyber-Ereignisse“ (Cybercrime, IT-Ausfälle, „Data Breaches“[13] etc.) seien von 37 % der Befragten als TOP-Geschäftsrisiko angesehen worden.[14]

Die aufgeführten Studien machen deutlich, dass die Einbeziehung von Dunkelfelderkenntnissen und weiteren externen Quellen zur umfassenden Lageeinschätzung im Bereich Cybercrime unabdingbar ist.

2.3 TATVERDÄCHTIGE

Im Jahr 2018 wurden insgesamt 22.051 Tatverdächtige (TV) von Cybercrime-Delikten registriert. Gegenüber dem Vorjahr entspricht das einem Rückgang um 1,1 % (2017: 22.296 TV). 67,1 % der Tatverdächtigen waren männlich, 32,9 % weiblich.

Auffällig ist, dass weibliche TV damit im Phänomenbereich CCieS im Verhältnis zu den Straftaten insgesamt (24,87 %) überrepräsentiert sind. Ausschlaggebend dafür ist der Straftatbestand des Computerbetruges, vornehmlich des Warenkreditbetruges. Er weist hohe Fallzahlen und einen hohen Anteil weiblicher Tatverdächtiger auf (Computerbetrug gem. § 263a StGB: 34,4 % weibliche TV; Warenkreditbetrug gem. §§ 263, 263a StGB: weibliche TV 33,6 %). Bei Cybercrime-Delikten mit geringeren Fallzahlen ist der Anteil der weiblichen TV wiederum fast konform mit dem Anteil an den Gesamtstraftaten (z. B. Ausspähen von Daten, Abfangen von Daten, Datenhehlerei

[11] Wirtschaftsschutzstudie 2018, abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, S. 14.
[12] Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2018, abrufbar unter: https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbfb7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, S. 3.
[13] Ein „Data Breach“ ist der bewusste oder unbewusste Verlust sensibler Daten in einer als nicht vertrauenswürdig anzusehenden Umgebung. Nähere Erläuterungen zu „Data Breaches“ ab S. 14.
[14] Allianz Risk Barometer. Top Business Risks for 2019, abrufbar unter: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf, S. 4.

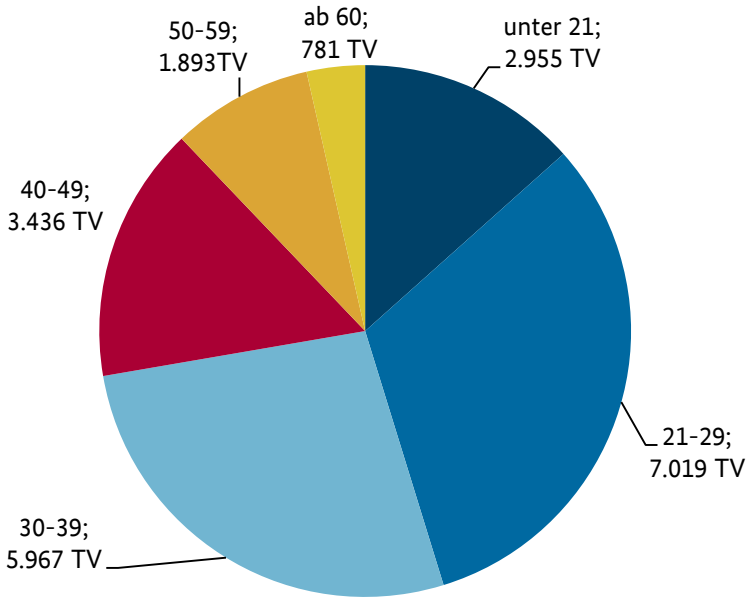
gem. §§ 202a-d StGB: 25,6 %) oder fällt sogar geringer aus (z. B. Datenveränderung, Computersabotage gem. §§ 303a, b StGB: 22,3 %).

Im Jahr 2018 hatten 16.832 der festgestellten Tatverdächtigen (76,3 %) die deutsche Staatsangehörigkeit. 5.219 Tatverdächtige waren Nichtdeutsche, wobei türkische (13,5 %), rumänische (9,7 %) und nigerianische (8,7 %) Staatsangehörige am häufigsten vertreten waren. Während bei den türkischen und rumänischen Staatsangehörigen ebenfalls der Warenkreditbetrug für den hohen Anteil verantwortlich ist, sind nigerianische Staatsangehörige insbesondere beim Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel vertreten.

Das Sicherheitsunternehmen FireEye gibt in seiner Analyse an, dass die Mehrheit der weltweit initiierten Cyberattacken im Bereich der staatlich gesteuerten nur von einigen wenigen Staaten (China, Russland und Nordkorea) initiiert wurde.[15] Diese Staaten sind bei den in der PKS aufgeführten Tatverdächtigen unterrepräsentiert (Russland: 131 TV, China 24 TV, VR Korea: 0 TV).

Mehr als die Hälfte (58,9 %) der registrierten Delikte der CCieS wurden von Tatverdächtigen begangen, die zwischen 21 und 39 Jahre alt waren.

Altersstruktur der Tatverdächtigen (2018)



Das Täterspektrum reicht vom Einzeltäter bis hin zu international organisierten Tätergruppierungen. Gemeinsam agierende Täter arbeiten im Bereich Cybercrime nur selten in hierarchischen Strukturen. Sie kennen sich häufig nicht persönlich und nutzen auch bei arbeitsteiligem Vorgehen die vermeintliche Anonymität des Internets.

Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Dienste, die nicht selbst erbracht werden können, werden von anderen hinzugekauft (Cybercrime-as-a-Service).

[15] Die Hackergruppen hinter Advanced Persistent Threats, abrufbar unter: https://www.fireeye.de/current-threats/apt-groups.html

2.4 ORGANISIERTE KRIMINALITÄT

Cybercrime ist auch im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität (OK) von Bedeutung. Im Jahr 2018 wurden 13 der insgesamt 535 registrierten OK-Gruppierungen im Kriminalitätsbereich Cybercrime erfasst (2017: 17 OK-Gruppierungen).

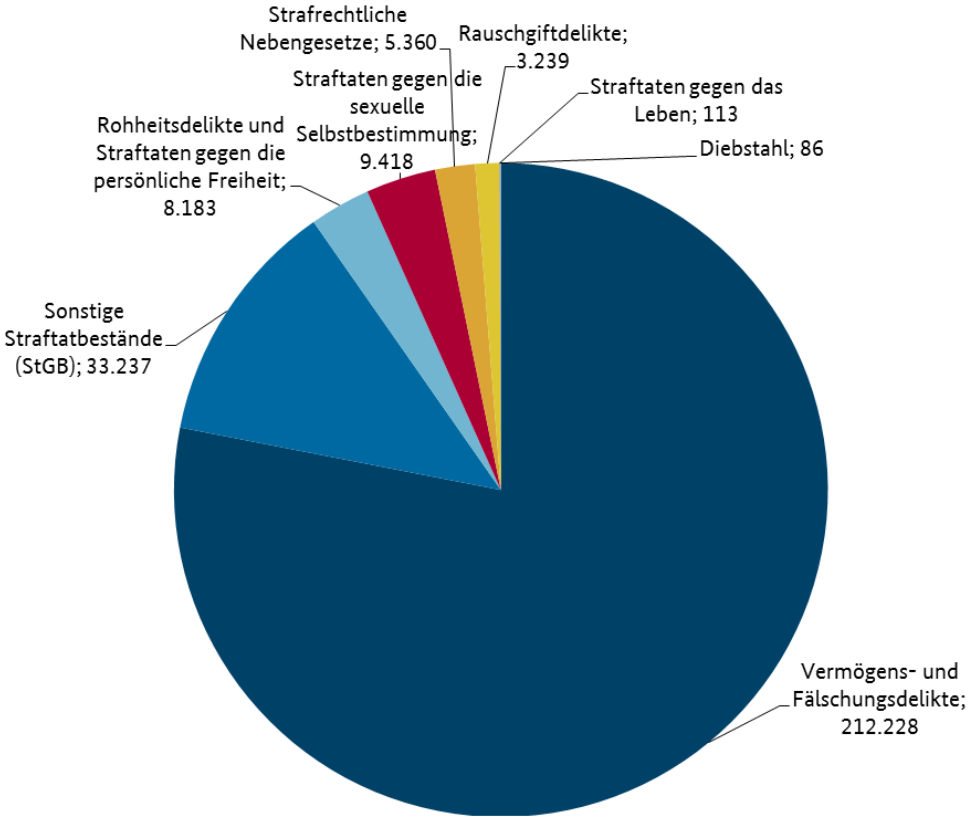
Deliktisch waren keine Unterschiede zu Einzeltätern oder losen Netzwerken feststellbar. Auch OK-Gruppierungen begingen die typischen Cybercrime-Delikte von Computerbetrug über Angriffe auf das Online-Banking bis hin zur Verbreitung von Ransomware mit dem Ziel der digitalen Erpressung.

2.5 TATMITTEL INTERNET

Im Jahr 2018 wurden in der PKS insgesamt 271.864 Fälle erfasst, bei denen das Internet als Tatmittel genutzt wurde. Dies entspricht einem Anstieg um 8,1 % gegenüber dem Vorjahr (2017: 251.617 Fälle).

Die PKS-Sonderkennung[16] „Tatmittel Internet“ wird bei der Erfassung berücksichtigt, wenn das Internet im Hinblick auf die Tatverwirklichung eine wesentliche Rolle spielt, z. B. bei Erpressungshandlungen i. Z. m. DDoS-Attacken oder bei der Abwicklung von Geschäften bei Online-Versandhäusern. Die Sonderkennung wird allerdings nicht verwendet, wenn z. B. im Vorfeld der eigentlichen Tat lediglich lose Kontakte zwischen Täter und Geschädigtem über das Internet bestanden.

Tatmittel Internet – Verteilung nach Deliktsbereichen (2018)



[16] Sonderkennungen sind in der PKS optional zu wählende Merkmale, die bei der Erfassung einer Straftat zusätzlich ausgewählt werden können. Mit Sonderkennungen werden bestimmte PKS-relevante Kriminalitätsformen gekennzeichnet.

Im Jahr 2018 handelte es sich bei 75,7 % (205.735 Fälle) aller Straftaten mit dem Tatmittel Internet um Betrug (2017: 74,4 %; 183.529 Fälle). Darunter waren 154.773 Fälle von Waren- und Warenkreditbetrug (2017: 134.476 Fälle), bei denen Tatverdächtige über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder in minderwertiger Qualität lieferten oder bei denen Tatverdächtige die Waren bestellten und nicht bezahlten.

3 Phänomene im Bereich Cybercrime

Der Diebstahl digitaler Identitäten ist Ausgangspunkt und „Treibstoff“ einer Vielzahl krimineller Verwertungsmodelle der Cybercrime.

DDoS-Angriffe haben an Quantität und Qualität stark zugenommen.

Über das Geschäftsmodell „Cybercrime-as-a-Service“ wird einem breiten Nutzerkreis ohne tiefgreifende computertechnische Kenntnisse die Begehung von Cybercrime-Straftaten ermöglicht.

Ransomware wurde verstärkt zur Erpressung kleiner und mittelständischer Unternehmen eingesetzt.

Schadsoftware, die wiederum weitere Schadsoftware nachlädt, ermöglicht den maßgeschneiderten Missbrauch kompromittierter Zielsysteme.

3.1 DIEBSTAHL DIGITALER IDENTITÄTEN / ID-THEFT

Die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte ist nach wie vor ein gängiges und lukratives Geschäftsmodell.

Was ist die digitale Identität?

Der Begriff „digitale Identität" bezeichnet die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner personenbezogenen Daten und Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret beinhaltet dies auch alle Arten von Nutzer-Accounts, also auch Zugangsdaten in den Bereichen:

- *Kommunikation (E-Mail- und Messengerdienste),*
- *E-Commerce (Online-Banking, Online-Aktienhandel, internetgestützte Vertriebsportale aller Art),*
- *berufsspezifische Informationen (z. B. für den Online-Zugriff auf firmeninterne technische Ressourcen),*
- *E-Government (z. B. elektronische Steuererklärung) sowie*
- *Cloud-Computing (Nutzung von als Dienstleistung angebotenem Speicherplatz, von Software oder Rechenleistung).*

Für Cyberkriminelle sind alle Daten bzw. Ausprägungen von digitalen Identitäten interessant, die für kriminelle Aktivitäten genutzt werden können. Im Vordergrund stehen hierbei meistens finanzielle Motive – so erfolgen z. B. bei Online-Shops Warenbestellungen durch den Täter unter Verwendung von Name und Adresse des Opfers (Warenkreditbetrug), kostenpflichtige Streaming-Dienste werden mittels der gestohlenen Identitäten gebucht oder Mobilfunkverträge werden widerrechtlich abgeschlossen.

Betrügereien im Online-Banking mittels gestohlener Daten haben weiterhin eine hohe Bedeutung im Bereich Cybercrime – hierzu werden unter Punkt 3.2 separate Ausführungen gemacht.

Die sog. „kriminelle Personifikation" zielt darauf ab, die Identität des Opfers zu stehlen, um diese in Zukunft für das Vortäuschen falscher Tatsachen zu benutzen oder durch Namensmissbrauch den Ruf des Opfers zu schädigen. Des Weiteren sind Mobbing und Stalking häufig mit einem Identitätsdiebstahl verbunden.

Der Identitätsdiebstahl ist häufig Ausgangspunkt weiterer Cyber-Straftaten. Nach Aussage des G4C-Mitglieds Link11 haben Cloud-Server für DDoS-Attacken an Bedeutung gewonnen. Mittels „gestohlener" Namen und E-Mail-Adressen können z. B. falsche Cloud-Konten erstellt werden, die dann für entsprechende Angriffe genutzt werden. E-Mail-Anschriften werden für den massenhaften Versand von Spam-Mails genutzt, um z. B. die Verteilung von Schadsoftware/Ransomware zu veranlassen.

Zugriff auf die Daten bekommen die Täter bspw. durch Phishing-Mails, den Einsatz von Schadsoftware (Spyware[17], Trojaner[18] und Keylogger[19]) oder über das Prinzip des Social Engineerings, bei dem die Täter auf zwischenmenschlicher Ebene gezielt Personen beeinflussen, um bestimmte Verhaltensweisen hervorzurufen (speziell im Bereich des „CEO-Frauds“[20]).

Über Datenlecks bei Firmen/Unternehmen geraten massenweise digitale Identitäten auf den „Cyber-Markt“, welche dann täterseitig genutzt werden können. Das BSI führt in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2018“ aus, dass dort die Verwendung von persönlichen Daten aus Datenabflüssen bei großen Dienstleistern, Kontakten aus E-Mail-Clients infizierter Systeme oder recherchierten Daten immer häufiger beobachtet wird.[21]

Durch die zunehmende Digitalisierung und steigende Nutzung sozialer Netzwerke wird es für Cyberkriminelle immer einfacher, digitale Identitäten zu "stehlen“.

Das BSI führt weiter aus, dass im März 2018 massiv gefälschte Nachrichten via Facebook-Messenger verschickt worden sind, welche einen Link zu einem angeblichen YouTube-Video enthielten. Folgte man diesem Link, gelangte man allerdings auf eine gefälschte Facebook-Anmeldeseite. Gab der Betroffene nun seine Anmeldedaten dort ein, konnten die Kriminellen hinter den gefälschten Nachrichten diese Daten abgreifen und so vollen Zugriff zum Account erhalten.

Eine weitere Methode, um in den Besitz digitaler Identitäten zu gelangen, ist das sog. „War-driving“. Dabei suchen die Täter aktiv nach ungeschützten WLAN-Netzwerken, um die Daten aller am WLAN-Router angeschlossenen Computer abgreifen zu können.

FORMJACKING

Im Jahr 2018 trat auch der Modus Operandi des sog. „Formjacking“ in den Vordergrund. Hierbei werden bösartige Codes auf den Webseiten von Online-Shops integriert. Diese Codes sind meist kleine aber stark verschleierte JavaScripts. Wenn der Kunde seine Zahlungsdaten in ein Online-Formular eingibt, um einen Online-Kauf zu tätigen, werden diese Kreditkartendetails nicht nur an den Händler weitergeleitet, sondern auch direkt an den Cyberkriminellen.

Gem. Aussagen des G4C-Mitglieds Symantec sind im Jahr 2018 mehr als 3,7 Mio. Formjacking-Angriffe auf sog. Endpunkte abgewehrt worden. Betroffen sollen auch bekannte Webseiten, z. B. von Ticketshops und Fluglinien, gewesen sein.[22] Insgesamt sind demnach von dem IT-Dienstleister durchschnittlich ca. 4.800 mit Formjacking infizierte Webseiten pro Monat festgestellt worden.

---

[17] Wortschöpfung aus Spy (spionieren) und Software. Als Spyware werden Programme bezeichnet, die heimlich Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

[18] Ein Trojaner ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Es verbreitet sich nicht selbst, sondern wirbt mit der angeblichen Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer. Der Benutzer kann auf die Ausführung dieser Funktion keinen Einfluss nehmen, z. B. könnte ein Trojaner einem Angreifer eine versteckte Zugriffsmöglichkeit zum Computer bieten.

[19] Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnet alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern, filtern.

[20] Bei der Betrugsmasche „CEO-Fraud“ werden Firmenmitarbeiter unter Verwendung falscher Identitäten zur Überweisung von Geldbeträgen auf vom Täter kontrollierte Konten veranlasst.

[21] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, S. 46.

[22] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, S. 14.

Ein zeitlicher Schwerpunkt habe u. a. im November/Dezember 2018 ausgemacht werden können.[23] Offensichtlich wurde von den Cyberkriminellen gezielt versucht, mittels dieses Modus Operandi illegale Gewinne aus dem „Black Friday“ bzw. dem „Weihnachtsgeschäft“ zu erwirtschaften.

DATA BREACHES

Im Jahr 2018 wurden diverse Data Breaches festgestellt, durch die umfangreiche Schäden entstanden.

Data Breaches:

Unter dem Begriff „Data Breach“ werden sowohl bewusste als auch unbewusste Verluste sensibler Daten an einen nicht vertrauenswürdigen Personenkreis zusammengefasst. Er umfasst damit sowohl „leaks“ (Datenlecks technischer Natur) als auch „intrusions“ (aktives Abgreifen, Abfangen oder Ausleiten von Daten durch Dritte).

