Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2017

Cybercrime in Zahlen 2017

85.960 Fälle von Cybercrime im engeren Sinne (+4 %)

251.617 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (4,4 % aller in der PKS erfassten Straftaten)

1.425 Fälle von Phishing im Onlinebanking (-34,5 %)

4.000 Euro/Fall durchschnittlicher Schaden beim Phishing im Onlinebanking (2016: 4.000 Euro/Fall)

71,4 Mio. Euro Schaden im Bereich Computerbetrug (2016: 50,9 Mio. Euro)

Zunahme bei mobiler Malware (+54 %)

17 OK-Gruppierungen im Kriminalitätsbereich Cybercrime; 3 % aller OK-Verfahren (2016: 22)

Inhaltsverzeichnis

1 Vorbemerkung

Cybercrime umfasst die Straftaten, die sich gegen Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels Informationstechnik begangen werden.

Das Bundeslagebild Cybercrime 2017 informiert über die polizeilich bekannt gewordenen Entwicklungen von Cybercrime im engeren Sinne. Dies sind im Einzelnen:

- **Computerbetrug als Cybercrime im engeren Sinne** (§ 263a StGB; Aufschlüsselung in verschiedene Betrugsarten s. S. 4 f.)
- **Sonstiger Computerbetrug** (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB)
- **Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei** (§§ 202a, 202b, 202c, 202 d StGB)
- **Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr** (§§ 269, 270 StGB)
- **Datenveränderung/Computersabotage** (§§ 303a, 303b StGB)
- **Missbräuchliche Nutzung von Telekommunikationsdiensten** (§ 263a StGB)

Grundlage für den statistischen Teil des Lagebilds 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 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 oder von behördlichen Einrichtungen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch solche von privaten Verbänden und Firmen, wie z. B. Antivirensoftware-Herstellern und IT-Sicherheitsdienstleistern.

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 qualitativ verbesserte Lagebewertung.

[1] G4C-Mitglieder: Commerzbank, ING-DiBa, Hypo-Vereinsbank, 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 (PKS)

Bei der Betrachtung von polizeilich erfassten statistischen Daten müssen die besonderen Erfassungs- bzw. Zählmodalitäten in der PKS berücksichtigt werden.

Der Phänomenbereich Cybercrime ist wie der gesamte Bereich der Informationstechnik von einer hohen Dynamik in der Entwicklung geprägt. Dementsprechend wurde die PKS in den letzten Jahren hinsichtlich der Erfassung der diesem Bereich zuzuordnenden Delikte weiterentwickelt. So werden seit dem Jahr 2014 Delikte der Cybercrime bundeseinheitlich nur dann in der PKS erfasst, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen.

Bei der Bewertung der Fallzahlen ist zu berücksichtigen, dass jede im Rahmen eines Ermittlungsvorgangs bekannt gewordene rechtswidrige Handlung, unabhängig von der Anzahl der Geschädigten, als nur ein Fall erfasst wird. So wurde beispielsweise die Softwaremanipulation von ca. 1,3 Mio. DSL-Routern eines deutschen Internetproviders durch Malware im November 2016 – trotz einer siebenstelligen Anzahl von Geschädigten – als nur ein Fall der Computersabotage in der PKS ausgewiesen.

Bei der Interpretation der Statistik ist ferner zu beachten, dass z. B. einzelne relevante Phänomene, wie Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch mit Ransomware, in der PKS in der Regel nicht als Cybercrime-Delikt, sondern gemäß PKS-Richtlinien als schwerwiegendere bzw. speziellere Tat, in diesem Fall als Erpressung, erfasst werden. Einzig über die im Jahr 2004 eingeführte PKS-Sonderkennung „Tatmittel Internet“ lässt sich ggf. ein Bezug zu Cybercrime herstellen.

Trotz der eingeschränkten Aussagekraft der PKS hinsichtlich der Gesamtheit der in Deutschland verübten Cybercrime-Straftaten ist festzuhalten, dass es sich deutschlandweit um die einzige statistische Datenerhebung handelt, die auf polizeilichen Ermittlungen basiert. Damit liefert sie eine qualitativ hochwertige Datenbasis zumindest für Trendaussagen in diesem Phänomenbereich.

Aussagen zur tatsächlichen Kriminalitätsbelastung lassen sich alleine auf Grundlage der PKS nicht treffen, da die Anzahl der tatsächlich begangenen nicht polizeilich bekannt gewordenen und erfassten Straftaten um ein Vielfaches höher liegen dürfte. Gründe hierfür sind zum einen in den dargestellten Erfassungsmodalitäten zu finden, 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

werden (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 beispielsweise im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner" nicht zu verlieren,

- Geschädigte erstatten beispielsweise 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 darauf hin, dass Geschädigte die entsprechenden Cybercrime-Straftaten auch anzeigen sollen, 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 -bestrafung möglich ist. Ziel muss es sein, die Urheber für Cyber-Angriffe zu identifizieren und weitere Angriffe zu unterbinden. Die Sanktionierung kriminellen Verhaltens sollte hierbei auch abschreckende Wirkung auf potenzielle Täter haben.