Oftmals wissen die betroffenen Personen gar nicht, dass ihre Daten „verloren gegangen“ bzw. entwendet worden sind. Dies wird häufig erst Monate oder Jahre später durch die Folgen des Datenmissbrauchs offensichtlich, z. B. in Form von wirtschaftlichen Nachteilen, da das Kreditkartenkonto von Kriminellen bis zum Limit ausgeschöpft wurde, oder in Form von persönlichen Nachteilen wie Imageschäden, weil unter Missbrauch der eigenen persönlichen Daten andere über ein soziales Netzwerk beleidigt oder gar sexuell belästigt wurden.

Die Ursachen für derartige Datenverluste sind vielfältig. Zum Teil ist ein nicht hinreichend gesicherter Umgang von Unternehmen mit Daten ursächlich. Zumeist stehen technisch versierte Täter, sog. Hacker, hinter den Angriffen.

Gruppen organisierter Kriminalität sollen laut IOCTA 2018 (Internet Organised Crime Threat Assessment) von Europol grundsätzlich für 50 % der Data Breaches verantwortlich sein. Weiteren Ausführungen zufolge seien insgesamt 76 % aller Angriffe finanziell motiviert gewesen.[24]

Im März 2018 konnte die spanische Polizei mit Unterstützung von EUROPOL den Kopf einer Tätergruppe festnehmen, die seit 2013 über fast fünf Jahre hinweg Banken mit Schadsoftware angegriffen haben soll. Die Täter hatten hierbei Phishing-Mails mit schadhaftem Anhang an Bankmitarbeiter gerichtet. Sobald jemand diese öffnete, installierte sich die Software auf dem Server der Bank, so dass die Täter massenweise auf Konten und Geldautomaten zugreifen konnten. Die Software war unter dem Namen Carbanak und Cobalt bekannt geworden, wobei ein Schaden von bis zu zehn Mio. Euro pro Angriff entstand.

[23] Ebd., S. 47.
[24] Internet Organised Crime Threat Assessment (IOCTA) 2018, abrufbar unter: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, S. 22.

Ebenfalls im März 2018 soll es bei der Fitness-App „MyFitnessPal“ des US-Unternehmens Under Armour einen Data Breach gegeben haben, bei dem bis zu 150 Mio. Nutzer betroffen gewesen sein sollen. Es sollen Benutzernamen, E-Mail Adressen und Passwörter gestohlen worden sein.[25] Ähnlich soll es Facebook im Oktober 2018 ergangen sein, wo Profilinformationen von ca. 30 Mio. Nutzern abgegriffen wurden.[26]

Der Data Breach von British Airways im August 2018 verdeutlicht, dass auch die Reisebranche ein beliebtes Angriffsziel darstellt. Bei Buchungen über die Internetseite und die App von British Airways sind nach Angaben der Fluggesellschaft die Daten von etwa 380.000 Kreditkarten gestohlen worden. Betroffen waren persönliche und finanzielle Details, nicht aber Pass-und Reisedaten.[27]

Laut IOCTA 2018 sei der Yahoo Data Breach aus dem Jahr 2013 der bisher weltweit größte Angriff seiner Art gewesen. Es sollen alle 3 Mrd. Kunden vom Abgreifen der Namen, E-Mail Adressen und Passwörter betroffen gewesen sein.[28]

DOXING/DOXXING

Doxing/Doxxing stellt grundsätzlich kein neues Phänomen dar. In der Vergangenheit wurde diese Form der Datenveröffentlichung wiederholt genutzt, um „Andersdenkende“ zu beeinflussen. Beispiele hierfür sind das sog. „Outing“, d. h. die Veröffentlichung von Informationen über den politischen Gegner, im Bereich der politisch motivierten Kriminalität, wie auch die namentliche Veröffentlichung von Aktivisten, die sich für Menschenrechte einsetzten und sich in der Folge derartiger Veröffentlichungen persönlichen Hetzkampagnen ausgesetzt sahen.

Eine Löschung von einmal im Netz veröffentlichten Daten ist nahezu unmöglich.

[25] Hacker stehlen Daten von 150 Millionen Nutzern, abrufbar unter: https://www.spiegel.de/netzwelt/apps/myfitnesspal-hacker-stehlen-daten-von-150-millionen-nutzern-a-1200644.html, veröffentlicht am 03.03.2018.
[26] Hackerangriff auf Facebook. Detailreiche Informationen ausspioniert, abrufbar unter: https://www.tagesschau.de/wirtschaft/facebook-datenpanne-103.html, veröffentlicht am 31.10.2018.
[27] Datenpanne bei British Airways, abrufbar unter: https://www.tagesschau.de/wirtschaft/datenpanne-british-airways-101.html, veröffentlicht am 10.07.2019.
[28] Internet Organised Crime Threat Assessment (IOCTA) 2018, abrufbar unter: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, S. 22.

Doxing/Doxxing:

Unter dem Begriff „doxing“ oder „doxxing“ versteht man das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, zumeist mit illegitimen Absichten gegenüber den Betroffenen. Der Ausdruck „Doxing“ stellt eine Abkürzung für “document tracing” bzw. “docs tracing” dar und wurde aus „docs“ abgeleitet.

Motive für das Täterhandeln können unter anderem die Deanonymisierung oder aber das reine öffentliche Bloßstellen sowie die Belästigung von Personen sein.

Basierend auf den veröffentlichten Daten kann es in der Folge zu weiteren Attacken bzw. Straftaten zum Nachteil der Betroffenen kommen.

In den Fokus der Öffentlichkeit rückte dieses Phänomen erneut ab dem Jahresende 2018, als private Informationen zu verschiedenen Politikern und weiteren Personen des öffentlichen Lebens einer breiten Internetöffentlichkeit zugänglich gemacht wurden. Einmal im Netz ist es schwer bzw. nahezu unmöglich, eine Löschung der veröffentlichten Daten in Gänze herbeizuführen. Umso wichtiger erscheint der Schutz digitaler Identitäten, insbesondere um Cyberkriminellen den Zugriff auf diese Art von „Grundstoffen“ für anknüpfende Cyber-Straftaten zu erschweren.

Fallbeispiel: Doxing/Doxxing

Vom 01.12.2018 bis 03.01.2019 wurden in Sozialen Netzwerken, vorrangig über "Twitter", unter täterseitiger Nutzung mehrerer Online-Identitäten, private Informationen zu verschiedenen Politikern und weiteren Personen des öffentlichen Lebens veröffentlicht. Dies erfolgte in Form von Webseiten-Links, die zu diversen Datenspeichern führten, auf denen Textdateien mit Informationen zu den betroffenen Personen hinterlegt waren (u. a. Namen, Telefonnummern, Anschriften, E-Mail-Adressen). Eine Vielzahl dieser allgemein zugänglichen Textdateien enthielt weitere Links zum Download von Dateien wie Ausweiskopien, Rechnungen, Kontoauszüge, Inhalte aus Sozialen Netzwerken der Betroffenen und private sowie berufliche Korrespondenz. Von dem Cyber-Angriff waren insgesamt ca. 1.000 aktive und ehemalige Politiker auf EU-, Bundes-, Landes- und kommunaler Ebene sowie andere Personen des öffentlichen Lebens (z. B. Journalisten) direkt und eine Vielzahl weiterer Personen mittelbar (z. B. über veröffentlichte Adressspeicher) betroffen.

Das BKA übernahm auf Ersuchen der Generalstaatsanwaltschaft Frankfurt am Main, Zentralstelle für die Bekämpfung der Internet und Computerkriminalität (ZIT), die zentralen Ermittlungen wegen Verdachts des Ausspähens von Daten, der Datenhehlerei und des Verstoßes gegen das Bundesdatenschutzgesetz. Im Rahmen dieser Ermittlungen wurde ein 20-jähriger deutscher Tatverdächtiger identifiziert und vorläufig festgenommen. In seiner Vernehmung gab sich die Person bezüglich der Tatvorwürfe umfassend geständig. Demnach war der Beschuldigte über öffentlich zugängliche Quellen oder über die E-Mail- bzw. Social Media-Accounts der Betroffenen, zu denen er sich Zugang verschafft hatte, an die persönlichen Daten gelangt.

Fallbeispiel: Doxing/Doxxing

Kurzbewertung:
Das Vorgehen des Täters verdeutlicht, wie einfach es u. U. sein kann, personenbezogene Daten im Netz zu erlangen und missbräuchlich zu nutzen. Der Beschuldigte gilt nicht als ausgereifter „Hacker", der besondere technische Sicherheitslücken ausnutzte oder sich spezieller Techniken/ Technologien bediente, um an persönliche Informationen zu gelangen bzw. Accounts von Betroffenen zu übernehmen. Sein Vorgehen basierte vielmehr auf dem Täuschen von Personen, dem sog. Social Engineering. Außerdem nutzte er individuell zu verortende Sicherheitsdefizite, die nicht immer von den späteren Opfern zu verantworten sind. So bediente er sich z. B. zuvor gelöschter und wieder frei gewordener Recovery E-Mail Adressen[29]. Um solche Straftaten durchzuführen, bedarf es keiner besonderen Kenntnisse, sondern allenfalls gründlicher Recherchen.

Der Fall verdeutlicht zudem die hohe Bedeutung, die „User" dem Schutz der digitalen Identitäten beimessen sollten. Regelmäßige Updates benutzter Software, Zwei- bzw. Multi-Faktor-Authentisierung für Zugänge zu Accounts und Plattformen sowie die Nutzung komplexer Passwörter bzw. von Passwort-Managern wären geeignet, um einen Identitätsdiebstahl zu erschweren.

3.2 PHISHING IM ONLINE-BANKING

Eine häufige Variante des digitalen Identitätsdiebstahls ist neben dem Massendiebstahl von digitalen Daten weiterhin das Phishing im Zusammenhang mit Online-Banking. In einer Welt, die sich immer weiter digitalisiert, ist es üblich, alltägliche Geschäfte online abzuwickeln. Dies erweitert die Angriffsfläche für Cyberkriminelle.

Im Jahr 2018 wurden 723 Fälle zum Phänomen Phishing gemeldet, was einem Rückgang von nahezu 50 % gegenüber dem Vorjahr entspricht. Damit setzte sich der im Jahr 2017 bereits festgestellte Trend fort. Seinerzeit hatte der Rückgang der Fallzahl gegenüber dem Jahr zuvor ca. 35 % betragen.

Nach Angaben des G4C ist das Dunkelfeld in diesem Bereich eher als gering anzusehen, da die Standardprozesse der Banken eine Erstattung nur in den Fällen erlauben, in denen kundenseitig eine polizeiliche Strafanzeige erfolgt ist. In der ersten Jahreshälfte 2018 wurde vom G4C-Mitglied Commerzbank beim Phishing im Online-Banking der Einsatz von Malware kaum beobachtet. Vielmehr lag der Schwerpunkt eher beim „klassischen Phishing", worunter das Abgreifen der Login-Daten für das Online-Banking zu fassen ist, indem Opfer über E-Mail kontaktiert und zur Preisgabe dieser Daten verleitet werden. In der zweiten Hälfte des Jahres 2018 stieg die Fallzahl zum Phishing mittels Malware wieder an – auch in Deutschland konnten Aktivitäten, z. B. im Zusammenhang mit der Malware *Trickbot,* festgestellt werden.

Eine weitere Form von Phishing im Zusammenhang mit Online-Banking ist das sog. SIM-Swapping bzw. SIM-Jacking. Hierbei handelt es sich um einen Account Take Over, bei dem die Täter die Ruf-

[29] Recovery E-Mail Adressen werden von den Nutzern bei verschiedenen Online-Plattformen zur Kontowiederherstellung angegeben. Für den Fall, dass die Anmeldung auf der Plattform auf dem üblichen Weg aus verschiedenen Gründen nicht funktionieren sollte, kann mittels dieser Recovery E-Mail-Adresse z. B. das Passwort für die Plattform zurückgesetzt werden.

nummer eines Ziels auf eine vom Angreifer gehaltene SIM-Karte übertragen lassen.[30] Um beim jeweiligen Telekommunikationsanbieter an eine SIM-Karte mit der Rufnummer des Opfers zu gelangen, sammeln die Täter häufig im Vorfeld über verschiedene Methoden (z. B. Phishing, Social Engineering) die dafür notwendigen Daten über das potenzielle Opfer[31]. Die SIM-Karte mit der Rufnummer des Opfers ermöglicht es den Tätern dann, bei einigen Anbietern Passwörter von Konten des Opfers (z. B. bei E-Commerce-Plattformen oder Banking-Apps) neu zu vergeben.[32]

Phishing im Online-Banking bleibt für Cyber-Täter ein lukratives Betätigungsfeld.

Anfang 2019 wurde eine bundesweit operierende Gruppe zerschlagen, welche sich seit 2018 illegal Online-Zugangsdaten von Kunden verschiedener Bankinstitute verschafft hatte, Ersatz-SIM-Karten angefordert und diese anstelle der rechtmäßigen SIM-Karten hatte aktivieren lassen. Dadurch war es ihnen ferner möglich, sich für Online-Überweisungen notwendige Transaktionsnummern (TAN) zusenden zu lassen und unter Angabe falscher Kontodaten Beträge von mehr als 1,5 Mio. Euro zu erbeuten.[33] Ein ähnliches Vorgehen erfolgt beim Missbrauch der sog. „pushTAN-Methode“, die u. a. beim mobilen Online-Banking der Sparkassen Anwendung findet.[34] Hierbei späht der Täter die persönlichen Daten der Geschädigten aus und kontaktiert das Service-Center der Sparkasse. Er lässt unter Angabe der Daten des jeweiligen Geschädigten die Rufnummer für das TAN-Verfahren ändern, sodass der Täter die Push-TAN über die Sparkassen-App auf seinem Smartphone mit der neuen Zielrufnummer erhält. Über diese lassen sich ohne weitere zusätzliche Geräte oder Kontakte Überweisungen ausführen.

In Deutschland konnten noch keine tatsächlich erfolgreichen technischen Angriffe gegen Mobile Banking Apps festgestellt werden.[36]

Laut dem BSI soll das Online-Banking mittlerweile nicht mehr nur mittels eines PC, sondern vermehrt mit mobilen Geräten, wie Smartphones oder Tablets erfolgen.[35] Es werden nicht nur die eigenen Apps der größeren Banken angeboten, sondern auch freie multibankfähige Apps, die es ermöglichen, Konten bei verschiedenen Banken zu verwalten. Zusätzlich werden diese Banking-Apps häufig mit einer zweiten Anwendung, der sog. TAN-App, kombiniert. Diese generiert eine Transaktionsnummer, um die in der Banking-App getätigte Transaktion abzusichern.

---

[30] SIM Swapping: Wie Hacker Millionen via Mobilfunkanbieter stehlen konnten, abrufbar unter: https://de.cointelegraph.com/news/sim-swapping-how-hackers-stole-millions-worth-of-crypto-via-victims-telecoms-operator, veröffentlicht am 19.08.2018.

[31] z. B. Bank- und Kreditkartendaten, SIM-Karten-Anbieter des Opfers etc.

[32] Wave of SIM swapping attack hit US cryptocurrency users, abrufbar unter: https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/, veröffentlicht am 03.06.2019.

[33] Gemeinsame Presseinformation der Staatsanwaltschaft Verden und der Polizeidirektion Hannover: Strafverfolgungsbehörden zerschlagen bundesweit operierende Bande von Online-Betrügern, abrufbar unter: https://www.staatsanwaltschaft-verden.niedersachsen.de/startseite/aktuelles/presseinformationen/gemeinsame-presseinformation-der-staatsanwaltschaft-verden-und-der-polizeidirektion-hannover-strafverfolgungsbehoerden-zerschlagen-bundesweit-operierende-bande-von-online-betruegern-176733.html, veröffentlicht am 26.04.2019.

[34] TAN-Verfahren. Mit pushTAN, smsTAN und chipTAN Aufträge sicher freigeben, abrufbar unter: https://www.sparkasse.de/service/sicherheit-im-internet/tan-verfahren.html.

[35] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, S. 19.

[36] Laut G4C-Mitglied Commerzbank.

Weil viele Nutzer den Schutzbedarf mobiler Geräte unterschätzen, nehmen Angreifer diese vermehrt ins Visier. Über manipulierte Apps, E-Mails, Chat- oder Kurznachrichten versuchen die Täter die Smartphone-Nutzer auf gefälschte Webseiten mit Eingabeaufforderungen zu locken, um dort Passwörter, Banking-TANs oder Kreditkartennummern abzugreifen.

3.3 MALWARE / SCHADPROGRAMME

Schadprogramme (Malware)

Schadprogramme führen unerwünschte oder schädliche Funktionen auf einem informationstechnischen System aus. Die Verbreitung und der Einsatz von Schadprogrammen auf Systemen der Geschädigten ist die wesentliche Basis für die Begehung von Cybercrime.

Die häufigsten Verbreitungswege von Schadprogrammen sind Anhänge in Spam-Mails sowie die vom Anwender unbemerkte Infektion beim Besuch von präparierten Webseiten (Drive-by-Infection). Die Verbreitung von Schadsoftware erfolgt zunehmend wurmartig. Ausdruck einer Professionalisierung in diesem Bereich ist unter anderem die Tatsache, dass durch die Schadsoftware automatisch Schwachstellen erkannt werden.

Cybercrime ist insbesondere aufgrund der weiten Verbreitung von Schadsoftware zu einem Massenphänomen geworden.

Laut Aussagen des BSI, das sich auf Feststellungen des Sicherheitsunternehmens AV-Test beruft, hat sich die Gesamtzahl der festgestellten Schadprogrammvarianten in den Jahren 2014-2017 bereits mehr als verdoppelt (konkret: 2014: 326,04 Millionen; 2017: 719,15 Millionen Schadprogramme). Für das Jahr 2018 wurde mit einem Gesamtaufkommen an Malware von mehr als 800 Millionen und einem durchschnittlichen Zuwachs von rund 390.000 neue Varianten pro Tag gerechnet.

Das BSI veröffentlichte im April 2019 die Ergebnisse der von der „Allianz für Cybersicherheit“ durchgeführten Cyber-Sicherheits-Umfrage. Demzufolge sollen 43 % von den befragten großen Unternehmen angegeben haben, 2018 von Cyber-Sicherheitsvorfällen betroffen gewesen zu sein. Bei den kleinen und mittelständischen Unternehmen lag der Wert bei 26 %. Bei 53 % der von den Befragten berichteten Angriffsfälle soll es sich um Infektionen, bei denen Schadprogramme in betriebliche IT-Systeme eindrangen, gehandelt haben.[37]

KRYPTOMINING

In diversen Publikationen berichtete die Privatwirtschaft (insb. Antiviren-Dienstleister, IT-Security-Dienstleister) Ende 2017/Anfang 2018 über eine steigende Bedrohungslage durch die Verbreitung bösartiger Kryptomining-Software. Ziel ist hier die Infiltration von privat sowie geschäftlich genutz-

[37] Cyber-Sicherheits-Umfrage –Cyber-Risiken & Schutzmaßnahmen in Unternehmen, abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9, S. 11.

ten Systemen, um die Rechenleistung dieser Systeme für die Errechnung von Kryptowährungen[38], insbesondere *Bitcoin*, zu nutzen. Hierunter leidet die Leistung der infizierten Systeme. Dies bewirkt einen erhöhten Stromverbrauch, was wiederum zu hohen Kosten auf Seiten der Betroffenen führen kann.[39]

Beim browserbasierten Kryptomining wird für den Zeitraum des Besuchs bestimmter Webseiten mit oder ohne Wissen des Betroffenen Kryptowährung generiert. Auch sog. intelligente Endgeräte des Internet of Things[40] (IoT) werden als Kryptominer missbraucht. Obwohl diese Geräte in der Regel nicht so leistungsstark sind, ziehen die Cyber-Täter ihren Nutzen aus deren unzureichenden Sicherheitskontrollen und der hohen Anzahl der über einen längeren Zeitraum zu nutzenden Systeme.

Die polizeilichen Datenbestände verzeichnen derweil kaum Fälle von Kryptomining-Malware. Dies dürfte insbesondere darauf zurückzuführen sein, dass der Schaden durch die Betroffenen nur selten oder zumindest verspätet bemerkt oder das Vorgehen seitens der Betroffenen nicht als strafbare Handlung bewertet wird.

Eine Abfrage bei den Länderdienststellen der Polizei ergab, dass im Zeitraum Januar 2017 bis Juni 2018 lediglich 13 Sachverhalte mit dem Tathintergrund Kryptomining zur Anzeige gebracht wurden. Anhand der polizeilichen Datenbasis ließ sich demzufolge der von den Antiviren-Dienstleistern festgestellte Trend extrem hoher Steigerungsraten in diesem Phänomenbereich nicht belegen.

Das Thema „Ausnutzung von Schwachstellen“ blieb im Jahr 2018 im IT-Bereich aktuell. Anfang des Jahres haben Sicherheitsforscher schwere Sicherheitslücken in den Prozessoren von Milliarden Computern entdeckt. Die als „Spectre“ und „Meltdown“ benannten Schwachstellen sollen sich u. a. in Prozessoren von AMD, ARM und INTEL befunden haben und erlaub(t)en es Angreifern, sensible Speicherbereiche auszulesen. Hersteller und Softwareentwickler boten kurz nach Entdeckung Sicherheitsupdates für Betriebssysteme und Browser an, welche die Gefahr von z. B. Datenabflüssen über diese Schwachstellen minimieren bzw. ausschließen sollten. Ein mögliches Ausnutzen der Schwachstellen „Spectre“ und „Meltdown“ manifestierte sich 2018 nicht in einem Anstieg des Fallaufkommens auf polizeilicher Seite.

EMOTET

Anfang Dezember 2018 warnte das BSI vor einer gefährlichen Schadsoftware namens *Emotet*, die eine akute Bedrohung für Unternehmen, Behörden und Privatanwender darstellt und in Deutschland zu diesem Zeitpunkt bereits Schäden in Millionenhöhe verursacht haben soll.[41]

[38] Alternative Bezeichnungen: virtuelle, alternative oder digitale Währungen, Geld oder Devisen.
[39] Executive Summary - 2018 Internet Security Threat Report (ISTR), Volume 23, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf, S. 1.
[40] Internet der Dinge; detaillierte Ausführungen siehe Kapitel 5.2.
[41] Gefährliche Schadsoftware – BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen, abrufbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html, veröffentlicht am 05.12.2018.

Fallbeispiel: *Emotet* Malware

Mitte November 2018 wurde das Klinikum Fürstenfeldbruck/Bayern Opfer von *Emotet*. Durch Öffnung eines mit Schadsoftware infizierten E-Mail-Anhangs wurden die ca. 450 vorhandenen Computer des Klinikums tagelang unbenutzbar. Zeitweise musste die Klinik gar von der integrierten Rettungsleitstelle des Landkreises abgemeldet werden.

Kurzbewertung:
Der Vorfall verdeutlicht die von *Emotet* ausgehende Bedrohung sowie die weitreichenden Folgen, die eine Infizierung mit *Emotet* haben kann.

Am Beispiel *Emotet* lässt sich erkennen, inwiefern die Anwendungsbereiche einer bestimmten Schadsoftware über die Zeit variieren können. Die *Emotet*-Schadsoftware war in ihren Ursprüngen im Jahr 2014 ein reiner Banking-Trojaner, der Online-Banking von Privatkunden deutscher Finanzinstitute zur Initiierung betrügerischer Transaktionen manipulierte. Mittlerweile hat sich der Trojaner in der Programmierung erheblich weiterentwickelt. *Emotet* kann nun eher als sog. „Downloader" oder „Dropper" bezeichnet werden, dessen vorrangige Funktion in der unbemerkten Primär-Infektion des Opfersystems und dem späteren modularen Nachladen weiterer Schadsoftware besteht. Diese Nachladefunktion von beliebiger Schadsoftware wird anderen Gruppierungen im Sinne des Crime-as-a-Service angeboten, um deren Schadsoftware (z. B. die Banking-Trojaner *Trickbot* oder *Dridex*) verbreiten zu lassen.

In der Regel wird *Emotet* im Rahmen von massenhaft versandten Spam-Mails verbreitet. Dabei beinhalten die E-Mails in der Regel eine Word-Datei im Anhang oder einen Link, bei dessen Anklicken eine Verbindung zum Internet hergestellt wird. Dabei wird versucht, eine Datei im Word-Format herunterzuladen. Durch das Öffnen des Dokuments und die Aktivierung der Makro-Funktion führt der im Dokument eingebettete Code zum Ausführen eines Kommandozeilen-Codes (Powershell) sowie der Download der eigentlichen *Emotet*-Schadsoftware zur Installation auf dem Zielsystem. Der Rechner ist sodann unter der Kontrolle der Täter. Bereits in seiner Grundausführung kann die *Emotet*-Schadsoftware ohne zusätzliche Module folgende, strafrechtlich relevante Aktivitäten entfalten:

- Ausspähen von Informationen über das Zielsystem und Übersenden dieser Informationen an Steuerungsserver der Täter
- Registrieren und Speichern von Tastaturanschlägen (sogenanntes Keylogging).

Darüber hinaus konnten in den vergangenen Monaten/Jahren die folgenden, nachladbaren Module der *Emotet*-Schadsoftware festgestellt werden:

- *Emotet*-Banking-Modul zur Manipulation des Online-Bankings,
- Ausspähen von in E-Mail-Programmen gespeicherten Passwörtern,
- Ausspähen von in Web-Browsern gespeicherten Passwörtern,
- Extraktion von Namen und E-Mail-Adressen der Kommunikationspartner in E-Mail-Programmen,
- *Emotet*-DDoS-Modul für sog. DDoS-Angriffe.

Es konnte außerdem festgestellt werden, dass *Emotet* neben den eigenen Modulen auch Schadsoftware anderer Gruppierungen nachgeladen hat, bspw.:

- *Dridex*-Banking-Trojaner
  Ein überwiegend in den USA, in Großbritannien, in der Schweiz und in Deutschland aktiver Trojaner, der das Online-Banking von Privat- und Geschäftskunden manipuliert (Verdacht des gewerbsmäßigen Computerbetrugs).

- *Trickbot*-Banking-Trojaner
  Ein überwiegend in den USA und in Großbritannien aktiver Trojaner, der das Online-Banking von Privatkunden manipuliert (Verdacht des gewerbsmäßigen Computerbetrugs).

- *UmbreCrypt*-Ransomware
  Eine Ransomware, die persönliche Dateien des Computernutzers, insbesondere Bilder und Dokumente, verschlüsselt und zur Entschlüsselung ein Lösegeld in *Bitcoin* fordert.

- *Ryuk*-Ransomware
  Siehe Punkt 3.4.

Die Schadprogramme werden aufgrund ständiger Modifikation zunächst meist nicht von gängigen Virenschutzprogrammen erkannt. Laut dem BSI sind einmal infizierte Systeme grundsätzlich als vollständig kompromittiert zu betrachten und müssen neu aufgesetzt werden.

Die Betroffenheit Deutschlands in Bezug auf den *Emotet*-Trojaner ist quantitativ schwer zu beziffern, da bei etwaigen Infektionen häufig nicht *Emotet* selbst, sondern die nachgeladene Schadsoftware auf betroffenen Systemen festgestellt wird. Das Nachladen der *Emotet*-Schadsoftware bzw. der jeweiligen Module erfolgt in der Regel nicht von tätereigenen, sondern von kompromittierten Systemen anderer Serverbetreiber. In diesem Zusammenhang werden regelmäßig auch Systeme in Deutschland zum Zwecke der Verteilung der Schadsoftware kompromittiert.

Angriffe auf Geldautomaten

Logische/digitale Angriffe auf Geldautomaten gewinnen zunehmend an Bedeutung, wenn auch in vergleichsweise geringer Fallzahl. Dabei kommt auch hier Schadsoftware zum Einsatz. Dieser Phänomenbereich unterscheidet diesbezüglich generell drei Modi Operandi:

a. Jackpotting (Angriffe auf den Rechner/PC eines Geldautomaten mittels Schadsoftware)

b. Blackboxing (Unterart des Jackpotting – Angriff auf das Auszahlungsmodul des Geldautomaten mittels tätereigener Hardware)

c. Netzwerkattacke (Malwareangriff auf die kartenausgebende Bank oder Processinggesellschaft um Transaktionsprozesse zu manipulieren; anschließend erfolgt ein sog. kartengebundener „Cash Out“ oder Malwareangriff auf die geldautomatenbetreibende Bank, um einen direkten Zugriff auf die im Netzwerk verbundenen Geldautomaten zu erhalten und einen sog. kartenungebundenen Cash Out durchzuführen).

Geldautomaten werden verstärkt digital angegriffen.

Nachdem im November 2017 erstmals der versuchte Einsatz einer bestimmten, über das Darknet vertriebenen Schadsoftware festgestellt wurde, die es auch technisch weniger versierten Tätern ermöglichen soll, Geldautomaten zu manipulieren und einen sog. „Cash Out“ durchzuführen, wurden in 2018 bereits 20 solcher Jackpotting-Angriffe mit einem Gesamtschaden von ca. 540.000 Euro bekannt.

Im Jahr 2018 erfolgten in Deutschland 43 Blackbox-Attacken, von denen lediglich vier erfolgreich verliefen. Der Schaden belief sich auf ca. 450.000 Euro.

Ferner kam es im Jahr 2018 zu Netzwerkattacken auf drei asiatische Banken, die einen „Cash Out“ u. a. auch in Deutschland zur Folge hatten. Der Schaden betrug weltweit ca. 39 Mio. Euro. Netzwerkattacken auf Geldautomaten werden seit dem Jahr 2016 weltweit vermehrt, u. a. mit Schadenssummen im zweistelligen Millionenbereich, festgestellt. Aufgrund der großen „Ertragserwartung“ für die Täter muss von einer anhaltend hohen Bedrohung ausgegangen werden.

Fallbeispiel: Einsatz von Malware zum Cashout von Geldautomaten

Seit Mitte Dezember 2017 führt das Bundeskriminalamt ein Ermittlungsverfahren der Staatsanwaltschaft Köln, Zentrale Ansprechstelle Cybercrime (ZAC) NRW, wegen des Verdachts des banden- und gewerbsmäßigen Computerbetruges zum Nachteil einer afrikanischen Großbank.

Hintergrund des Verfahrens ist der im November 2017 in Deutschland und den Vereinigten Arabischen Emiraten (VAE) simultan erfolgte, missbräuchliche Einsatz von 15 regulär in einem afrikanischen Staat ausgegebenen Kreditkarten. Der Schaden mehrerer hunderter Geldabhebungen betrug ca. 550.000 Euro.

Im Verlauf der Ermittlungen wurden Querverbindungen bezüglich der Modi Operandi sowie personelle Überschneidungen in den Täterstrukturen zu einem weiteren in Deutschland, ebenfalls unter Sachleitung der ZAC NRW, geführten Ermittlungsverfahren festgestellt. Verfahrensgegenständlich sind hier 2.176 missbräuchliche Nutzungen von 157 Kreditkarten im Februar 2017. Hierbei wurde ein Schaden von ca. 3,1 Millionen Euro zum Nachteil einer weiteren afrikanischen Großbank verursacht. Die betrügerischen Abhebungen erfolgten zum damaligen Zeitpunkt koordiniert in Deutschland sowie in der Schweiz, in Luxemburg und in den Niederlanden.

Durch die Ermittlungen konnte nachgewiesen werden, dass die Täter die IT-Infrastruktur der afrikanischen Banken dauerhaft infiltriert hatten, indem sie mehrere Rechner mit verschiedenen Malware-Varianten infiziert und gleichzeitig die vorhandene Anti-Viren-Software deaktiviert hatten. Aufgrund einer vorhandenen Keylogger-Funktionalität war es den Tätern gelungen, die Zugangsberechtigungen von Mitarbeitern der Bank auszuspähen, um letztlich unautorisiert Zugriff auf für die Abhebungs- und Abrechnungsprozesse zuständigen Datenbanken zu erlangen. Über Manipulation eben jener Datenbanken waren Kartenlimits und Anzahl der täglichen Abhebungen so heraufgesetzt worden, dass die oben benannten missbräuchlichen Abhebungen ermöglicht wurden.

Im Rahmen der Ermittlungen konnten diverse Tatverdächtige afrikanischer Herkunft in Deutschland, Frankreich und in der Schweiz identifiziert werden.

In enger Absprache mit den französischen Behörden erfolgten Exekutivmaßnahmen gegen Mitglieder der Gruppierung, darunter die Vollstreckung eines Haftbefehls gegen eine in Deutschland aufhältige Zielperson.

Kurzbewertung:
Erstmalig wurde durch das BKA eine Cyberkomponente mit ausgeprägtem Bezug nach Afrika festgestellt.

Der technische Modus Operandi (Netzwerkeinbrüche, persistente Infiltration und nachfolgende Manipulationen) ist eindeutig (auch ausweislich der gerichtlichen Würdigung) im Phänomenbereich CCieS zu verorten. Die Tatbegehungskomponenten (Rekrutierung von „Läufern“ auf dem afrikanischen Kontinent zur Konteneröffnung, Beschaffung zahlreicher originaler Kreditkarten, Transport der Tatmittel in die Einsatzgebiete in Europa und in den VAE, Rekrutierung von Abhebern und simultane Durchführung internationaler Verwertungshandlungen, sog. Cashouts) und die dadurch erlangten erheblichen kriminellen Gewinne deuten auf international organisierte, kriminelle Strukturen hin.

3.4 RANSOMWARE – DIGITALE ERPRESSUNG

Der Einsatz von Ransomware führt in der Regel zur Verschlüsselung von Daten eines digitalen Systems und in vielen Fällen auch zur Sperrung anderer, in einem Netzwerk erreichbarer Endgeräte (bspw. in Firmennetzwerken).

Infizierte Systeme werden oftmals vollständig verschlüsselt und gesamte Netzwerke erheblich gestört. Betroffene, die ihre IT-Infrastruktur nicht durch aktuelle Backups wieder aufbauen können, erleiden massive Beeinträchtigungen bis hin zu einem kompletten Ausfall des Geschäftsbetriebs. Angesichts dieses hohen Schadenspotenzials zahlen viele Geschädigte die vergleichsweise niedrigen geforderten Lösegelder.

In den meisten Fällen fordern die Täter ein Lösegeld, das in Form von Kryptowährungen zu zahlen ist. Nach Zahlung der geforderten Summe wird den Geschädigten die Übermittlung eines Freischaltcodes zugesagt, mit dem sie das blockierte System entsperren bzw. entschlüsseln und anschließend wieder nutzen können.

Welche Arten von Ransomware gibt es?

Grundsätzlich kann bei Ransomware zwischen zwei Varianten unterschieden werden:

a) *Ransomware, die keine Verschlüsselung der Festplatte durchführt, sondern durch eine Manipulation lediglich den Zugriff auf das System versperrt. Die wohl bekanntesten Ausprägungen sind Schadprogramme, bei denen bekannte Namen und Logos von Sicherheitsbehörden[42] missbraucht werden, um der kriminellen Zahlungsaufforderung einen offiziellen Charakter zu verleihen.*

b) *Sog. Krypto-Ransomware, die die Daten auf den infizierten Endsystemen und aktuell auch mittels Netzwerk verbundenen Systemen (Server, Dateiablagen etc.) tatsächlich verschlüsselt. Diese Variante birgt für den Betroffenen ein weitaus größeres Schadenspotenzial, da die genutzten Verschlüsselungen nicht in allen Fällen überwunden werden können. Die Zahlung des geforderten Lösegelds führt darüber hinaus häufig nicht zur Entschlüsselung des infizierten Systems.*

Aus polizeilicher Sicht ist von entsprechenden Zahlungen abzuraten, da hierdurch das kriminelle Geschäftsmodell Ransomware unterstützt wird, Anreize zur weiteren Tatbegehung geschaffen werden und insbesondere die Zahlung keine Gewähr für die Wiederherstellung der verschlüsselten Daten darstellt.

Betroffene können möglicherweise auch selbst gegen die Infizierung vorgehen: Es empfiehlt sich eine „Open-Source-Recherche“ nach frei verfügbaren Entschlüsselungstools, so bspw. über das von EUROPOL und der niederländischen Cybercrime-Dienststelle (NHTCU) in Zusammenarbeit mit der Privatwirtschaft initiierte Projekt www.nomoreransom.org. Das BKA unterstützt ausdrücklich die Zielrichtung dieses Projekts und ist seit 29.09.2017 offiziell „Supporting Partner“.

Strafrechtlich betrachtet handelt es sich beim Einsatz von Ransomware um eine Kombination der Delikte Computersabotage gem. § 303 b StGB und Erpressung gem. § 253 StGB.

Digitale Erpressung mittels Ransomware ist schon seit längerem ein in Deutschland und auch weltweit häufig auftretendes Phänomen. Nachdem das Jahr 2017 von den Ransomware-Wellen *WannaCry* und *Petya* (siehe auch Bundeslagebild Cybercrime 2017) geprägt war, waren im Jahr 2018 Ransomware-Wellen dieses Ausmaßes nicht festzustellen. Gleichwohl gab es im Berichtsjahr gezielte Ransomware-Attacken, die sich vornehmlich gegen Unternehmen richteten.