Cybercrime im engeren Sinne umfasst folgende Delikte:

- **Computerbetrug als Cybercrime im engeren Sinne;** dieses Delikt wird seit 01.01.2016 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** gem. § 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).
- Das **Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei** (§§ 202a, 202b, 202c, 202 d 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 in der „Underground Economy"[2]

[2] Überregionale Online-Schwarzmärkte, oft im Darknet, über die Anbieter und Käufer ihre kriminellen Geschäfte rund um die digitale Welt anbahnen und abwickeln können.

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.

- Die Straftatbestände **Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr** (§§ 269, 270 StGB) 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.

- Bei **Datenveränderung/Computersabotage** (§§ 303a, 303b StGB) 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 die Denial of Service-Angriffe (DoS-/DDoS-Angriffe[3]), ebenso wie die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojaner, Viren, Würmer usw.).

Die **missbräuchliche Nutzung von Telekommunikationsdiensten** 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.

[3] 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.

2.2 FALLZAHLEN CYBERCRIME

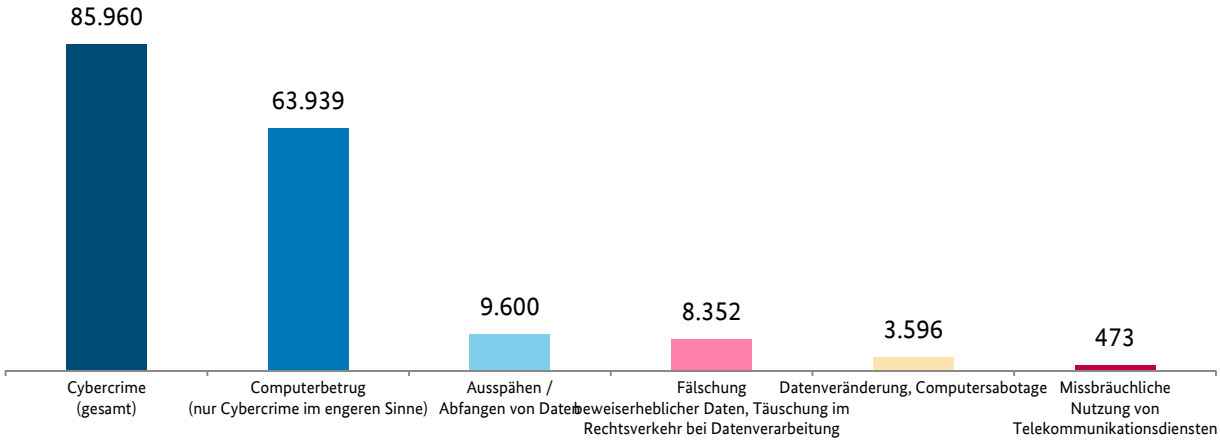
Im Jahr 2017 war ein Anstieg der Straftaten von Cybercrime im engeren Sinne zu verzeichnen. Die PKS wies insgesamt 85.960 Delikte aus. Dies bedeutete einen Anstieg gegenüber dem Vorjahr um 4,0 % (2016: 82.649). Die Aufklärungsquote betrug 40,3 %, was einem Anstieg gegenüber dem Vorjahr um 1,6 Prozentpunkte entspricht.

Drei Viertel aller Straftaten wurden als Fälle von Computerbetrug registriert.[4] Bereits bei der Auswertung der PKS-Fallzahlen 2016 zur Cybercrime im engeren Sinne wurde festgestellt, dass der Anstieg der Fallzahlen mit einem vergleichsweise starken Anstieg im Bereich des Computerbetrugs einherging. Für 2017 war in diesem Deliktsfeld ein weiterer Anstieg von 9,1 % zu verzeichnen. In 2017 durchgeführte Recherchen in zwei großen Bundesländern führten zu dem Ergebnis, dass die unter den relevanten Schlüsselzahlen des Computerbetrugs erfassten Delikte in den meisten Fällen keine „Cybercrime im engeren Sinne“ darstellten. In den meisten Fällen wurden Sachverhalte hierunter erfasst, bei denen das Internet lediglich als Tatmittel fungierte. Auch aus diesem Grund müssen die Fallzahlen der PKS differenziert betrachtet und bewertet werden.

Die Fallzahl zur missbräuchlichen Nutzung von Telekommunikationsdiensten gem. § 263a StGB sank um 41,7 %. Bereits im Bundeslagebild 2016 wurde auf die Änderung des PKS-Straftatenschlüssels zur Erfassung dieses Delikts hingewiesen. Der starke Rückgang in diesem Deliktsbereich setzte sich nunmehr weiter fort; insgesamt wurden lediglich noch 473 Fälle statistisch erfasst. Dies entspricht einem prozentualen Anteil von unter einem Prozent an allen Cybercrime-Fällen.

[4] Zur differenzierteren Abbildung erfolgt seit Januar 2016 folgende Aufschlüsselung der Computerbetrugsarten, die zuvor als „sonstiger Computerbetrug“ nach § 263a StGB (PKS-Schlüssel 517500) erfasst worden waren: Sonstiger Computerbetrug gem. § 263 Abs. 1 und 2 (PKS-Schlüssel 517510) sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB (PKS-Schlüssel 517520), betrügerisches Erlangen von Kfz gem. § 263a StGB (PKS-Schlüssel 511120), weitere Arten des Kreditbetruges gem. § 263a StGB (PKS-Schlüssel 512212), Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB (PKS-Schlüssel 516520), Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB (PKS-Schlüssel 516920), Leistungskreditbetrug gem. § 263a StGB (PKS-Schlüssel 517220), Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB (PKS-Schlüssel 518112), Überweisungsbetrug gem. § 263a StGB (PKS-Schlüssel 518302).

Fälle von Cybercrime im engeren Sinne (2017)



In einer im Oktober 2017 veröffentlichten Studie berichtet der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), dass ca. jeder zweite Internetnutzer in Deutschland Geschädigter von Cybercrime geworden sei. Lediglich 18 % dieser Geschädigten hätten angegeben, dass sie Anzeige bei der Polizei oder Staatsanwaltschaft erstattet haben.[5] Rechnet man diese Zahlen auf die Bevölkerung und die Internetnutzer hoch, wird deutlich, dass die tatsächliche Belastung durch Straftaten im Bereich Cybercrime erheblich höher ausfallen dürfte als in der PKS abgebildet.

Zur Betroffenheit von Wirtschaftsunternehmen durch Cybercrime veröffentlichte BITKOM in 2017 eine weitere Studie. In dem Bericht „Wirtschaftsschutz in der digitalen Welt“ führt der Digitalverband aus, dass mehr als die Hälfte der Unternehmen in Deutschland (53 %) in den vergangenen beiden Jahren Geschädigte von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden seien.[6]

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

[5] **Https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**
[6] **https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.**

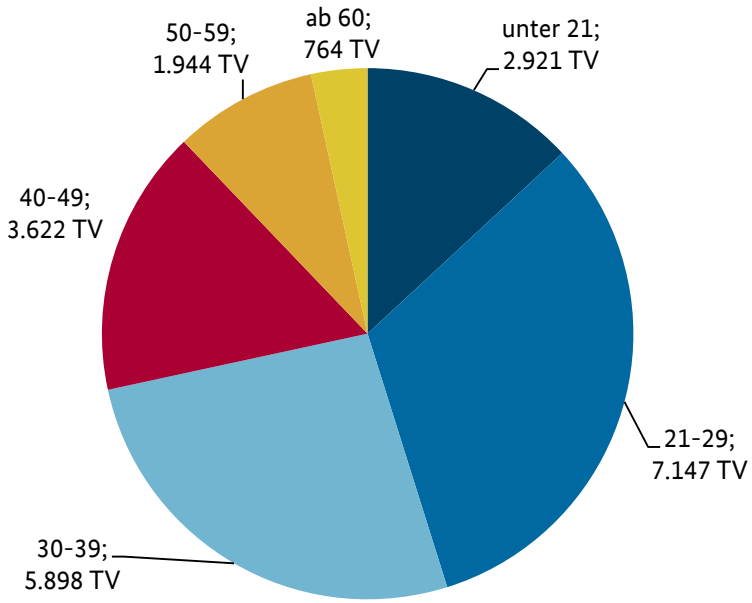
2.3 TATVERDÄCHTIGE

Im Jahr 2017 wurden insgesamt 22.296 Tatverdächtige (TV) von Cybercrime-Delikten registriert (+ 6,6 %; 2016: 20.920). 68,3 % der Tatverdächtigen waren männlich, 31,7 % weiblich.

Insgesamt hatten 17.131 der festgestellten Tatverdächtigen (76,8 %) die deutsche Staatsangehörigkeit. 5.165 Tatverdächtige waren Nichtdeutsche, wobei türkische (14,0 %), rumänische (9,9 %) und polnische (6,4 %) Staatsangehörige am häufigsten vertreten waren.

Mehr als die Hälfte (58,5 %) der registrierten Delikte der Cybercrime im engeren Sinne wurde von Tatverdächtigen begangen, die zwischen 21 und 39 Jahre alt waren.

Altersstruktur der Tatverdächtigen (2017)



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.