Auch das BSI stellt im Bericht zur Lage der IT-Sicherheit in Deutschland 2018 fest, dass sich die Bedrohung durch Ransomware zwar im Jahr 2018 fortsetzte, allerdings in geringerem Umfang als

[42] Bekannte Beispiele sind der sog. „BKA-Trojaner“ und der „GVU-Trojaner“ (GVU: Gesellschaft zur Verfolgung von Urheberrechtsverletzungen).

zuvor. Als Begründung werden die Verlagerung bzw. Ergänzung durch Kryptomining und die Konzentration der Täter auf gezieltere Angriffe angeführt, was aber insbesondere auf Seiten der Unternehmen – auch im Bereich sog. Kritischer Infrastrukturen (KRITIS) - zu einem hohen Druck führt, um Angriffe abzuwehren bzw. zu begrenzen und potenzielle Schäden zu minimieren.[43]

Ransomware-Angriffe richten sich zunehmend gegen Unternehmen.

Das G4C-Mitglied Symantec stellte für das Jahr 2018 einen Rückgang von 20 % im Gesamtbereich der Ransomware gegenüber dem Vorjahr fest – allerdings soll die Anzahl der Ransomware-Varianten, die gezielt Unternehmen angreifen, im gleichen Zeitraum um 12 % gestiegen sein. Diese Entwicklungen belegen eine zunehmende Bedrohung für die Wirtschaft und sprechen für ein gezielteres und professionelleres Vorgehen der Cyberkriminellen, die ihre Aktivitäten in „lukrativere" Geschäftsfelder verlagern.[44]

Die Ransomware-Szene zeichnet sich durch eine zunehmende Professionalisierung aus.

Der ENISA[45] Threat Landscape Report 2018 weist den Bereich Ransomware weiterhin als Bedrohung aus, auch wenn in dem Bericht mit Bezug auf mehrere Cyber-Sicherheitsunternehmen darauf verwiesen wird, dass generell ein Rückgang von Ransomware-Vorfällen zu verzeichnen ist. Durch die Spezialisierung der Cyberkriminellen seien verschiedene bzw. spezielle Bereiche in deren Fokus gerückt. Laut ENISA-Report handelte es sich bei 85 % der Malware-Angriffe auf medizinische Geräte um Angriffe mit Ransomware.[46]

GandCrab wurde erstmals im Januar 2018 als eine neue Malwarekampagne entdeckt, die im gesamten Jahresverlauf aktiv blieb und auch darüber hinaus noch eine weltweite Bedrohung darstellte. Die Verbreitung erfolgte klassisch per Mails mit infiziertem Anhang, aber auch über gecrackte Software bis hin zu Exploit-Kits[47]. In Deutschland zählte sie zu den aktivsten Ransomware-Familien. Die bisher bekannten Mails richteten sich v. a. an Unternehmen, von denen sich die Täter höhere Lösegeldsummen als von Privatpersonen versprachen.

Anhand von Untersuchungen der *GandCrab*-Ransomware stellt der IT-Security-Dienstleister Check Point in seinem Security Report für das Jahr 2018 indes fest, dass durch das Geschäftsmodell „Ransomware-as-a-Service" auch „Amateure" von diesem Erpressungsgeschäft profitieren würden. So sollen die eigentlichen Cyberkriminellen und die Entwickler der Malware arbeitsteilig vorgehen und die erpressten Gelder im Verhältnis 60:40 teilen. Check Point geht weiter davon aus, dass *GandCrab* innerhalb von zwei Monaten im Jahr 2018 über 50.000 Netzwerke infiziert hat und die Täter hierbei Lösegelder zwischen 300.000 und 600.000 Dollar gefordert haben.[48]

---

[43] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, S. 13.

[44] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, S. 9.

[45] European Network and Information Security Agency / Europäische Agentur für Netz- und Informationssicherheit.

[46] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, abrufbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, S. 100.

[47] Schadprogramme, die zur Ausführung Sicherheitslücken von auf dem Zielsystem installierten Programmen ausnutzen

[48] The GandCrab Ransomware Mindset, abrufbar unter: https://research.checkpoint.com/gandcrab-ransomware-mindset, veröffentlicht am 13.03.2018.

Die Malware *GandCrab* wird per Spam-Mails mit schadhaftem Anhang verschickt. Diese Spams sind als Bewerbungsmails getarnt und enthalten – in einer Zip-Datei verpackt – einen Lebenslauf, ein Bewerbungsfoto sowie ein Anschreiben. Beim Anklicken der Datei gibt das Dokument vor „mit einer älteren Version von Microsoft Word" erstellt worden zu sein und versucht das Opfer dazu zu verleiten, per Kompatibilitätsmodus aktive Inhalte des Dokuments zu aktivieren. Sobald dies geschieht, wird die in der Zip-Datei enthaltene Malware aktiviert. Der Trojaner kann auf das System zugreifen und wichtige Daten verschlüsseln.

GandCrab ermittelt zahlreiche Informationen über den PC eines Nutzers, wie z. B. den Nutzernamen, den PC-Namen, die Domäne, das Tastaturlayout und das Betriebssystem. Außerdem wird die öffentliche IP-Adresse gespeichert. Für jeden Nutzer wird eine eindeutige Adresse auf einem Tor Hidden Service (Netzwerk zur Anonymisierung von Verbindungsdaten) generiert, unter der der vom Erpresser geforderte Betrag und Anweisungen zur Zahlung eingesehen werden können. Die Höhe des Betrags wird an das jeweilige Opfer angepasst. Die Kriminellen nutzen dabei jeden Tag leicht veränderte Versionen der Malware, um die Erkennung für Antivirenprogramme zu erschweren. So werden die Bewerbungsmails unter verschiedenen Namen verschickt und weisen unterschiedlich angepasste Betreffzeilen auf.

Auch das Online-Magazin ZDNet berichtete über *GandCrab*. Demnach sollen die Hinterleute dieser Ransomware angekündigt haben, dass sie ihr Geschäftsmodell „Ransomware-as-a-Service" innerhalb eines Monats einstellen wollten. Die Ankündigung soll von einer Quelle aus der Malware-Community stammen, welche durch einen Beitrag der Akteure in einem Hacking-Forum scheinbar bestätigt wird. Demnach habe die Gruppe nach eigenen Angaben mehr als 2 Mrd. Dollar Lösegeld erpresst und bereits gewaschen („legalized").

Im Oktober 2018 wurde bekannt, dass die rumänische Polizei in Zusammenarbeit mit anderen Staaten, EUROPOL und dem Internet Security Unternehmen Bitdefender die Möglichkeit der Entschlüsselung für verschiedene Versionen der Ransomware-Variante von *GandCrab* gefunden hat. Auf die Möglichkeit der Entschlüsselung reagierten die Täter mit dem Einsatz einer neuen Variante der Malware.

Ransomware findet u. a auch über die in Kapitel 3.3 dargestellte Malware den Weg auf die betroffenen Rechner der Geschädigten. So diente z. B die Schadsoftware *Emotet* dazu, die Ransomware *Ryuk* auf befallene Computer nachzuladen. Im Mai 2018 veröffentlichte das Federal Bureau of Investigation (FBI) einen Bericht, wonach *Ryuk* seit August 2018 durch unbekannte Cyberkriminelle dazu genutzt worden sein soll, mehr als 100 internationale Unternehmen zu erpressen. Dabei sollen einzelne Forderungssummen bis zu einer Höhe des Gegenwerts von 5 Mio. US-Dollar in *Bitcoins* festgestellt worden sein. Im Gegenzug soll den Opfern ein Entschlüsselungsprogramm versprochen worden sein.

Die Ransomware verschlüsselt Daten auf Netzlaufwerken und infizierten Dateisystemen, v. a die Daten, die *Emotet* zuvor als sensibel bzw. wichtig eingestuft hat. Das Besondere an *Ryuk* ist, dass neben der Verschlüsselung der wichtigen Daten im gleichen Zuge alle hiervon existierenden Sicherheitskopien gelöscht werden. Somit wird die Wiederherstellung erheblich erschwert. Die ausgewählten Ziele von *Ryuk* sind unterschiedlich, jedoch konzentriert sich der Angriff auf Unternehmen mit einem hohen Jahresumsatz, in der Hoffnung, eine höhere Geldsumme erbeuten zu können.

3.5 BOTNETZE – MASSENHAFTE FERNSTEUERUNG VON COMPUTERN

Auch wenn in der jüngeren Vergangenheit größere Botnetz-Architekturen wie *Avalanche*[49] und *Andromeda*[50] zerschlagen werden konnten, spielten Botnetze auch im Jahr 2018 eine zentrale Rolle für Cybertäter. Neben Computern wurden vermehrt auch mobile sowie sog. intelligente Endgeräte[51] des Internet of Things (IoT) „zusammengeschlossen". Insbesondere das IoT bietet vielfältige Möglichkeiten zum Ausbau von Botnetzen.

Wie entstehen Botnetze?

Botnetze entstehen durch die zumeist für den Besitzer unbemerkte Installation einer Schadsoftware auf dem PC des Geschädigten.
Die Installation der Schadsoftware kann auf verschiedene Arten erfolgen, sei es durch Öffnung eines infizierten E-Mail-Anhangs oder auch mittels „Drive-by-Infection".

Eine weitere Variante ist die Verteilung der Schadsoftware über soziale Netzwerke (z. B. Facebook). Den Mitgliedern/Usern der Netzwerke werden von vermeintlichen Bekannten oder Freunden Nachrichten mit infizierten Anhängen zugesandt. Ein Öffnen dieser Anhänge oder ein Klick auf einen eingefügten Link führt zur Infektion des Computers.

Weitere Verbreitungskanäle sind das Usenet[52] *und Tauschbörsen/Peer to Peer-Netze, in denen die Schadsoftware meist als Video- oder Sounddatei getarnt zum Download angeboten wird.*

In der Folge hat der Täter durch die zuvor installierte Schadsoftware einen nahezu vollständigen Zugriff auf das infizierte System des Geschädigten. Die zahlreichen, per Schadcode infizierten Geräte der Geschädigten werden ohne Wissen ihrer Besitzer über sog. „Command & Control-Server" ferngesteuert.

Aufgrund der vielfältigen Nutzungsmöglichkeiten von Botnetzen (Identitätsdiebstahl, DDoS-Angriffe, Verteilung von Schadprogrammen/Spam-Mails) hat die Bedrohung durch sie als zentrale Angriffsressource nicht an Bedeutung verloren.

[49] Die Zerschlagung von *Avalanche* erfolgte im Jahr 2016 durch die Staatsanwaltschaft Verden in Zusammenarbeit mit der Zentralen Kriminalinspektion Lüneburg und internationalen Partnern.
[50] Im Jahr 2017 konnte die Botnetz-Architektur Andromeda durch das FBI u. a. in enger Zusammenarbeit mit der Zentralen Kriminalinspektion Lüneburg zerschlagen werden.
[51] Intelligente Endgeräte sind internetfähige Alltagsgegenstände, mit denen der Nutzer oder weitere Geräte über das Internet kommunizieren können.
[52] Eigener selbstständiger Dienst des Internets, der neben dem gängigen World Wide Web besteht.

Das BSI informiert in seinem Jahresbericht 2018, dass von Sicherheitsforschern täglich bis zu 10.000 Botnetzinfektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-Provider gemeldet würden. Eine valide Angabe zur Gesamtzahl der in Deutschland bzw. weltweit in Botnetzen zusammengeschlossenen Rechner sei jedoch kaum möglich. Schwerpunktmäßig sollen Microsoft-Windows-Systeme betroffen sein, wobei auch weitere Betriebssysteme und Android-Geräte für das Phänomen Botnetze an Bedeutung gewinnen würden.[53]

Das BSI berichtet weiter, dass sich die gemeldeten Infektionen im Berichtszeitraum auf 130 verschiedene Botnetz-Familien verteilten.[54] Eine detailliertere Betrachtung dieser Botnetze habe aufgezeigt, dass folgende Verwendungen der Botnetze im Vordergrund standen:

- Online-Banking-Betrug
- Dropper, die zum Nachladen weiterer Schadprogramme dienen
- Klickbetrug
- Bitcoin-Mining
- Spam-Versand
- DDoS-Angriffe

Zum Teil sind Botnetze multifunktional konzipiert und lassen sich somit flexibel für unterschiedliche kriminelle Zwecke verwenden.

Das BKA unterstützte im Jahr 2018 Ermittlungen des US-amerikanischen FBI gegen die Hintermänner des *Necurs*-Botnetzes. Den Ermittlungen zufolge dürften wichtige Teile der kriminellen Infrastruktur in Deutschland gehostet sein.

Fallbeispiel: *Necurs*-Botnetz

Im August 2018 wurde das *Necurs*-Botnetz mit einem Angriff in Verbindung gebracht, welcher sich gegen Unternehmen aus dem Finanzbereich richtete. Hierbei wurden sog. RATs (Remote Access Trojans) verbreitet. Das Sicherheitsunternehmen „Cofense“ berichtete, dass bei diesem Angriff massenhaft Spam-Mails gezielt an ca. 2.700 Banken verschickt wurden. Die Nachrichten wurden sehr knapp und einfach verfasst mit allgemein gehaltener Betreffzeile. Laut Cofense hörte diese Spam-Kampagne abrupt nach ihrer Entdeckung auf.

Kurzbewertung:
Das *Necurs*-Botnetz wird aufgrund seiner Größe und seiner vielseitigen Einsatzmöglichkeiten (u. a. Spam-Mail-Versand, Ransomware-Verbreitung, Initiierung von DDoS-Attacken) als eines der „gefährlichsten“ Botnetze weltweit bewertet. Der „Crime-as-a-Service“-Gedanke spielt auch in diesem Phänomenbereich der Cybercrime eine bedeutende Rolle.

[53] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, S. 28
[54] Ebd., S. 30.

Laut dem US-amerikanischen IT-Unternehmen „International Business Machines Corporation“ (IBM) soll das *Necurs*-Botnetz aus bis zu 6 Mio. Bots bestehen. Es existiert seit mehreren Jahren, wird im Verlauf eines Jahres allerdings nur vereinzelt für gezielte Angriffe aktiv. Unter Einsatz des *Necurs*-Botnetzes wurden bisher millionenfach Spam-Mails versandt. Neben diesem primären Nutzungszweck werden auch Rechner mit Ransomware und Malware über dieses Botnetz infiziert, DDoS-Angriffe initiiert und Zugangsdaten ausgespäht.[55]Bekannt wurde das *Necurs*-Botnetz zum einen durch die Verbreitung von Trojanern, wie *Dridex* oder *Trickbot*, zum anderen aber durch die Verbreitung von Ransomware, wie *Locky* oder *Scarab*.

Ein weiteres Beispiel für die Multifunktionalität von Botnetzen und die zunehmende Professionalisierung der Cyberkriminellen in diesem Bereich stellt das Phänomen „Click-Fraud“ dar, bei dem die Täter unter Einsatz einer großen IT-Infrastruktur in Deutschland bereits erhebliche kriminelle Gewinne erzielen konnten:

Fallbeispiel: Botnetz – „Click-Fraud“

Das BKA wurde im Rahmen eines Ermittlungsverfahrens der US-amerikanischen Behörden gegen unbekannte Täter, die seit Jahren Computerbetrug zum Nachteil der (digitalen) Werbeindustrie und deren Kunden mittels Click-Fraud begingen, um Unterstützung gebeten.
Die Täter hatten sich bei dem von den US-Behörden als „Metan Fraud Scheme“ bezeichneten Modus Operandi als Werbeträger für Internetwerbung angeboten. Im Anschluss an die getroffene Vereinbarung, wonach der Werbeträger nach der Anzahl von Klicks auf geschaltete Werbung vergütet wird, wurden täterseitig tausende von Servern bei einem deutschen Hosting-Provider angemietet. Während ein paar Server zur Steuerung und Kontrolle verwendet wurden, installierten die Täter auf dem Großteil der anderen Server sog. „Browser-Bots“, durch die unzählige Klicks auf die täterseitig gehostete Fremdwerbung ausgelöst wurden.

Um zu verschleiern, dass die Klicks durch Bots herbeigeführt wurden, leiteten die Täter zusätzlich Datenverkehr von mit Malware infizierten Computern normaler PC-Benutzer in den USA weiter, so dass es für die Werbefirmen den Anschein haben konnte, dass normale Endnutzer aus den USA auf ihre Werbung klickten.

Nach Schätzung der US-Behörden belief sich die Gesamtschadenssumme zwischen den Jahren 2014 und 2018 auf mehr als 36 Mio. US-Dollar. Dem gegenüber standen Kosten für das von den Tätern in Deutschland „aufgebaute“ Botnetz in Höhe von ca. 250.000 Euro pro Monat.

Kurzbewertung:
Durch schadsoftwarebasierte Botnetze begangene „Click-Frauds“ stellen keine Neuheit dar.
Neu ist an diesem Modus Operandi aber, dass die Täter ein eigenes, auf gemieteten Servern basierendes Botnetz zum Generieren der Clicks verwendeten und das User-PC-Botnetz lediglich zur Verschleierung einsetzten.

Der Sachverhalt verdeutlicht, dass die bisherigen Schutzmechanismen der Werbeindustrie nicht ausreichend greifen. So ist das „Metan Fraud Scheme“-Botnetz bereits seit 2014 aktiv und erwirtschaftet, trotz immenser täterseitiger Kosten für den Aufbau des Botnetzes in Deutschland (ca. 250.000 Euro pro Monat), enorme finanzielle Gewinne.

[55] Necurs Spammers Go All In to Find a Valentine’s Day Victim, abrufbar unter: https://securityintelligence.com/necurs-spammers-go-all-in-to-find-a-valentines-day-victim, veröffentlicht am 12.02.2018.

3.6 DDOS-ANGRIFFE

DDoS-Angriffe zielen darauf ab, Webpräsenzen, Server und Netzwerke von Personen oder Organisationen jedweder Art zu überlasten und so eine Nichterreichbarkeit ihrer Dienste herbeizuführen. Für einen derartigen Angriff sind hunderte bis tausende Systeme notwendig, sodass Kriminelle v. a. über Botnetze DDoS-Attacken ausführen bzw. ausführen lassen.

DDoS-Angriffe

Bei sog. „Distributed Denial of Service" (DDoS)-Angriffen werden massive Datenanfragen durch Botnetze an ausgewählte Server gestellt, bis die maximale Kapazität der attackierten Systeme erreicht ist und diese unter der Anfragelast „zusammenbrechen".