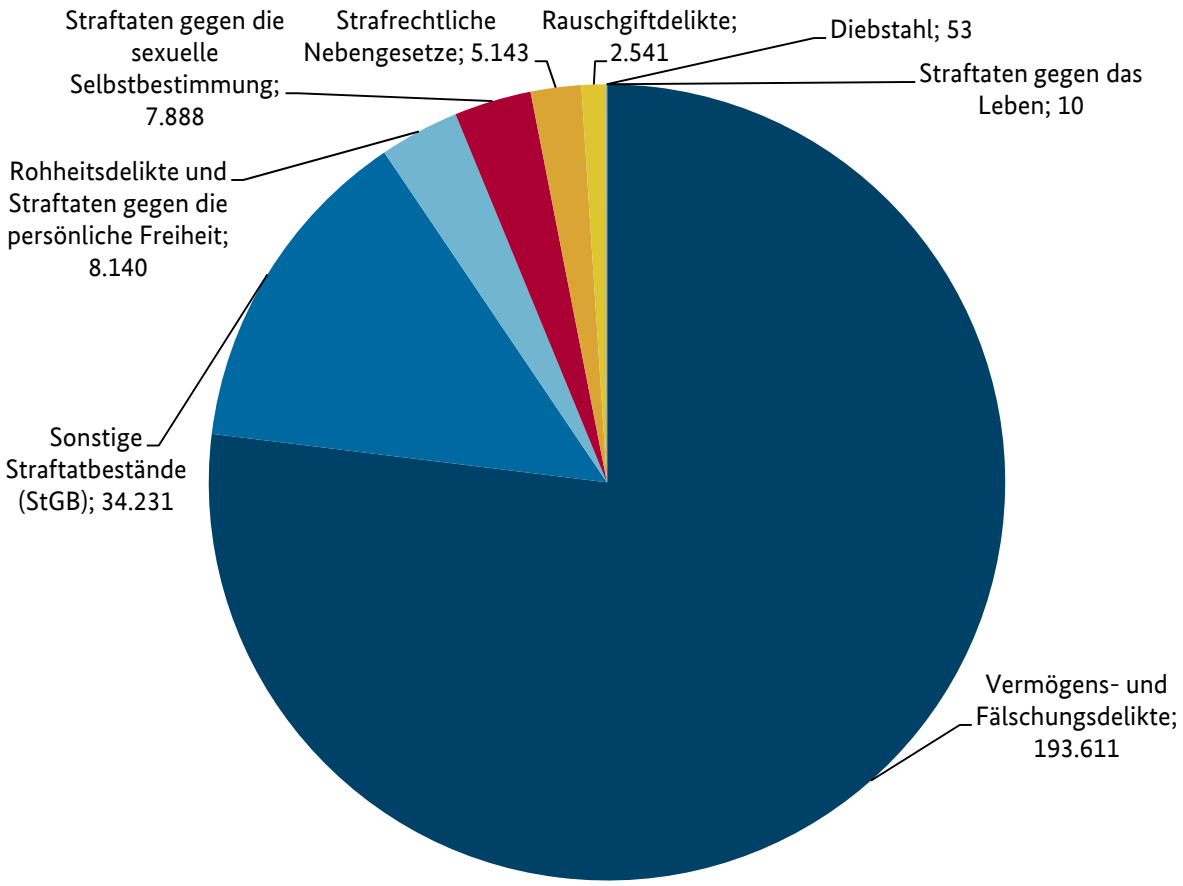
Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Dienste, die nicht selbst erbracht werden können, werden von anderen hinzugekauft (Cybercrime-as-a-Service).

Cybercrime ist auch im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität von Bedeutung. Im Jahr 2017 wurden 17 OK-Gruppierungen (Gesamtzahl der im Jahr 2017 registrierten OK-Gruppierungen: 572) im Kriminalitätsbereich Cybercrime erfasst (2016: 22). Deliktisch sind keine Unterschiede zu Einzeltätern oder losen Netzwerken feststellbar. Auch OK-Gruppierungen begehen die typischen Cybercrime-Delikte von Computerbetrug über Angriffe auf das Onlinebanking bis hin zur Verbreitung von Ransomware mit dem Ziel der digitalen Erpressung.

2.4 TATMITTEL INTERNET

Im Jahr 2017 wurden in der PKS insgesamt 251.617 Straftaten erfasst, bei denen das Internet als Tatmittel genutzt wurde. Dies entspricht einem Rückgang um 0,7 % gegenüber dem Vorjahr (2016: 253.290 Fälle).

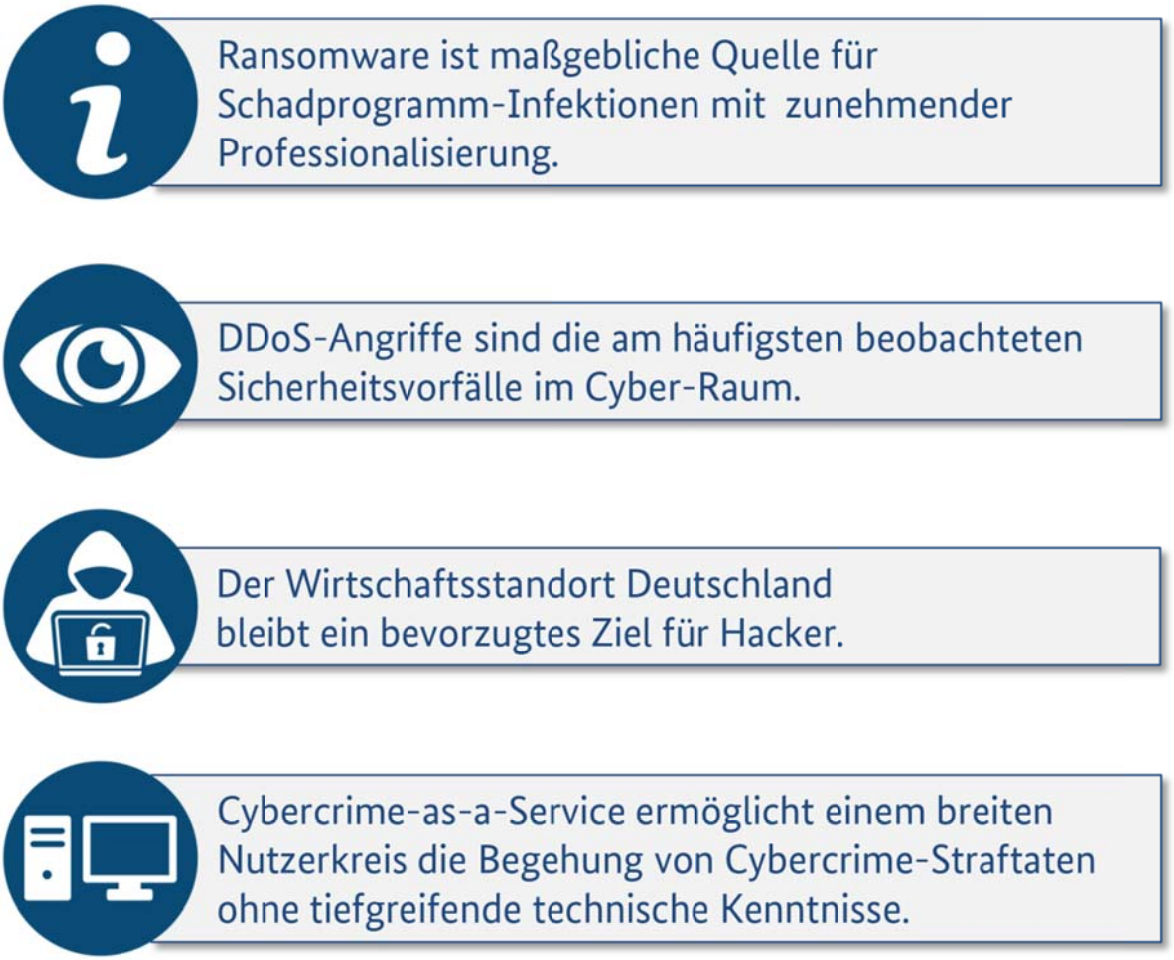
Tatmittel Internet – Verteilung nach Deliktsbereichen (2017)



Die PKS-Sonderkennung „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.

In 74,4 % der in 2017 erfassten Fälle handelte es sich um Betrug (183.529 Fälle). Darunter waren vor allem Fälle von Waren- und Warenkreditbetrug (134.476 Fälle), bei denen Tatverdächtige über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder in minderwertiger Qualität lieferten oder Tatverdächtige die Waren bestellten und nicht bezahlten.

3 Aktuelle Phänomene



3.1 RANSOMWARE[7] – DIGITALE ERPRESSUNG

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

In den meisten Fällen fordern die Täter ein Lösegeld, das in Form von digitaler Währung 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.

[7] 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.

Digitale Erpressung mittels Ransomware ist ein in Deutschland und auch weltweit häufig auftretendes Phänomen. Neben Unternehmen sind auch Privatpersonen zunehmend von Ransomware betroffen.

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

Das BKA führte für das Jahr 2017 eine gezielte Bund-Länder-Fallerhebung durch, um das Aufkommen an angezeigten Fällen von Ransomware besser abzubilden. Gemäß dieser Erhebung wurden insgesamt 5.191 Fälle von Malware angezeigt, davon 2.772 Fälle von Ransomware.[8] Elf der Länder war es darüber hinaus möglich, auch die einzelnen Ransomware-Familien abzubilden. Auf Grundlage dieser Datenbasis waren 2017 die am häufigsten polizeilich angezeigten Ransomware-Familien der sog. „BKA-Trojaner" (720 Fälle), CryptXXX (170 Fälle), Cerber (117 Fälle) und Locky (55 Fälle).

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[9] 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 ist weitaus gefährlicher, 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.*

Das BSI stellt im Bericht zur Lage der IT-Sicherheit in Deutschland 2017 fest, dass Ransomware auch 2017 die maßgebliche Quelle für Schadprogramminfektionen geblieben sei.[10]

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 zahlreiche Geschädigte die vergleichsweise niedrigen geforderten Lösegelder.

[8] An der Erhebung nahmen 13 Länder teil. Die Zahl ist mit den vorgenannten Zahlen mithin nicht vergleichbar und spiegelt ausschließlich den Ist-Stand an Ransomware-Anzeigen wider, die mittels der genannten Methodik erhoben wurden. Ein Trend (Zunahme oder Abnahme von Ransomware) kann hieraus zum aktuellen Zeitpunkt nicht abgeleitet werden.
[9] Bekannte Beispiele sind der sog. „BKA-Trojaner" und der „GVU-Trojaner".
[10] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**

Aus polizeilicher Sicht ist von entsprechenden Zahlungen abzuraten, da hierdurch das kriminelle Geschäftsmodell Ransomware unterstützt wird und Anreize zur weiteren Tatbegehung geschaffen werden. Dies insbesondere vor dem Hintergrund, dass möglicherweise der Betroffene selbst gegen die Infizierungen vorgehen kann: Bei Betroffenheit durch Ransomware empfiehlt sich eine „Open-Source-Recherche“ nach frei verfügbaren Entschlüsselungstools, so beispielsweise über das von Europol und der niederländischen Cybercrime-Dienststelle (NHTCU) in Zusammenarbeit mit der Privatwirtschaft initiierte Projekt **www.nomoreransom.org**.