Die Motivationen hinter derartigen Attacken sind vielfältig und umfassen u. a. monetäre Interessen[56], die Schädigung von geschäftlichen Konkurrenten oder politisch motivierte Beweggründe. Auch wenn die konkreten Ziele der Kriminellen voneinander abweichen, so ist ihre primäre Intention beim Einsatz von DDoS-Angriffen das Verursachen von möglichst großem Schaden gegen die hinter dem angegriffenen System stehenden Personen oder Organisation.

Durch die Nichterreichbarkeit der Webpräsenzen entstehen den Betreibern nicht nur Ausfälle in Geschäftsabläufen, Einbrüche von Verkaufszahlen und damit erhebliche wirtschaftliche Schäden, sondern ebenso Reputations- und Vertrauensverlust bei Partnern und Kunden. DDoS-Angriffe sind deshalb nicht selten für existenzielle Notlagen von Betrieben verantwortlich: Das auf die Abwehr von DDoS-Angriffen spezialisierte IT-Unternehmen und G4C-Mitglied Link11 beziffert den möglichen Schaden pro erfolgreich durchgeführtem DDoS-Angriff auf 45.000 Euro.[57]

Nach Informationen von Link11 haben DDoS-Angriffe im Jahr 2018 an Quantität und Qualität stark zugenommen. Im Vergleich zu 2017 soll 2018 nicht nur ihre Anzahl um 34 % angestiegen sein, auch erhöhte sich die durchschnittliche Angriffsbandbreite derartiger Attacken von 1,7 Gbit/s[58] auf 4,9 Gbit/s, wodurch ein schnellerer Kollaps angegriffener Dienste erreicht wurde.[59] Im Jahr 2018 registrierte das Link11 Security Operation Center über 54.000 DDoS-Attacken allein auf Ziele in Deutschland, Österreich und der Schweiz.[60]

DDoS-Angriffe nehmen weiter an Quantität und Qualität zu.

Auch der Fokus von DDoS-Angriffen hat sich verändert. Dabei sind Anbieter von Cloud-Speichern (z. B. Amazon) in den Fokus von Kriminellen gerückt, sei es als Ziel eines Angriffs oder aber als Plattform, um Angriffe zu starten. So fand im Jahr 2018 jeder dritte DDoS-Angriff über widerrechtlich

DDoS-Angriffe dürften zukünftig zielgerichteter gegen Branchen und Unternehmen eingesetzt werden.

[56] Sog. Ransom – DDoS: Drohung mit einem DDoS-Angriff, um das Opfer zu erpressen.
[57] G4C Workshop vom 12.03.2019.
[58] Gigabit pro Sekunde ist eine Einheit, mit der Datenübertragungsraten dargestellt werden können.
[59] G4C Workshops vom 12.03.2019.
[60] LINK11 DDoS-Report für die DACH-Region, abrufbar unter: https://www.link11.com/de/ddos-report/.

genutzte Cloud-Server statt, was gegenüber dem Vorjahr einen Anstieg um ca. 80 % darstellt. Die Cloud-Server wurden dabei entweder direkt gehackt oder z. B. unter falschen Namen und mit gestohlenen Kreditkartendaten angemietet.

Auch in Bezug auf Intensität und Ziele der Kriminellen hat sich der Fokus verschoben. Im Jahr 2018 wurde an für Online-Händler und Handelsplätze im Web wichtigen Kalendertagen (z. B. Cyber-Monday von Amazon oder der Black Friday) ein Anstieg der DDoS-Attacken um bis zu 70 % festgestellt[61]. Doch nicht nur die Anbieter (zumeist Online-Händler oder Handelsbörsen) selbst waren betroffen, auch Payment-Anbieter wie PayPal oder Logistiker wurden an jenen Tagen Ziele von DDoS-Angriffen. Ebenso waren KRITIS und auch mittelständische Unternehmen von kriminellen Aktivitäten dieser Art betroffen. Es ist davon auszugehen, dass DDoS-Angriffe künftig noch zielgerichteter gegen bestimmte Branchen und Unternehmen eingesetzt werden.

DDoS-Attacken traten im Jahr 2018 v. a. im Rahmen sog. Multivektor-Angriffe in Erscheinung. Deren Gefährdungspotenzial ergibt sich aus dem Umstand, dass nicht nur eine Attacke, sondern mehrere synchron ablaufende Angriffe unterschiedlicher Art abgewehrt werden müssen. Multivektorielle Angriffe stellten im Jahr 2018 59 % aller DDoS-Angriffe dar.

Ein ebenso bedrohlicher Trend in diesem Phänomenbereich sind sog. Level-7-Angriffe. Ihr Name bezieht sich auf den Aufbau des sog. OSI-Modells[62], einem Referenzmodell für Netzwerkprotokolle, welches aus sieben Schichten (englisch: layers oder level) besteht. Die siebte Schicht des OSI-Modells ist die sog. Anwendungsschicht. Diese stellt Dienste zur direkten Interaktion mit Usern bereit, agiert oftmals ähnlich einer Programmierschnittstelle (API) und ist für Datenein- und ausgaben, wie auch für ihre Überprüfung zuständig. Dies ist z. B. der Fall, wenn ein User sich in seinen E-Mail-Account einloggt.

Während konventionelle DDoS-Angriffe oftmals ein gesamtes Netzwerk bzw. System attackieren, wird bei einem Level-7-Angriff nur die Programmierschnittstelle einer Webseite oder eines Dienstes überlastet und so ein „Kollaps“ eben jener herbeigeführt. Diese Art von Angriffen ist für Cyberkriminelle attraktiv, da sie weniger Ressourcen (und damit Systeme innerhalb eines Botnetzwerkes) benötigen, um das angegriffene System zu überlasten. Außerdem werden sie zunächst kaum als „Botangriff“ identifiziert, da ihr Verhalten (die Verwendung von legitimen Netzwerkabfragen) zunächst unverdächtig erscheint.[63]

[61] LINK11 DDoS-Report für die DACH-Region, abrufbar unter: https://www.link11.com/de/ddos-report/.
[62] Open Systems Interconnection Model.
[63] Defending against Layer 7 DDoS Attacks, abrufbar unter: https://blog.verisign.com/security/defending-against-layer-7-ddos-attacks/, veröffentlicht am 29.09.2016.

Fallbeispiel: Webstresser

Im April 2018 wurde im Rahmen einer koordinierten Aktion von Strafverfolgungsbehörden aus den Niederlanden, Großbritannien, Serbien, Kroatien, Spanien, Italien, Deutschland, Australien, Hongkong, Kanada und den USA in Zusammenarbeit mit EUROPOL der größte Marktplatz für DDoS-Angriffe namens „Webstresser“ vom Netz genommen. Bei solch einem „DDoS-for-hire“-Marktplatz können Kunden ein Botnetz mieten und ohne eigene computertechnische Kenntnisse DDoS-Angriffe auf Webseiten starten, zumal das Ziel des Angriffs über ein Webinterface[64] ausgewählt werden kann. Die Infrastruktur des Dienstes befand sich in Deutschland, in den Niederlanden und in den USA.

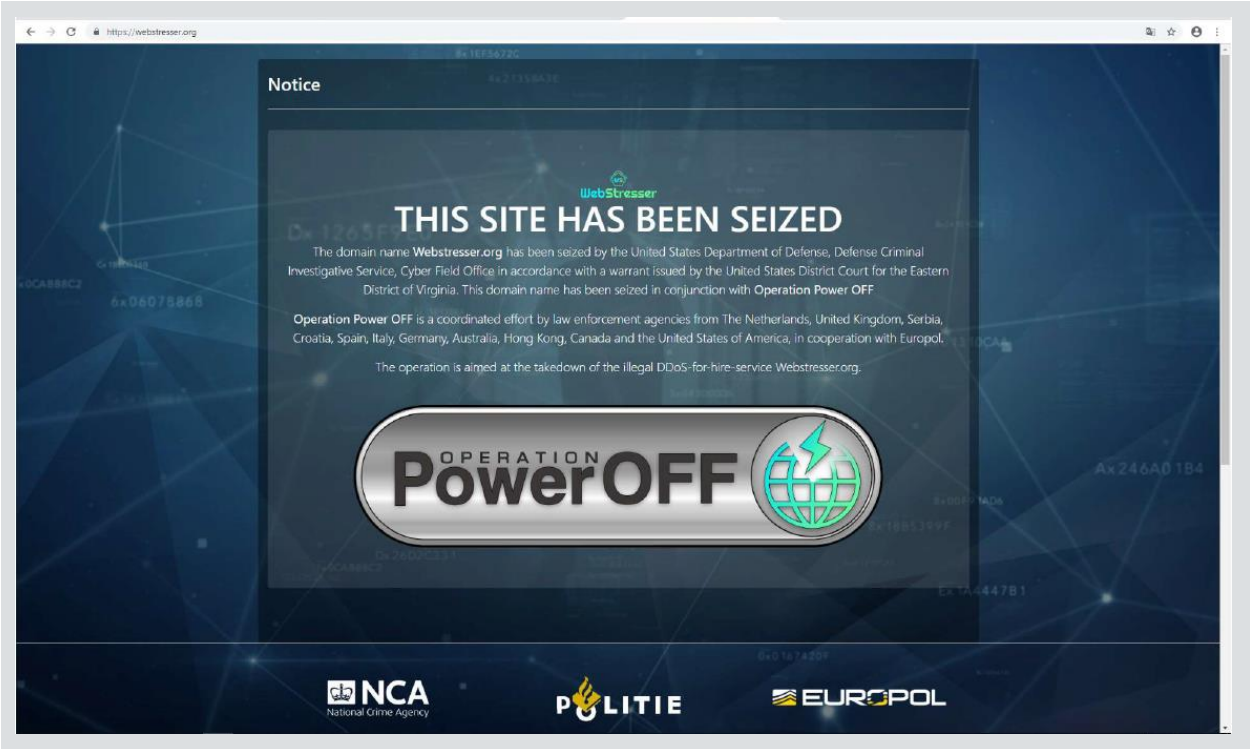
Der „Webstresser“-Server war bei einem bekannten deutschen Rechenzentrum in Frankfurt gehostet. Dieser wurde im Rahmen von operativen Maßnahmen beschlagnahmt und die Administratoren von „Webstresser.org“ am 24. April 2018 festgenommen. Mittlerweile müssen sich außerdem über 250 Nutzer dieser Plattform für DDoS-Angriffe vor Gericht verantworten.

„Webstresser.org“ wurde im Jahr 2015 eingeführt und war ursprünglich ein kleiner Dienst, der sich im Laufe der Jahre zum weltweit größten „DDoS-for-hire“-Marktplatz entwickelte. Bei „Webstresser“ waren rund 151.000 Nutzer registriert. Bis April 2018 sollen hierüber vier Mio. Angriffe erfolgt sein, welche sich v. a. gegen Regierungsbehörden, Banken, Polizeibehörden und die Spieleindustrie richteten. Angriffe waren bereits ab einem Betrag von 15 Euro zu realisieren.

Kurzbewertung:
Da sich Administratoren, Nutzer, Opfer und die Infrastruktur in verschiedenen Ländern befanden, war die gute internationale polizeiliche Zusammenarbeit maßgebliche Voraussetzung für das erfolgreiche strafprozessuale Vorgehen gegen die Verantwortlichen.

Nach Abschaltung des Portals wurde ein merklicher Rückgang der DDoS-Angriffe in ganz Europa festgestellt. Gleichwohl bleibt die „DDoS-for-hire“-Problematik, die wiederum unter den Begriff „Crime-as-a-Service“ subsumiert werden kann, generell bestehen.

[64] Bei einem Webinterface kann es sich um eine grafische Benutzeroberfläche, bei der der User z. B. unter Benutzung eines Web-Browsers mit dem System interagiert, oder um einen Webservice handeln, bei dem das System anderen Systemen verschiedene Funktionen und Daten zur Verfügung stellt.



Ende September 2018 meldete das BSI einen gezielten DDoS-Angriff gegen die Internetpräsenz des Energieversorgers RWE.[65] In einem auf der Plattform YouTube veröffentlichten Video hätten Unbekannte bereits im Vorfeld mit einem Angriff auf RWE-Server gedroht, sofern die Rodung des Hambacher Forstes fortgesetzt würde. Hacker attackierten die Webseite der RWE, indem sie vorsätzlich eine Flut von Anfragen erzeugten, die der Server für den Webseiten-Betrieb nicht mehr verarbeiten konnte. Infolgedessen war die Internetpräsenz zeitweise nicht erreichbar. Dies belegt, dass auch „politische Konflikte“ in den Cyberraum übertragen werden.

3.7 MOBILE MALWARE

Mobile Endgeräte wie Smartphones und Tablets verdrängen insbesondere in den privaten Haushalten, zunehmend den Computer. Laut einer Umfrage von „bitkom“ nutzen acht von zehn Menschen in Deutschland ein Smartphone.[66]

Damit geht einher, dass auch der Einsatz von „Mobile Malware“, spezifisch auf mobile Endgeräte abgestimmte Schadsoftware, seit Jahren stetig ansteigt [67]. Dieser Trend zeigt sich auch in einer Vielzahl an Delikts- und Angriffsarten auf Nutzer: Phishing, Social Engineering, Drive-by-Infection, Download von infizierten Apps oder Ausnutzung von Sicherheitslücken in den jeweiligen Betriebssystemen. Häufig werden Bank- und Zahlungsdaten gestohlen oder Daten der SIM-Karte per Malware unterschiedlichster Art abgegriffen. Auch dienen Smartphones häufig als Eintrittspforte für Malware, um weiter Firmensysteme und Geschäftsnetzwerke zu befallen.

[65] Cyber-Angriff auf RWE, abrufbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriff_RWE_25092018.html, veröffentlicht am 25.09.2018.
[66] Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro, veröffentlicht am 20.02.2019.
[67] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, abrufbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, S. 27.

Die Attraktivität von „Mobile Malware“ steigt seit Jahren an.

Ein weiteres Risiko der Infizierung mobiler Endgeräte mit Schadsoftware besteht beim Surfen der Anwender in offenen WLAN-Netzwerken oder beim Herunterladen von Apps aus unbekannten Quellen anstelle der offiziellen Stores. Aber selbst die Verwendung der offiziellen Stores von Google oder Apple garantieren keinen Schutz vor Schadsoftware. Immer wieder gelingt es Tätern, infizierte Apps auf die Plattformen der offiziellen Stores zu schleusen. Laut Symantec handele es sich bei 17 % aller Android-Apps tatsächlich um getarnte Malware.[68] Allein im Jahr 2018 hätten Forscher von Symantec im Google Play Store 38 schädliche Apps entdeckt, die ihr Vorhandensein auf den Geräten der Nutzer nach der Installation verschleiern.[69] Das Softwareunternehmen „Avast“ betonte in seinem Bericht „Mobile Threat Predictions“, dass im Jahr 2018 der Einsatz von Trojanern im Online-Banking Bereich bei mobilen Geräten um 150 % gegenüber dem Vorjahr angestiegen sei.[70] Zudem sollen das Auftreten von Fake-Apps um 24 % und von werbebasierter Malware um 49 % gestiegen sein.

McAfee unterstreicht ebenfalls die Zunahme an Malware auf mobilen Geräten im Jahr 2018. Fake - Apps gehörten zu den effektivsten Methoden, um Nutzer unauffällig zu täuschen und bösartige Anwendungen zu installieren.[71] Insbesondere Android-Nutzer sollen davon betroffen sein: Im Durchschnitt verzeichnete G-Data 11.700 neu-identifizierte „Mobile Malware“ für Android pro Tag, somit alle acht Sekunden eine neue Malware[72]. Allerdings würden auch vermehrt IOS-Endgeräte von Malware jeder Art geschädigt[73].

G-Data bezifferte die Anzahl der im Jahr 2018 auftretenden Malware-Variationen alleine für Android-Geräte auf ca. 4,1 Mio. - ein Zuwachs von knapp 27 % im Vergleich zum Vorjahr. Insgesamt, so McAfee, habe sich die Anzahl der im Umlauf befindlichen „Mobile Malware“ Varianten erstmalig auf über 30 Mio. belaufen.[74]

---

[68] Executive Summary - 2018 Internet Security Threat Report (ISTR), Volume 23, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf

[69] Hidden App Malware Found on Google Play, abrufbar unter: https://www.symantec.com/blogs/threat-intelligence/hidden-app-malware-google-play, 09.05.2018.

[70] 2019 Predictions, Part 2: Mobile threats, abrufbar unter: https://blog.avast.com/avast-mobile-threat-predictions, veröffentlicht am 09.01.2019.

[71] McAfee Mobile Threat Report Q1, 2019, abrufbar unter: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf, S. 2.

[72] Cyberangriffe auf Android-Geräte nehmen stark zu, abrufbar unter: https://www.gdata.de/blog/2018/11/31254-cyberangriffe-auf-android-gerate-nehmen-stark-zu, veröffentlicht am 07.11.2018.

[73] Sophoslabs 2019 Threat Report, abrufbar unter: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf, S. 20.

[74] G DATA Internet Security. Android erreicht Höchstwertung bei AV-Comparatives und AV-TEST, abrufbar unter: https://www.gdata.de/news/2019/04/31641-g-data-internet-security-android-erreicht-hochstwertung-bei-av-comparatives-und-av-test, veröffentlicht am 10.04.2019.

Insbesondere Mobile Ransomware erfreut sich immer größerer Beliebtheit unter Kriminellen: Laut Symantec belegt Deutschland in Bezug auf die Häufigkeit von Infizierungen durch Mobile Ransomware den dritten Platz hinter den USA und China.[75]Es sind v. a. mangelnde Sicherheitsvorkehrungen und fehlende Sicherheitsupdates, ferner unzureichende Verschlüsselungen persönlicher Daten, welche mobile Endgeräte als einfaches Ziel von Malware erscheinen lassen.

Mangelnde Sicherheitsvorkehrungen und fehlende Updates machen mobile Endgeräte besonders anfällig.

Laut Symantec befinden sich auf einem von 36 mobilen Endgeräten maliziöse Apps.[76]
Die Gesamtzahl der von Symantec blockierten, boshaften Apps betrage ca. 10.500 pro Tag.