Vorwiegend wurde auch in 2017 weiterhin Ransomware mit Verschlüsselungsfunktionen eingesetzt. Vor allem bei mobilen Betriebssystemen wie Android wurden einfache Sperrbildschirme ohne Verschlüsselung der Festplatte weiterhin als Modus Operandi festgestellt.[11]

Im Jahr 2017 hat sich die Ransomware-Szene weitgehend professionalisiert. Zum einen prägten professionell codierte und vertriebene Varianten wie Locky, CryptXXX und Cerber weiterhin den Markt, was auch der Einschätzung des G4C entspricht. Zum anderen taten sich neue Varianten wie WannaCry dadurch hervor, dass alternative Verbreitungswege, hier die wurmartige Verbreitung über IT-Schwachstellen, genutzt wurden. Insgesamt gab es gezieltere Attacken mit in Einzelfällen erheblich höheren Lösegeldsummen. Ziele wurden tendenziell sorgfältiger ausgewählt als noch im Jahr 2016.[12] Das Gros der Ransomware bildeten jedoch weiterhin massenhafte Verbreitungswellen mit relativ niedrigen geforderten Lösegeldern. Die durchschnittliche Erpressungssumme für Ransomware-Fälle belief sich 2017 gem. einer Auswertung des G4C-Mitglieds Symantec auf ca. 522 US-Dollar (umgerechnet ca. 425 €).[13] Das Jahr 2016 war noch von einem starken Aufkommen der Ransomware geprägt. Zahlreiche Varianten wurden mit der Zielrichtung entwickelt, kurzfristige Gewinne zu erzielen; in Teilen wurden hier bestehende Varianten schlichtweg kopiert. Viele der 2016 festgestellten Varianten waren darüber hinaus unprofessionell codiert und wiesen Fehler auf.

Fallbeispiel: Verschlüsselungssoftware WannaCry

Im Mai 2017 fand ein massiver weltweiter Cyber-Angriff auf Computersysteme von Firmen, Institutionen und Privatpersonen mittels der Ransomware WannaCry statt. In Deutschland wurden u. a. Systeme der Deutschen Bahn infiziert. Dies äußerte sich durch ausgefallene Ticketautomaten und Erpressernachrichten auf zahlreichen Anzeigetafeln in deutschen Bahnhöfen. Ferner waren zahlreiche private Systeme vom Angriff betroffen.

Die europäische Cybersicherheitsagentur ENISA (European Union Agency for Network and Information Security) schätzte, dass über 230.000 Systeme in über 150 Ländern der Welt von der Attacke betroffen waren. In Großbritannien kam es beispielsweise zu erheblichen Beeinträchtigungen im Gesundheitsdienst. Weitere bekannte Infektionen fanden u. a. in Russland, China, der Ukraine, den USA, Spanien, Frankreich, Hong Kong und Japan statt.

[11] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**
[12] Diese Einschätzung teilt auch das German Competence Centre against Cyber Crime (G4C e.V.).
[13] Vgl. Symantec ISTR 2018; **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf.**

Fallbeispiel: Verschlüsselungssoftware WannaCry

Die Ransomware WannaCry breitete sich weitgehend selbstständig, wurmartig, aus. Hierzu wurde eine bekannte Schwachstelle im SMB-Protokoll von Windows ausgenutzt, die unter dem Codenamen ETERNALBLUE firmiert. Vorläufig angehalten wurde die Verbreitung durch einen IT-Sicherheitsexperten mittels einer Kill-Switch-Domain.

Kurzbewertung:
Die Ransomware WannaCry zeichnete sich durch eine weitgehend selbstständige, wurmartige Verbreitung über IT-Schwachstellen aus. So entstandene Schäden sind enorm und verdeutlichen das Schadenspotenzial von Ransomware im Jahr 2017.

3.2 WEITERE 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-Downloads). Die Verbreitung von Schadsoftware erfolgt zunehmend wurmartig durch die automatische Erkennung von Schwachstellen.

Laut dem BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2017“ wird die Gesamtzahl der Schadprogrammvarianten für Computersysteme auf über 600 Mio. geschätzt (2016 über 560 Mio.).

Neben Ransomware wurden auch im Jahr 2017 zahlreiche weitere Arten von Schadsoftware festgestellt. Dazu zählen vor allem Banking-Trojaner, Keylogger, Adware und Spyware. Darüber hinaus werden auch Angriffe auf Geldautomaten festgestellt, die ebenfalls auf Schadsoftware basieren.[14]

Gemäß einer Umfrage des BSI waren im Jahr 2017 70 % der befragten deutschen Wirtschaftsunternehmen von Cyber-Angriffen betroffen. Der Großteil dieser Angriffe (57 %) sei mittels Schadsoftware durchgeführt worden.[15]

Im Rahmen einer Erhebung des BKA (s. S. 10) zu polizeilich angezeigter Schadsoftware wurden insgesamt 924 Fälle von Banking-Trojanern festgestellt. Dies entspricht einem Anteil von ca. 16 % der gemeldeten Malware-Fälle.

[14] Vgl. BKA, Angriffe auf Geldautomaten, Bundeslagebild 2017, S. 11.
[15] **Https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Allianz_digitalundsicher_15022018.html.**

Insbesondere zum Jahresende 2017 wurden nach Informationen des G4C vermehrt Schadprogramme festgestellt, die dem sog. Cryptomining dienen. Ziel ist hier die Infiltration von privat sowie geschäftlich genutzten Systemen, um die Rechenleistung dieser Systeme für die Errechnung von Kryptowährungen, insbesondere Bitcoin, zu nutzen. Hierunter leidet die Leistung der infizierten Systeme. Dies kann auch zu einem erhöhten Stromverbrauch und dadurch bedingt zu hohen Kosten auf Seiten der Betroffenen führen.[16] Die polizeilichen Datenbestände verzeichnen für das Jahr 2017 derweil kaum Fälle von Cryptomining-Malware. Dies dürfte insbesondere darauf zurückzuführen sein, dass der Schaden auf Seiten der Betroffenen nur selten oder zumindest verspätet bemerkt wird und seitens der Betroffenen kein strafbares Verhalten angenommen wird.