Das BSI gibt an, dass mehr als einem Drittel der Smartphone-Nutzer nicht bekannt ist, dass ein Smartphone dieselben Sicherheitsvorkehrungen und Schutzmaßnahmen wie ein PC benötigt.[77]
Diesbezüglich ließen sich weitere, besonders auf Smartphones angepasste Angriffsvektoren identifizieren: Neben Phishing-Versuchen via E-Mail können besonders Instant Messaging Dienste wie Telegram oder WhatsApp und SMS für diese Zwecke zusätzlich verwendet werden.
Auch Social-Media-Apps wie Twitter oder Instagram können für Social Engineering missbraucht werden, indem dort Vertrauen und Authentizität, zwei Kernaspekte der Funktionsweisen Sozialer Medien, vorgetäuscht werden[78]. Auch das sog. URL-Padding[79] nutzt eine Besonderheit des Smartphones, nämlich seinen kleinen Bildschirm: Aufgrund der begrenzten Darstellungsfläche des Smartphones kann der Nutzer eine künstlich verlängerte URL nicht vollständig sehen. Diese zur Verschleierung der wahren Domain manipulierte URL führt zu einer kompromittierenden Webseite. Die Ziel-Webseite selbst dient als Download-Ort für Schadsoftware.

Ein besonderes Fallbeispiel für „Mobile Malware“ ist *Gustuff*, ein Trojaner, welcher spezifisch für das Betriebssystem Android geschrieben wurde. *Gustuff* wurde bereits mehrfach von seinen Entwicklern aktualisiert und mit diversen Funktionen erweitert. Zurzeit ist *Gustuff* in der Lage, Anmeldedaten von ca. 100 Banking-Apps und 32 Kryptowährungs-Apps zu stehlen.[80] Seine bevorzugten Ziele sind Banking-Apps; neuerdings kann *Gustuff* aber auch Daten von Bezahl- und Messaging-Apps wie PayPal, Skype und WhatsApp auslesen.

Im Gegensatz zu *Gustuff* verteilt sich *TimpDoor* über SMS und Textnachrichten. Via Phishing-Methoden soll das Opfer zum Herunterladen einer gefälschten Sprachnachrichten-App verleitet werden. Tatsächlich ermöglicht die Installation der App den Kriminellen, Sicherheitsmaßnahmen des Geräts zu umgehen und auf interne Netzwerke und Daten zuzugreifen.

---

[75] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, S. 41.
[76] Ebd.
[77] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6.
[78] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, abrufbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, S. 41.
[79] The Mobile Phishing Threat You'll See Very Soon: URL Padding, abrufbar unter: https://info.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding, veröffentlicht am 15.06.2017.
[80] Gustuff: Android-Trojaner nimmt mehr als 120 Banking- und Messaging-Apps ins Visier, abrufbar unter: https://www.zdnet.de/88357205/gustuff-android-trojaner-nimmt-mehr-als-120-banking-und-messaging-apps-ins-visier, veröffentlicht am 29.03.2019.

Das Gerät kann ferner, als Teil eines Botnetzes, für den Versand weiterer Phishing-Nachrichten oder DDoS-Attacken missbraucht werden.[81]

Wie in den meisten Phänomenbereichen des Deliktfelds Cybercrime ist von einem überdurchschnittlich hohen Dunkelfeld auszugehen. Dies ist primär auf eine niedrige Anzeigequote, aber auch auf Unwissenheit darüber, tatsächlich Opfer eines Verbrechens geworden zu sein, zurückzuführen. Besonders Letzteres stellt ein immer häufiger auftretendes Problem dar: Kryptojacking-Malware und weitere Schadsoftware entwickeln sich hinsichtlich ihrer Techniken zur Verschleierung der eigenen Existenz sowie der Tarnung auf dem Zielsystem ständig weiter.

[81] McAfee Labs Threats Report, December 2018, abrufbar unter https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf, S. 12.

3.8 UNDERGROUND ECONOMY – DIGITALE SCHWARZMÄRKTE

Illegale Foren oder Marktplätze im Clearnet, Deepweb und im Darknet spielen weiterhin eine zunehmende Rolle bei der Begehung von Cybercrime.

Begriffsbestimmungen

Clearnet: *(auch: Visible Web, Surface Web, Open Web). Das der Allgemeinheit „bekannte" Internet; es ist für jedermann zugänglich, bedienbar mit normalen Browserprogrammen und z. B. unterstützt durch einfache Handhabung mittels Suchmaschinen. Auch im Clearnet sind vielfältige illegale Inhalte vorhanden, z. B. Delikte politisch motivierter Kriminalität, Verbreitung von Kinderpornografie, Seiten der „Underground Economy" (Straftaten überwiegend aus dem Bereich der Cybercrime im engeren Sinne) u. v. m.*

Deep Web: *(auch Hidden Web, Invisible Web). Der Teil des Internet, dessen Inhalte nicht durch Suchmaschinen auffindbar sind, weil z. B. Webseiten nicht indexiert/in Suchmaschinen verlinkt wurden oder weil sie nicht für den Gebrauch von jedermann gedacht sind. Inhalte des Deep Web können z. B. Datenbanken, Intranets oder Fachwebseiten sein und sind - sofern die URL bekannt ist und eine Zugangsberechtigung besteht – mit „normalen" Browsern erreichbar.*

Darknet: *Das Darknet ist dadurch gekennzeichnet, dass die Inhalte ausschließlich durch Nutzung spezieller Software, die der Anonymisierung dient, einsehbar sind. Bestandteile des Darknet sind z. B. Foren, Blogs/Wikis mit unterschiedlichsten – auch legalen – Zielrichtungen. In großen Teilen sind die Inhalte des Darknet jedoch als illegal einzustufen. Einen bedeutenden Teil machen z. B. die Darknet-Märkte aus, bei denen (größtenteils inkriminierte) Güter anonym gehandelt werden. Auch bestehen zahlreiche Angebote für Crime-as-a-Service (das Angebot, kriminelle Handlungen im Auftrag durchzuführen) oder Darknet-Seiten mit kinderpornografischen Inhalten. Andere Bereiche des Darknet unterscheiden sich vom Aufbau und der Nutzung her nicht vom Clearnet. Auch im Darknet werden in Foren Meinungen geäußert und Diskussionen geführt, Wikis enthalten Erläuterungen. Allerdings bezieht sich beides im Darknet meist auf illegale Aktivitäten und Inhalte (z. B. Betäubungsmittel).*

Nachfolgend werden die Straftatbestände aufgeführt, die über die vorgenannten Marktplätze i. d. R. verwirklicht werden

- Unerlaubter und gewerbsmäßiger Handel mit Betäubungsmitteln,
- gewerbsmäßiger Handel mit Waffen, Kriegswaffen und Explosivstoffen ohne die erforderliche Erlaubnis,
- gewerbsmäßige Geldfälschung und Inverkehrbringen,
- Verbreitung, Erwerb und Besitz kinderpornografischer Schriften,
- gewerbsmäßige Urkundenfälschung und Handel damit,
- Ausspähen von Daten und Datenhehlerei,
- gewerbsmäßiger Computerbetrug,
- Verstöße gegen die Strafvorschriften des Arzneimittelgesetzes.

Auf nahezu jedem Darknet-Markt stellt das Angebot an verbotenen Betäubungsmitteln die mit Abstand größte Warengruppe dar. Die Dimension dieser Angebote ist mittlerweile als Massendelikt zu bezeichnen. Nationale wie internationale Ermittlungen sowohl gegen Plattformbetreiber als auch Anbieter (sog. Vendoren) belegen, dass ein hohes Angebot nahezu aller Betäubungsmittelarten inkl. Neuer Psychoaktiver Stoffe (NPS) sowohl im Clearnet als auch im Darknet festgestellt werden kann.

Betäubungsmittel stellen die größte Warengruppe im Darknet dar.

Der Anteil von Waffenangeboten ist im Vergleich zum Angebot anderer inkriminierter Güter im Darknet deutlich geringer. Mit Blick auf das grundsätzlich vorhandene Gefährdungspotenzial von Waffen haben polizeiliche Aktivitäten im Darknet zur Identifizierung von realen Waffenangeboten und potenziellen Waffenerwerbern aus Deutschland jedoch besondere Bedeutung. Mittlerweile wird der Handel mit erlaubnispflichtigen Schusswaffen bei den meisten Plattformen untersagt. User/Vendoren, die hiergegen verstoßen und diese „forbidden goods“ veräußern bzw. kaufen, werden von den Marktplätzen ausgeschlossen. Ähnlich verhält es sich bei Materialien mit kinderpornografischen Inhalten – auch diese werden vielfach als „forbidden goods“ eingestuft.

Kryptowährungen sind im Darknet ein beliebtes Zahlungsmittel.

Bei Darknet-Märkten ist die finanzielle Gewinnerzielung vorrangig. Die Administratoren der Foren und Marktplätze partizipieren häufig über ein Treuhand-System an den Erlösen aus dem Verkauf der illegalen Waren. Zur Bezahlung der gehandelten Waren werden ausschließlich digitale Kryptowährungen akzeptiert, die ein anonymes bzw. pseudonymes Bezahlen ermöglichen sollen. Hingegen geht es z. B. bei Seiten, die durch pädosexuelle Nutzer besucht werden, vorwiegend um das Tauschen kinderpornografischer Inhalte oder im Bereich politisch motivierter Kriminalität um den Informationsaustausch mit Gleichgesinnten oder die Werbung für die eigenen politischen Ziele.

Mit Blick auf die steigende Nutzung digitaler Angebote ist anzunehmen, dass der Trend zur immer stärkeren Nutzung des Internets und des Darknets als Tatmittel weiter zunehmen wird. Dabei ist ebenso wahrscheinlich, dass die Nutzungsformen – unter Ausnutzung der technischen Entwicklung – immer weiter professionalisiert werden.

Nach der Abschaltung der digitalen Schwarzmärkte *Alpha Bay* und *Hansa Market* im Jahr 2017 wurden seitens der zuständigen Strafverfolgungsbehörden in Deutschland intensive Ermittlungen geführt, die ergaben, dass sich User und Vendoren Alternativen gesucht haben. Stellte man in der Vergangenheit fest, dass nach der Abschaltung von Marktplätzen neue, kleinere Marktplätze gegründet wurden, verhielt sich dies im Jahr 2018 anders. Die Kauf- und Verkaufsaktivitäten verlagerten sich auf wenige, größere und vermeintlich „sichere" Plattformen. Zu einer dieser Plattformen zählte der digitale Schwarzmarkt *Wall Street Market*.

Fallbeispiel: Wall Street Market

Seit November 2017 ermittelte das BKA unter der Sachleitung der Generalstaatsanwaltschaft Frankfurt/M., ZIT gegen die Betreiber und Administratoren des digitalen Schwarzmarktes *Wall Street Market* (WSM). Im Rahmen der Ermittlungen erfolgte eine intensive Zusammenarbeit der Strafverfolgungsbehörden auf nationaler und internationaler Ebene, u. a. mit den Niederlanden, den USA und EUROPOL.

Bei WSM handelte es sich im Zeitraum der Ermittlungen um eine der größten Darknet-Plattformen, die dem unerlaubten Handel mit verschiedenen Waren, hierbei insbesondere Betäubungsmittel (BtM), diente. Die Handelsplattform war ebenso wie das dazugehörige Forum nur über das TOR-Netzwerk erreichbar.

Ein Großteil der Waren, insbesondere BtM, wurde aus Deutschland verschickt. Im Verlauf der Ermittlungen konnten über 400.000 Verkäufe registriert werden, die über die Plattform erfolgreich abgeschlossen wurden. In 250.000 Fällen wurden hierbei Geschäfte mit illegalen BtM durchgeführt, die insbesondere aus Deutschland verschickt wurden. Durchschnittlich erfolgten ca. 1.250 Transaktionen pro Tag, wobei die Betreiber/Administratoren jeweils eine Verkaufsprovision von zwei bis sechs Prozent der Verkaufssumme erhielten. Für die Bezahlung verwendeten die Nutzer des Online-Marktplatzes die Kryptowährungen *Bitcoin* und *Monero*.

Als die mutmaßlich Verantwortlichen des illegalen Online-Marktplatzes (drei deutsche Staatsangehörige) begannen, bereits zum Marktplatz transferierte Geldbeträge der Kunden an sich selbst zu übersenden (sog. „Exit-Scam"), erfolgten umfangreiche Durchsuchungsmaßnahmen. In den Wohnungen der Tatverdächtigen wurden insgesamt über 550.000 Euro Bargeld sowie Kryptowährungen *Bitcoin* und *Monero* im umgerechnet zweistelligen Millionen-Euro-Bereich, mehrere hochwertige Kraftfahrzeuge und zahlreiche weitere Beweismittel (v. a. Computer und Datenträger) sichergestellt.

Die WSM-Infrastruktur erstreckte sich auf Server in Deutschland, den Niederlanden und Rumänien. Bis zum 02.05.2019 konnten weitere rechtliche und technische Voraussetzungen zur koordinierten Abschaltung/Übernahme der technischen Infrastruktur von WSM geschaffen und dies öffentlichkeitswirksam per Seizure Banner dokumentiert werden.

Kurzbewertung:
Durch intensive Ermittlungen konnte einer der größten und international bedeutendsten Darknet-Märkte abgeschalten werden. Dies gelang trotz der Tatsache, dass das täterseitige Vorgehen in hohem Maße anonymisiert und konspirativ erfolgte und die technische Infrastruktur von WSM komplex aufgebaut und über mehrere Staaten verteilt war. Die intensive und vertrauensvolle Zusammenarbeit zahlreicher nationaler und internationaler Strafverfolgungs- und Sicherheitsbehörden hat wesentlich zu dem Ermittlungserfolg beigetragen.

Inklusive des WSM wurden seit dem Jahr 2017 insgesamt sechs digitale Marktplätze bzw. Foren und Newsseiten unter Beteiligung deutscher Strafverfolgungsbehörden abgeschaltet:

- *Deutschland im Deep Web* – offizieller Beginn: März 2013, abgeschaltet: Juni 2017
- *AlphaBay* – offizieller Beginn: Dezember 2014, abgeschaltet: Juli 2017
- *Hansa Market* – offizieller Beginn: Juli 2015, abgeschaltet: Juli 2017
- *Silkkitie / Valhalla Market* – offizieller Beginn: Oktober 2013, abgeschaltet: April 2019
- *deepdotweb.com* – offizieller Beginn: Oktober 2013, abgeschaltet: Mai 2019

In vier Fällen wurden die Ermittlungen vom BKA geführt. Die Anzahl der registrierten Nutzer je Plattform reichte von ca. 23.000 bis ca. 1,8 Millionen. Die erzielten Gewinne der illegalen Marktplätze variierten dementsprechend. Im Falle des AlphaBay-Marktplatzes belief sich der Gewinn auf ca. 628 Mio. Euro.

Cybercrime-as-a-Service

Die Underground Economy stellt eine große Bandbreite an illegalen Angeboten bzw. Dienstleistungen zur Verfügung, welche die Durchführung jeder Art von Cybercrime ermöglichen bzw. erleichtern. Das Angebot umfasst z. B.

- digitalen Datendiebstahl,
- Bereitstellung von Botnetzen für verschiedene kriminelle Aktivitäten,
- DDoS-Attacken,
- Malware-Herstellung und -Verteilung,
- Verkauf/Angebot kompromittierter, sensibler Daten, z. B. Zugangs- oder Zahlungsdaten,
- Vermittlung von Finanz- oder Warenagenten zur Verschleierung der Herkunft und Sicherung durch Straftaten erlangter Finanzmittel oder Waren,
- Kommunikationsplattformen zum Austausch von kriminellem Know-how, z. B. Foren,
- Anonymisierungs- und Hosting-Dienste zur Verschleierung eigener Identitäten und
- passwortgeschützte „Dropzones“ (digitale Speicherorte) zur Ablage illegal erlangter Daten bzw. Informationen, z. B. Passwörter und Kontodaten.

Darüber hinaus werden den Nutzern auf derartigen Plattformen häufig auch flankierende Unterstützungsleistungen angeboten, wie z. B.

- Updates von Schadsoftware,
- Beratungsdienste,
- weitergehende Anti-Erkennungsmechanismen,
- Hilfestellung bei technischen Problemen.

Die Auflistung verdeutlicht, dass potenzielle Straftäter auch ohne eigene technische Fähigkeiten und mit geringem Aufwand Zugang zu ausgefeilten und gefährlichen Werkzeugen erhalten, mit denen vielfältige Angriffe aus dem Bereich der Cybercrime ausgeführt und gegen eine Identifizierung des Urhebers abgesichert werden können.

Kriminelles Know-How kann von jedermann im Netz erworben werden.

Die Phänomene Malware/Ransomware, Botnetze und DDoS sind Beleg für die umfängliche Umsetzung des „Cybercrime-as-a-Service“-Gedankens bzw. dieses Geschäftsmodells.

3.9 DIGITALE WÄHRUNGEN

Kryptowährungen, z. B. *Bitcoin* (BTC), *Tether* (USDT) oder *Monero* (XMR), sind digitale bzw. virtuelle Zahlungsmittel, deren Genese und Verwendung auf mathematischen Berechnungen, kryptografischen Verfahren und digitalen Signaturen beruhen. Ihre Nutzung durch Privatpersonen setzt lediglich die Installation einer bestimmten Software zur Einrichtung eines digitalen Kontos (sog. „Wallet“) voraus. Auf zahlreichen Plattformen wie *Coinbase*, *Gemini* oder *BitPanda* sind der legale Erwerb wie auch die Veräußerung verschiedener Kryptowährungen möglich. Die meisten Kryptowährungen basieren technisch auf dem Prinzip der „Blockchain“, welches beschrieben werden kann als ein öffentliches oder privates, dezentral geführtes, digitales Buchführungssystem zur kontinuierlichen Aufzeichnung von Transaktionen (Distributed Ledger Technology).

Kryptowährungen als solche, ihre Generierung und auch ihre Verwendung sind grundsätzlich legal. Auf unzähligen Plattformen können Kryptowährungen legal veräußert oder als Zahlungsmittel eingesetzt werden. Aufgrund der dezentralen Buchführung, der nichtstaatlichen oder nicht durch Banken regulierten Aufsicht, der schnellen, globalen Erreichbarkeit und Verwendbarkeit im internationalen Handel und der Pseudoanonymität als Teil eines Netzwerkes haben sich Kryptowährungen als ein beliebtes Zahlungsmittel von Kriminellen etabliert. Durch ihre Verwendung ist eine grundsätzliche Verschleierung von Identitäten möglich: Zwar ist nachzuverfolgen, dass Transaktionen getätigt wurden und welche Sende- wie auch Zieladresse diese Transaktion besitzt, jedoch ist nicht einsehbar, wer die Besitzer der an den Transaktionen beteiligten Wallets sind.

Damit einhergehend stehen Kryptowährungen nicht nur als Mittel zum Zweck im Fokus krimineller Aktivitäten, sondern auch als zu erbeutendes Ziel: Betrugsversuche (engl. Scams), Diebstahl digitaler Geldbörsen, Kryptojacking sowie das Ausnutzen technischer Infrastrukturen für kriminelle Zwecke sind dabei nur einige Deliktsbereiche, welche sich um Kryptowährungen etabliert haben. Auch Geldwäsche digitaler Beträge ist ein zunehmendes Phänomen,[82] das durch unregulierte Handelsplattformen, unzureichende Sicherheitsmaßnahmen für Wallets und Krypto-Tauschbörsen oder auch durch fehlende Umsetzung von Anti-Geldwäsche-Gesetzen im Internet (z. B. mangelnde Identifikationsverifizierungen oder andere Know-Your-Customer-Verfahren) zusätzlich gefördert wird.

Es ist davon auszugehen, dass durch die zunehmende Akzeptanz von digitalen Währungen auf dem freien Markt sowie das Erscheinen von neuen, auf erweiterte Anonymität setzenden Kryptowährungen zusätzliche Anreize zur Verwendung im kriminellen Kontext geschaffen werden.

3.10 TECHNICAL SUPPORT SCAMS / SEXTORTION

Die Cybercrime-Dienststellen wurden im Jahr 2018 nicht nur mit der Bearbeitung von Phänomen der Cybercrime im engeren Sinne konfrontiert. So stellten Phänomene wie der „Technical Support Scam“ oder die Bearbeitung einer großen Anzahl von „Sextortion“-Fällen die Strafverfolgungsbehörden vor weitere Herausforderungen.

Bei „Technical Support Scams“ handelt es sich um eine Betrugsart: Am Telefon geben Betrüger an, dass sie Support-Mitarbeiter einer Software-Firma seien (z. B. Microsoft) und dass ein gravierendes Problem bzgl. des Computers des Opfers vorliege. Die Betrüger weisen das Opfer an, ein Remote

[82] Geldwäscheverdacht bei Kryptowährungen, abrufbar unter: https://www.bundestag.de/hib#url=L3ByZXNzZS9oaWIvNjQ4OTA2LTY0ODkwNg==&mod=mod454590, veröffentlicht am 21.06.2019.

Access Tool [83] zu installieren, um eine vermeintliche Fernwartung und Behebung des Problems durchführen zu können. Aus der Ferne werden dann allerdings Daten des Opfers manipuliert, Daten ausgelesen oder Malware installiert. [84] Mitunter wird dieser Betrug mit folgendem Modus Operandi vorbereitet: Über kompromittierte Webseiten werden dem Opfer falsche Warn- und Fehlermeldungen angezeigt. Gleichzeitig präsentiert die gefälschte Meldung eine vermeintliche Support-Hotline, tatsächlich betrieben von Betrügern, die das Opfer anrufen soll. Am Ende des Vorgangs erhält das Opfer eine Zahlungsaufforderung, sei es in Form einer falschen Rechnung oder aber durch die Infizierung mit einer Ransomware.

„Sextortion" hingegen ist eine Art der Erpressung, welche darauf basiert, dass Täter angeblich den Computer bzw. die Webcam ihres Opfers gehackt und es beim Besuchen von pornografischen Webseiten bzw. beim Masturbieren gefilmt hätten. Gedroht wird mit der Veröffentlichung des angeblich vorliegenden Materials per E-Mail an die Kontaktliste des Opfers oder auf sozialen Netzwerken.[85] Insbesondere geben die Täter vor, dass das Opfer dies einzig durch die Überweisung eines monetären Betrags an die Erpresser verhindern könne.

3.11 „LIVING-OF-THE-LAND" / „SUPPLY-CHAIN-ATTACKS"

Die im Phänomenbereich Cybercrime bereits bekannten „Living-of-the-Land"-Methoden (LotL) und „Supply-Chain-Attacks" haben im Jahr 2018 einen signifikanten Anstieg erfahren und könnten aufgrund inhärenter Spezifika auch künftig von Cyberkriminellen weiter verstärkt genutzt werden.

„LotL"-Methoden, auch bekannt als „Fileless Attack" oder „Fileless Malware", unterscheiden sich gegenüber „traditionellen" Angriffsarten insofern, dass primär keine externe Malware auf dem Zielsystem installiert wird. Vielmehr nutzen Angreifer bereits auf dem Zielsystem vorhandene Admin- bzw. System-Tools, Skripte oder Software-Makros wie Powershell oder MS-Office, um einen Angriff zu initiieren. Zweck dieser Angriffe ist oftmals Datendiebstahl, Spionage oder die Verbreitung weiterer Malware.

Da zunächst keine Malware installiert wird, sondern gebräuchliche Tools und Software bösartig zweckentfremdet werden, hinterlassen derartige Angriffe nur minimal modifizierte Systemdateien und sind daher nur schwer zu entdecken und zurückzuverfolgen. Aufgrund dessen ist diese Art des Angriffs sehr beliebt unter Kriminellen: Laut Symantec hat sich die Anzahl der blockierten bösartigen Powershell-Skripte, einem Admin-Skript von Windows-Systemen, im Jahr 2018 um 1.000 % im Vergleich zum Vorjahr erhöht. Auch konnten vermehrte Angriffe auf MS-Office-Dokumente festgestellt werden.[86]

„Supply-Chain-Attacks" verfolgen einen anderen, indirekteren Ansatz: Hierzu werden zunächst Teilsysteme, Informations- und Kommunikationsketten, Clouds oder Software von Dritten infiziert. Über diese erfolgt dann die weitere Verbreitung der Malware und die Infizierung des eigentlichen Zielsystems, oftmals Systeme von Unternehmen. Insofern stellt das zuerst attackierte Opfer die Brücke zum eigentlichen Ziel dar. Im September 2017 wurde die Software *CCleaner* durch un-

[83] Remote Access Tools ermöglichen den Fernzugriff auf einen Computer von einem anderen Computer aus. Hierbei können sämtliche Eingaben aus der Ferne vorgenommen werden (Tastatur, Maus).
[84] Protect yourself from tech support scams, abrufbar unter: https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams.
[85] Sextortion Bitcoin scam makes unwelcome return, abrufbar unter: https://blog.malwarebytes.com/cybercrime/2019/02/sextortion-bitcoin-scam-makes-unwelcome-return, veröffentlicht am 11.02.2019.
[86] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, S. 11.

bekannte Hacker infiziert und als solch ein Eintrittspunkt missbraucht. Das infizierte Programm wurde dann von ca. 2,3 Mio. Anwendern heruntergeladen.[87] Die Malware im infizierten Programm las Daten und Informationen der Nutzer aus und entschied, welche Nutzer als eigentliches Ziel geeignet waren. In der Folge sollten diese dann mit weiterer Malware infiziert werden. Das eigentliche Ziel des Angriffs war es, Daten von hochrangigen Angestellten diverser Unternehmen auszuspähen.

„Supply-Chain-Attacks" suchen sich die Teile der „Supply-Chain", welche am schwächsten geschützt sind. Ist ein Teil der „Supply-Chain" infiziert, kann der Angreifer zu seinem eigentlichen Ziel vordringen. Auch diese Art von Angriff ist aufgrund seiner indirekten Art und teilweise internationalen Verbundketten zwischen Systemen schwer zu erkennen. Ebenso sind die Arten der ersten Infizierung vielfältig und können auf Malware, Spear-Phishing[88] oder Social Engineering basieren.

Ein Fallbeispiel für eine kombinierte „Supply-Chain-Attack" mit „LotL"-Methoden war *Petya*, eine Ransomware, welche sich v. a. in der Ukraine ausbreitete. Obwohl das Ziel von *Petya* Systeme von dort ansässigen multinationalen Unternehmen waren, begann der Angriff bei *MEDoc*. Dabei handelt es sich um eine in der Ukraine beliebte Steuersoftware, die auch von den täterseitig anvisierten internationalen Firmen genutzt wird. Von MEDoc aus verbreitete sich *Petya* via Ausnutzung auf den Systemen vorhandener Ressourcen, wie z. B. der Windows Management Instrumentation Command-Line oder dem Windows Server Message Block, weiter in seine eigentlichen Zielsysteme.[89]

3.12 CLOUD-COMPUTING / ZUNEHMENDE VERNETZUNG DURCH DAS INTERNET DER DINGE

Der Bereich Cloud-Computing wird durch weitere Entwicklungen für Strafverfolgungsbehörden und auch für Kriminelle an Relevanz gewinnen. Im Jahr 2018 wurden neuerlich Häufungen von Angriffen auf Cloud-Instanzen verzeichnet. Bspw. wurden auf Amazons Cloud-Service AWS S3-Bucket vermehrte Angriffe verzeichnet, bei denen insgesamt ca. 70 Mio. Datensätze gestohlen wurden.[90]

Die schlechte Sicherung von Cloud-Instanzen birgt für Unternehmen nach wie vor ein großes Risiko. Besonders für den Wirtschaftsstandort Deutschland bedeuten derartige Angriffe Ausfälle im Geschäftsprozess wie auch Reputationsverluste bei Kunden.

Cloud Computing gewinnt weiter an Bedeutung.

Auch das sog. Internet der Dinge bzw. Internet of Things (IoT) muss - v. a. aufgrund der stark zunehmenden Nutzung von entsprechenden Geräten – als sehr hoher Unsicherheitsfaktor bewertet werden. Im Durchschnitt verfügt jeder deutsche Haushalt über sechs IoT-Geräte, welche durch Exploits oder einfache Passwörter grundsätzlichen Risiken ausgesetzt sind. Scan-Listen und

[87] Do not become a link in a supply chain attack, abrufbar unter: https://www.kaspersky.com/blog/ccleaner-supply-chain/21785, veröffentlicht am 26.03.2018.
[88] Beim "Spear-Phishing" werden betrügerische E-Mails an täterseitig gezielt ausgewählte Organisationen versendet. Diese enthalten z. B. einen Internet-Link, der - einmal durch einen Mitarbeiter betätigt - Malware auf dem betroffenen Rechner installiert.
[89] Petya ransomware outbreak: Here's what you need to know, abrufbar unter https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper, veröffentlicht am 24.10.2017.
[90] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, abrufbar unter: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, S. 19.

spezielle Suchmaschinen wie *Shodan* vereinfachen der Täterseite die entsprechende Vorbereitung, indem sie mit dem Internet verbundene Geräte auflisten, darunter Web-Kameras oder gar Ampelanlagen.

Pro Haushalt gibt es in Deutschland durchschnittlich sechs IoT-Geräte.

Besonders gefährdet sind IoT-Geräte ferner durch die stets wachsende Anzahl an IoT-Malware. So wurde allein im dritten Quartal des Jahres 2018 ca. 45.000 neu aufgekommene, für IoT-Geräte spezifizierte Malware identifiziert.[91] Das vermehrte Nutzen von IoT-Geräten direkt am Arbeitsplatz (Sprachassistenten, Sicherheitskameras etc.), erhöht zudem die Bedrohung für Firmennetzwerke und Unternehmenssysteme weiter.

3.13 MASCHINELLES LERNEN

Der Einsatz künstlicher Intelligenz bzw. das maschinelle Lernen bleibt weiterhin ein wichtiges Phänomen der digitalen Welt. Dieser Bereich bietet Chancen, birgt aber auch Risiken. Zur Abwehr von Cyberdelikten besteht die Möglichkeit, Künstliche Intelligenz (KI) und maschinelles Lernen dazu zu verwenden, Anomalien in Netzwerken und Systemen frühzeitig zu erkennen oder Malware zu entdecken und zu beseitigen. V. a. für Unternehmen wäre dies eine positive Entwicklung im Hinblick auf die Sicherheit ihrer Daten.

Künstliche Intelligenz birgt Chancen und Risiken.

Auch für Strafverfolgungsbehörden dürften sich neue Möglichkeiten ergeben. Die Polizei Niedersachsen entwickelt mit dem Projekt „Cyberguide“ eine interaktive Geschäftsprozessanwendung. Es stellt in Aussicht, dass durch maschinelles Lernen Geschäftsprozesse und Vorgangsbearbeitungen automatisiert werden können. „Cyberguide“ soll so z. B. perspektivisch zur Anzeigeaufnahme im Bereich Cybercrime eingesetzt werden. Zunächst soll „Cyberguide“ über Frage-Antwort-Prozesse lernen, Sachverhalte korrekt einzuordnen, um dann mit Zugriff auf diverse Wissensbestände Hinweise auf Zuständigkeiten und zu ergreifende Maßnahmen zu liefern.[92]

Aber auch Kriminelle werden maschinelles Lernen nutzen - für illegale Zwecke. Es ist u. a. zu befürchten, dass KI genutzt wird, um mit Malware zu kommunizieren; außerdem könnte KI als Monitoring-Programm für Malware fungieren und diese dynamisch steuern, indem sie z. B. Entscheidungen über die anzusteuernden Dateien bzw. Dateipfade auf dem kompromittierten System trifft. Ebenso ist nicht auszuschließen, dass KI pseudoauthentische Zertifikate zur Täuschung von Sicherheitssystemen erstellen bzw. fälschen kann.[93] Weiter könnte es möglich sein, dass KI für Phishing bzw. Social Engineering verwendet wird, indem von ihr Informationen im Internet über das Ziel gesucht und zusammengetragen, automatisierte E-Mails geschrieben oder gar Chatbots imitiert werden.

---

[91] McAfee Labs Threats Report, December 2018, abrufbar unter: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf, S. 28.

[92] proPOLIZEI. Informationen für Niedersachsens Polizei, Heft Mai/Juni 2016, abrufbar unter: https://www.polizei-nds.de/download/72565/proPOLIZEI_Mai_Juni_2016.pdf, S. 5 ff.

[93] Under the Radar – The Future of Undetected Malware, abrufbar unter: https://resources.malwarebytes.com/files/2018/12/Malwarebytes-Labs-Under-The-Radar-APAC-1.pdf, S. 10.

4 Angriffe auf Wirtschafts-unternehmen/Angriffe auf Kritische Infrastrukturen

Cyberangriffe zielen nicht nur auf Behörden ab, sondern auch auf Unternehmen: Hierbei werden Daten ausgespäht, verändert oder zerstört; ebenso werden Webserver in ihrer Erreichbarkeit beeinträchtigt und/oder mit Schadsoftware infiziert sowie auf Servern vorgehaltene Inhalte manipuliert.

In diesem Kontext ergeben sich neue Gefahrenpotenziale und Auswirkungen durch Cyberangriffe auf die „Zentralen Nervensysteme" der Gesellschaft, die sog. Kritischen Infrastrukturen (KRITIS). Hierunter fallen die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Transport und Verkehr, Gesundheit, Medien und Kultur sowie Staat und Verwaltung.

Der reibungslose Betrieb Kritischer Infrastrukturen sichert die Funktionalität und fundamentale Prozesse moderner Gesellschaften, eine zeitgemäße IT-Infrastruktur erhöht ihre Leistungs- und Zukunftsfähigkeit. Daher kommt einer zeitnahen und wirksamen polizeilichen Interventionsfähigkeit im Rahmen polizeilicher Gefahrenabwehr und Strafverfolgung eine herausragende Bedeutung zu.

In Deutschland wurden bereits diverse beeinträchtigende Cyberangriffe auf Unternehmen der KRITIS-Sektoren, wie z. B. Gesundheit, Transport und Verkehr sowie Energie, verzeichnet.
Den bei den Landeskriminalämtern und dem BKA angesiedelten Zentralen Ansprechstellen Cybercrime gelangten im Zeitraum 01.10.2017 bis 25.10.2018 insgesamt 21 Cyberangriffe auf KRITIS-Unternehmen[94] zur Kenntnis.

Für die KRITIS-Unternehmen besteht bei festgestellten Störungen nach dem BSI-Gesetz eine Verpflichtung zur Meldung an das BSI. In seinem Lagebericht 2018 weist das BSI für den Zeitraum 01.06.2017 bis 31.05.2018 insgesamt 145 Meldungen aus. Der Schwerpunkt lag wie im Jahr zuvor im Sektor Informationstechnik und Telekommunikation.[95]

Von einer weiteren Zunahme derartiger Angriffsversuche auf Kritische Infrastrukturen und damit verbundener gefährdungsrelevanter Auswirkungen ist auszugehen.

Angriffe staatlicher Akteure erfolgen zumeist in Form von Advanced Persistent Threats (APT). Diese sind eine ernstzunehmende und weiterhin steigende Bedrohung für die Wirtschaft sowie für öffentliche und nicht-öffentliche Stellen und Institutionen. Dies gilt besonders für Unternehmen der KRITIS.

[94] Kritische Infrastrukturen (KRITIS) sind definiert als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

[95] Die Lage der IT-Sicherheit in Deutschland 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, S. 10.

APT-Angriffe (Advanced Persistent Threat)

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Kennzeichnend für APT-Angriffe ist, dass sie sowohl zur Spionage, das heißt zum Ausspähen von Daten, als auch zur Sabotage, also zum Stören von Abläufen, genutzt werden.

Das BKA stellt im Bereich der Cyberspionage Folgendes fest:

- Cyber-Angriffe gegen Deutschland haben sich als eine wichtige Methode der Informationsgewinnung für ausländische Nachrichtendienste etabliert.

- Weltweit werden bei Cyberspionage-Angriffen immer wieder dynamisch gestaltete Serverinfrastrukturen sowie hoch professionelle und einer steten Weiterentwicklung unterliegende Schadsoftwarekomponenten verwendet.

- Hauptangriffsvektor ist der Versand von „Spear-Phishing-E-Mails“[96], sowohl mit maliziösen Links als auch mit Schadanhang, mittels derer die Systeme der Geschädigten infiziert werden. Den Cyberspionage-Angriffen gehen in der Regel professionelle Abklärungen der Zielpersonen voraus. Dies geschieht nicht nur durch gezielte Aufklärung im Internet und in Sozialen Medien, sondern auch durch klassische Spionage in Form von Fernmeldeaufklärung und den Einsatz von Agenten.

- Veröffentlichungen zahlreicher IT-Sicherheitsunternehmen weisen regelmäßig auch auf eine Betroffenheit Deutschlands bei Cyberspionage-Angriffen hin. Eine konkrete und tatsächlich belastbare Attribution ist bei diesen staatlich/nachrichtendienstlich gesteuerten Angriffen nur schwer möglich.