Fallbeispiel: Malware NotPetya

Im Juni 2017 kam es weltweit zu einem massiven destruktiven Einwirken einer Schadsoftware auf IT-Systeme von Unternehmen.

In Deutschland wurden Unternehmen, vornehmlich aus den Branchen Logistik, Finanzen und Gesundheit, angegriffen.

Die Malware „NotPetya“ infizierte mehrere Unternehmen, vornehmlich in der Ukraine, über eine Schwachstelle in einer Buchhaltungssoftware. Die Malware breitete sich daraufhin selbstständig und wurmartig auf zahlreiche weitere Unternehmen aus, die ebenfalls die genannte Software nutzten. Neben Unternehmen in der Ukraine wurden Unternehmen in zahlreichen weiteren Staaten mit „NotPetya“ infiziert.

Die Schäden durch „NotPetya“ waren enorm. Die kompromittierten Systeme wurden in wesentlichen Teilen, teils dauerhaft, unbrauchbar. Einzelne Unternehmen konnten ihre IT-Infrastrukturen auch mehrere Wochen nach dem Angriff nicht vollständig wiederherstellen. Die dänische Reederei MAERSK und der Frachtdienstleister TNT Express bezifferten die ihnen entstandenen Schäden jeweils auf über 300 Mio. US-Dollar. Insgesamt wird der allein in Europa entstandene Schaden auf über 1 Milliarde Euro geschätzt.

Kurzbewertung:
Entgegen der vielfach getroffenen initialen Bewertung, dass es sich bei „NotPetya“ um eine Variante der Ransomware Petya handelte, stellte sich heraus, dass diese nicht mit dem klassischen Ziel, Lösegelder zu erpressen, verteilt worden ist. Vielmehr zielte die Verbreitung der Malware auf die Zerstörung von Daten und das Blockieren/Sabotieren von Geschäftsprozessen ab. Die Verbreitung von „NotPetya“ stellte damit zuvorderst einen Akt der Cybersabotage dar.

Das Fallbeispiel illustriert das enorme Schadenspotenzial, welches von Malware ausgeht. „NotPetya“ zeichnet sich hier insbesondere durch den intelligenten Verbreitungsweg aus. Nach initialer Infektion breitete sich die Schadsoftware selbstständig auf weitere vulnerable Systeme aus, auch außerhalb der bereits infizierten Unternehmen. Dies belegt eine zunehmende technische Weiterentwicklung von Malware.

[16] Vgl. auch **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf**.

3.3 BOTNETZE – MASSENHAFTE FERNSTEUERUNG VON COMPUTERN/DDOS-ANGRIFFE

3.3.1 Botnetze

Auch in 2017 hat die Bedrohung durch Botnetze als zentrale Angriffsressource nicht an Bedeutung verloren. Bei Botnetzen handelt es sich um zahlreiche, per Schadcode infizierte Systeme von Geschädigten, die ohne Wissen ihrer Besitzer über „Command & Control-Server" (C&C-Server) ferngesteuert werden. Hierzu zählen neben Computern vermehrt auch mobile sowie sog. intelligente Endgeräte des Internet of Things[17] (IoT).

Wie entstehen Botnetze?

Botnetze entstehen durch die zumeist für den Besitzer unbemerkte Installation einer Schadsoftware auf dem PC des Geschädigten.

Die Installation der Schadsoftware erfolgt unterschiedlich, 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 Teilnehmern 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 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.

Aufgrund der vielfältigen Nutzungsmöglichkeiten von Botnetzen sind diese nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy. Valide Angaben zur Gesamtzahl der in Deutschland bzw. weltweit in Botnetzen zusammengeschlossenen Rechner sind jedoch kaum möglich.

Die Betreiber der Botnetze vermieten Bots, durch die beispielsweise mittels DDoS-Attacken gezielte Angriffe auf Unternehmensserver durchgeführt, massenweise Spam-Mails versendet werden oder auch gezielte Datendiebstähle erfolgen können.

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

[17] Internet der Dinge; detaillierte Ausführungen siehe Kapitel 5.2.

Fallbeispiel: Botnetz - „Andromeda“

Im November 2016 wurde durch eine international koordinierte Aktion die Botnetzstruktur „Avalanche“ vom Netz genommen. In dieser Infrastruktur wurde auch die Schadsoftware „Andromeda“ festgestellt, die über ein weiteres Botnetz verteilt wurde. Nach umfangreichen internationalen Ermittlungen, die in Deutschland in Niedersachsen (Staatsanwaltschaft Verden/Zentrale Kriminalinspektion Lüneburg) geführt wurden, konnten das Botnetz analysiert und strukturrelevante Steuerserver identifiziert werden. Im November 2017 erfolgte im Rahmen eines Action-Days der Takedown dieser international agierenden Botnetzstruktur.

Der mutmaßliche Haupttäter konnte an dem Action-Day in Weißrussland festgenommen werden. Neben der Beschlagnahme umfangreichen Beweismaterials konnten auch die zur Verbreitung der Schadsoftware eingesetzten sieben Steuerserver in sechs verschiedenen Staaten beschlagnahmt bzw. abgeschaltet werden. Darüber hinaus wurden 1.500 Domains der Schadsoftware mit einer sog. Sinkholing-Maßnahme[18] belegt. Dadurch wurden allein am 30.11.2017 weltweit 1,35 Mio. IT-Systeme identifiziert, die von „Andromeda“ befallen waren.