- Es ist von einer hohen Dunkelziffer durch nicht erkannte bzw. nicht angezeigte Angriffe auszugehen.

Es ist davon auszugehen, dass der Wirtschaftsstandort Deutschland aufgrund der vergleichsweise hohen Konkurrenzfähigkeit und technologischen Expertise der angesiedelten Unternehmen ein interessantes Ziel für Cyber-Spionage und/oder allgemeinkriminelle Hacker bleiben wird.

[96] Verfeinertes Phishing mit einem gezielteren persönlichen Ansatz („spear“ – steht für Speer).

5 Schäden durch Cybercrime

Cybercrime verursacht bei Bürgern, Behörden und Wirtschaftsunternehmen hohe materielle und immaterielle Schäden, die bis zur Existenzgefährdung reichen können.[97] Millionenfacher Datendiebstahl, Manipulationen einer Vielzahl von technischen Geräten und die entsprechende Berichterstattung in den Medien führen zu einer deutlichen Beeinträchtigung des Sicherheitsgefühls der Bevölkerung Einer Umfrage des BSI und des Programms Polizeiliche Kriminalprävention (ProPK)[98] zufolge schätzten etwa ein Drittel der Befragten (29 %) ihre persönliche Gefahr, Opfer von Cyber-Kriminalität zu werden, als hoch oder sehr hoch ein[99].

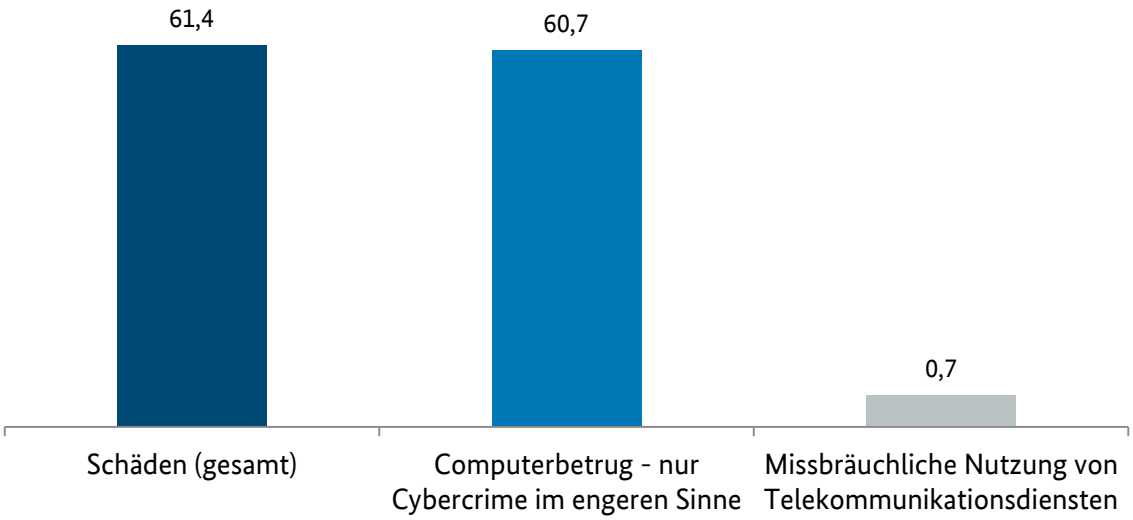
Auch Menschen, die das Internet nicht aktiv nutzen, sind von der reibungslosen Funktionsfähigkeit von Datennetzen und insbesondere dem Internet abhängig. So werden Strom und Gas von den großen Anbietern auf digitalem Wege eingekauft und die Verteilung wird über Netzwerke gesteuert. Auch der stationäre Handel speichert zunehmend die Daten seiner Kunden in Datenbanken, die ebenso als Angriffsziele krimineller Hacker dienen und missbraucht werden können. Kurz: Auch das „analoge“ Leben ist stark von uneingeschränkten Ablaufprozessen von IT- und Kommunikationsstrukturen, Dienstleistungsunternehmen, Industrie oder auch des Groß- und Einzelhandels abhängig und teils existenzsichernd.

Gemäß der ARD/ZDF-Onlinestudie 2018 sind über 90 % der deutschen Bevölkerung (ca. 63,3 Mio. Menschen) Onlinenutzer. Im Vergleich zum Vorjahr liegt die Steigerung damit bei 1,4 Prozent bzw. 0,9 Mio. Menschen. Auch die Nutzungsfrequenz von Online-Medien soll gestiegen sein: Im Jahr 2018 war der durchschnittliche Nutzer ca. 3:16 Stunden online; 47 Minuten länger als noch in 2017.[100]

Valide Aussagen zum tatsächlichen monetären Gesamtschaden durch Cybercrime lassen sich auf Basis der PKS nicht treffen, da in dieser ausschließlich Schäden in Fällen des Computerbetrugs und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen werden.
Die für das Jahr 2018 ausgewiesene Schadenssumme in diesen Bereichen belief sich insgesamt auf 61,4 Mio. Euro (2017: 71,8 Mio. Euro). Davon entfielen rund 60,7 Mio. Euro (2017: 71,4 Mio. Euro) auf den Bereich Computerbetrug und knapp 0,7 Mio. Euro (2017: 0,4 Mio. Euro) auf die missbräuchliche Nutzung von Kommunikationsdiensten.

[97] Wirtschaftsschutzstudie 2018, abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, S. 25.
[98] Polizeiliche Kriminalprävention der Länder und des Bundes
[99] Digitalbarometer 2019: Bürgerbefragung zur Cyber-Sicherheit, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2019.pdf?__blob=publicationFile&v=3
[100] ARD/ZDF-Onlinestudie 2018, abrufbar unter: http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2018.

Schäden durch Cybercrime in Mio. Euro (2018)[101]



Neben den statistischen Einschränkungen gilt es zu bedenken, dass finanzielle Schäden eines erfolgreichen Cyber-Angriffs oft nicht gänzlich bekannt oder bezifferbar sind. Reputationsverluste oder Imageschäden lassen sich in finanzieller Hinsicht ebenfalls schwerlich umreißen. Hinzu kommt, dass, je nach Ausgestaltung des Angriffs, oft nicht nur ein einzelnes System für einen bestimmten Zeitraum ausfällt, sondern mitunter komplette Netzwerke und daran gebundene Lieferketten beeinträchtigt werden.

Einige Studien treffen Aussagen zur Darstellung des tatsächlichen Schadensausmaßes. So stellten z. B. das Zentrum für Strategische und Internationale Studien (CSIS) und die Sicherheitsfirma McAfee einen Anstieg des wirtschaftlichen Schadens durch Cyberkriminalität auf weltweit 600 Mrd. US-Dollar fest. Der Diebstahl geistigen Eigentums soll laut der Untersuchung etwa ein Viertel des Schadens ausmachen.[102]

Es gibt große Diskrepanzen zwischen den in der PKS registrierten Schäden und den Feststellungen der Privatwirtschaft.

Nach Ausführungen des G4C-Mitglieds R+V geht deren Versicherungssparte CyberRisk von Kosten zwischen 10.000 und 25.000 Euro pro Schadensfall bei kleineren und mittleren Unternehmen bis 10 Mio. Euro Umsatz aus. Dies hänge maßgeblich davon ab, welche „Qualität“ der Angriff hat, ob Datensicherungen vorliegen und wie viele Rechner betroffen sind. CyberRisk kalkuliert für die Wiederherstellung von einem Rechner ungefähr 1.000 Euro. Bei einem System, d. h. einem Netzwerk oder Verbund mehrerer Computer, liege die Summe im Schnitt bei 5.000 Euro. Erpressungsgelder selbst seien hierbei nicht berücksichtigt, da diese nicht versichert seien.

[101] Bei Fällen mit unbekannter Schadenshöhe wird ein symbolischer Schaden von einem Euro erfasst.
[102] Economic Impact of Cybercrime, abrufbar unter: https://www.csis.org/analysis/economic-impact-cybercrime, veröffentlicht am 21.02.2018.

In einer weiteren Studie des Bundesverbands „bitkom“ haben Befragungen von Internetnutzern ergeben, dass in 54 % der berichteten Fälle auch tatsächlich ein finanzieller Schaden entstanden sein soll.[103]

„bitkom“ bemisst in einer Studie den finanziellen Schaden für die deutsche Wirtschaft durch Delikte der Cybercrime für die letzten zwei Jahre auf 43,4 Mrd. Euro.[104] Grundlage dieser Zahl sollen Angaben von betroffenen Unternehmen sein, die im Rahmen der Studie erhoben wurden. Problematisch bei der Betrachtung der durch Cyber-Angriffe entstandenen Schäden bleibt die Frage, welche Kostenarten hierunter zu fassen sind. Eine einheitliche Regelung gibt es hierfür nicht. Auch konkrete Schadenssummen für Privatpersonen konnten bisher nicht erhoben werden.

Es bleibt zu konstatieren, dass die verhältnismäßig geringen Schadenssummen in polizeilichen Statistiken das tatsächliche Ausmaß in keiner Weise widerspiegeln dürften.

[103] Cybercrime: Jeder zweite Internetnutzer wurde Opfer, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html, veröffentlicht am 10.10.2017.

[104] Cyberattacken auf deutsche Industrie nehmen stark zu, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Cyberattacken-auf-deutsche-Industrie-nehmen-stark-zu.html, veröffentlicht am 11.10.2018.

6 Gesamtbewertung und Ausblick

Die Nutzung digitaler Informations- und Kommunikationstechnologien ist eine wesentliche Basis des modernen gesellschaftlichen und wirtschaftlichen Lebens. Das Internet und die hierauf gestützten Dienstleistungen rücken weiter an die Menschen heran: So werden über sog. Wearables (z. B. Smartwatches, Fitnesstracker, Kleidung) körperbezogene Messdaten und personenbezogene Standortdaten permanent erfasst und verarbeitet. Die bei Internetdienstleistern gespeicherten Daten ermöglichen die Fertigung von umfassenden Persönlichkeits- und Aktivitätsprofilen.

Mit fortschreitenden Entwicklungen, wie dem Internet der Dinge/Internet of Things (IoT), Industrie 4.0, „Smart Home“ oder Automotive IT (AIT) und stark zunehmenden „adressierbaren“ Objekten im Internet wird das Spektrum potenzieller Ziele für Cyberkriminelle erweitert. Unzureichende Absicherungen sowie veraltete Technologien wirken sich dabei kriminalitätsfördernd aus.

Zunehmende Digitalisierung bedeutet auch mehr Tatgelegenheiten für Cyberkriminelle.

Die hochdynamischen Entwicklungen im Bereich der Künstlichen Intelligenz (KI) beinhalten bedeutende Potenziale für die wirtschaftliche Wertschöpfung. Sie bergen jedoch auch umfangreiche kriminelle Nutzungsmöglichkeiten (z. B. als „lernende Schadsoftware“). Kurz: Je umfassender sich die Gesellschaft in der digitalen Welt bewegt und je mehr Möglichkeiten diese bietet, desto mehr Tatgelegenheiten ergeben sich für Cyberkriminelle.

Dies zeigt sich nicht nur an den im Vergleich zum Vorjahr erhöhten Fallzahlen bei gleichzeitig niedrigerer Aufklärungsquote, sondern z. B. auch an dem massiven Anstieg der Vielfalt von Schadsoftware: So konnten im ersten Halbjahr 2018 vom G4C-Mitglied G DATA durchschnittlich ca. 13.000 gänzlich neu programmierte Arten bösartiger Software identifiziert werden[105]. Viele davon wurden spezifisch für mobile Endgeräte programmiert, sind beinahe unsichtbar (z. B. Kryptojacking-Malware) oder haben die Fähigkeit, sich durch Updates anzupassen und bedrohlichere Eigenschaften zu entwickeln. Die Qualität dieser Attacken hat durch technischen Fortschritt und durch eine zunehmende Professionalisierung von Angriffsvektoren deutlich zugenommen. Dieser Dynamik muss durch entsprechende Sicherheitsupdates und -maßnahmen kontinuierlich entgegengewirkt werden.

Es gibt jedoch auch positive Entwicklungen bei der Bekämpfung und Prävention im Phänomenbereich Cybercrime. So lassen sich z. B. die rückläufigen Zahlen beim Phishing im Online-Banking auf sicherheitsorientierte Weiterentwicklungen der entsprechenden TAN-Verfahren und das damit einhergehende effektive Schließen der erkannten Sicherheitslücken zurückführen.

Nicht nur die Gestaltungspotenziale der digitalen Welt erweitern sich, auch der Umgang mit technischem Know-how erfährt eine zunehmende, besorgniserregende Entwicklung: Zum einen erlauben das Internet im Allgemeinen, das Darknet im Speziellen, den Austausch von Expertise bzgl. des Einsatzes krimineller Malware. Zum anderen ist dieses Wissen aufgrund der Verfügbarkeit von Cybercrime-as-a-Service nicht mehr notwendig. Jeder Teilaspekt für einen Angriff, sei es betreffend der Software oder des Wissens um deren Anwendung, kann auf digitalen Schwarzmärkten angekauft und so auch von „technischen Laien“ mit kriminellen Absichten verwendet werden.

[105] G DATA-Blog; Malwarezahlen erstes Halbjahr 2018: Die Gefahr lauert im Web, abrufbar unter: https://www.gdata.de/blog/2018/08/31027-malwarezahlen-erste-halbjahr-2018-die-gefahr-lauert-im-web

Deutschland stellt aufgrund seines hohen Entwicklungsstands und Know-hows (insbesondere der Wirtschaft) ein attraktives Ziel für Cyberkriminelle dar: Angriffe auf Unternehmensprozesse und auf IT-Systeme von KRITIS stellen eine abstrakt hohe Bedrohung für die öffentliche Ordnung dar. Auch kleinere und mittlere Unternehmen stehen vermehrt im Fokus krimineller Aktivitäten (v. a. durch Ransomware-Angriffe).

Die Vorgehensweise der Täter, z.B. bei Attacken gegen mittelständische Unternehmen ist hochprofessionell: Einem Angriff geht häufig eine Informationssammlung über das Unternehmen voraus. Täter erhoffen sich hierbei Daten und Fakten zum Unternehmen, die sie für ihre spätere Erpressung ausnutzen können. Insbesondere Umsatzzahlen werden von Kriminellen genutzt, um ihre Lösegeldforderungen anzupassen.

Doch nicht nur IT-Systeme an sich müssen geschützt werden, auch Beschäftigte von Unternehmen müssen für Phänomene wie Social Engineering oder Phishing sensibilisiert werden.

Das gesamte Bedrohungspotenzial Cybercrime lässt sich angesichts der rasanten Entwicklung und aufgrund der Tatsache, dass viele Attacken bzw. Straftaten im Dunkelfeld verbleiben, kaum ab-schätzen. Es ist davon auszugehen, dass sowohl Fallzahlen als auch Schadenssummen sowie die Anzahl der Geschädigten weitaus höher sind, als es die polizeilichen Statistiken ausweisen. Um annähernd valide Aussagen zum tatsächlichen Ausmaß von Cybercrime treffen und Cybercrime wirkungsvoll bekämpfen zu können, sind diverse Maßnahmen auf Seiten der Strafverfolgungs- und Sicherheitsbehörden notwendig. Diese betreffen sowohl personelle, finanzielle und v. a. technische Aspekte, wie die Vermittlung von Grundkompetenzen, weiterführende Aus- und Fortbildung sowie die Bereitstellung geeigneter Hard- und Software. Auch eine verstärkte Kooperation mit Forschungsinstituten und der Privatwirtschaft kann dazu beitragen, das Dunkelfeld im Bereich Cybercrime zumindest in Teilbereichen aufzuhellen.

Auch die Nutzer selbst sind angehalten, für die Sicherheit ihrer technischen Geräte und die Vermeidung achtloser Informationsweitergabe im Netz Sorge zu tragen. Dabei ist es unumgänglich, dass Nutzer sich entsprechend informieren und Mittel bzw. Maßnahmen erlernen, mit denen man sich vor Attacken verschiedener Art schützen kann.

Cybercrime kennt keine nationalen Grenzen.

Cybercrime ist ein spezifisches, quantitativ wie qualitativ an Bedeutung gewinnendes Kriminalitätsphänomen, für das staatliche Grenzen irrelevant/bedeutungslos sind. Umso mehr gilt es, neben der nationalen auch die internationale Kooperation zwischen den Sicherheitsbehörden und den Partnern aus Forschung, Industrie und Handel weiter auszubauen.

Im November 2010 hat der Rat der Europäischen Union den EU-Politikzyklus („EU-Policy Cycle“) zur Bekämpfung der organisierten und schweren internationalen Kriminalität eingerichtet. Mit diesem mehrjährigen Politikzyklus soll in kohärenter und methodischer Weise gegen die größten Bedrohungen für die EU durch organisierte und schwere Kriminalität vorgegangen werden, und zwar in Form einer optimierten Zusammenarbeit zwischen den zuständigen Dienststellen der Mitgliedsstaaten, den Institutionen und Agenturen der EU sowie Drittländern und Organisationen, auch unter Einbeziehung des Privatsektors. Umgesetzt wird diese Zusammenarbeit über die hierfür eingerichtete Plattform EMPACT (European Multidisciplinary Platform Against Criminal Threats). Das Phänomen Cybercrime gehört zu den priorisierten Phänomenbereichen, die in diesem Kontext gemeinsam auf europäischer Ebene zu bekämpfen sind.

Die Schwerpunkte für das Jahr 2019 im Bereich der Bekämpfung der „Cybercrime“ liegen in der Umsetzung einer von allen Teilnehmerstaaten erarbeiteten gemeinsamen Bekämpfungsstrategie. Diese beinhaltet operative Maßnahmen wie z. B. die Entwicklung neuer Auswertungstools, die Koordinierung gemeinsamer Ermittlungsverfahren mit verstärkter operativer Ausrichtung, die Kooperation mit Drittstaaten und die Erweiterung der Kooperation mit privaten Partnern. Aufgrund der dabei anfallenden erheblichen Datenmengen sind damit einhergehend Maßnahmen notwendig, um die Datenerhebungen und Analysemethoden für Strafverfolgungsbehörden international wie auch national zu erleichtern. Diese Entwicklungen sind durch entsprechende Fortbildungsmaßnahmen für die polizeiliche Bearbeitung zu ergänzen. Nur so kann mit den dargestellten Entwicklungen im Bereich Cybercrime Schritt gehalten werden.

Eine Antwort auf die anwachsende Cybercrime ist der Ausbau und die Verbesserung der nationalen und internationalen Kooperation.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Oktober 2019

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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

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