Die Infektion des Systems des Geschädigten erfolgte zum einen per E-Mail, welche einen schadhaften Link enthielt; zum anderen über sog. Drive-by-Exploits, die sich auf kompromittierten Werbebannern oder Websites, hauptsächlich solche mit zweifelhaftem Inhalt (Pornographie, illegale Verkäufe, Verstoß gegen Urheberrechte durch Videostreaming etc.), befanden. Die Schadsoftware spähte das infizierte System des Geschädigten aus und war in der Lage, einen Banking-Trojaner nachzuladen, der auf die ausgespähten Daten der Geschädigten abgestimmt war. Es gelang den Tätern in den letzten Jahren mehrere Millionen PC-Systeme zu infizieren. Brennpunkte waren Nordamerika, Asien und Europa, wobei hier Systeme in Rumänien, Italien, Deutschland und Polen am meisten betroffen waren.

An den polizeilichen Maßnahmen waren neben Deutschland die Staaten Finnland, Frankreich, Polen, Italien, Russland, Niederlande, Weißrussland und USA beteiligt. Weltweit waren 27 Staaten in die Aktion eingebunden.

Unterstützt wurden die Aktionen durch das BSI, das Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), die Shadowserver Foundation sowie den Registrar of Last Resort (ROLR). Außerdem waren EUROPOL und EUROJUST maßgeblich an der Koordinierung der Maßnahmen beteiligt.

Kurzbewertung:
Vor dem Hintergrund, dass bis Anfang 2018 trotz aller Maßnahmen bundesweit weiterhin 39 % der ursprünglich in Avalanche betroffenen Computersysteme infiziert waren – weltweit sogar 55 % – wird die Notwendigkeit, weitergehende Anstrengungen insbesondere im Bereich der Bereinigung von als Bot identifizierten Systemen vorzunehmen, verdeutlicht.

[18] Umleitung von Anfragen botnetzinfizierter Systeme in andere Computersysteme, die i. d. R von Computer-Sicherheitsspezialisten betrieben werden.

3.3.2 DDoS-Angriffe

DDoS-Angriffe sind eng mit der Thematik Botnetze verknüpft, da die in einem Botnetz zusammengeschlossenen Systeme der Geschädigten zur Durchführung dieser Angriffe genutzt werden. DDoS-Angriffe gehören zu den am häufigsten beobachteten Sicherheitsvorfällen im Cyber-Raum. Kriminelle haben hieraus entsprechende Geschäftsmodelle entwickelt und vermieten Botnetze verschiedener Größen.

Polizeiliche Daten zur Anzahl und Dauer von DDoS-Angriffen in Deutschland liegen dem BKA nicht vor. Nach einer Untersuchung des G4C-Mitglieds Link11 haben sich neben der Anzahl der Attacken auch die Dauer der Angriffe sowie die durchschnittliche Bandbreite in 2017 erhöht.[19]

Die Nichterreichbarkeiten von Vertriebsportalen (z. B. Online-Shops, Service-Provider, Kryptowährungs-Handelsplattformen) in Folge eines DDoS-Angriffs können im wettbewerbsintensiven Marktsegment Internet erhebliche wirtschaftliche Schäden nach sich ziehen.

DDoS-Angriffe zeichnen sich durch rasant steigende Bandbreiten aus. Durch die Nutzung von IoT-Geräten erreichen sie neue Dimensionen.

Die Motivlagen der Täterseite umfassen rein monetäre Interessen (Ransom-DDoS), Erlangen von Wettbewerbsvorteilen, Rache oder auch politische bzw. ideologische Motive.

Die durch DDoS-Angriffe verursachten Schäden für den Betroffenen lassen sich nicht abschließend quantifizieren, da Folgewirkungen der Angriffe wie

- Systemausfälle/Unterbrechung der Arbeitsabläufe,
- aktuelle und langfristige Umsatzausfälle (Kunden- und Reputationsverlust) und
- aufwändige Schutz- und Vorsorgemaßnahmen zur Abwendung künftiger Angriffe

oftmals nur sehr schwer zu beziffern sind.

Signifikant für die im Netz erhältlichen und hier genutzten Dienstleistungen sind folgende Punkte: Die Produktpakete unterscheiden sich in der Dauer des Angriffs und der Anzahl der jeweiligen Angriffstage (30 oder 90 Tage). Außerdem unterscheiden sich die Angriffsmöglichkeiten in der Durchsatzrate/in der Stärke (i. d. R 15-20 Gigabit pro Sekunden). Es werden unterschiedliche Angriffsmethoden mit unterschiedlicher Stärke angeboten. Als Bezahlmethoden werden Bitcoin und PayPal verwendet. Für die Registrierung werden nur Benutzername, eine E-Mail-Adresse sowie ein selbst gewähltes Passwort benötigt.

[19] Vgl. Link11 DDoS-Report für die DACH-Region; **https://www.link11.com/de/ddos-report/.**

Fallbeispiel: DDoS-Angriffe

Die Kriminalpolizei Bielefeld ermittelte im Jahr 2017 gegen einen 24-jährigen deutschen Staatsangehörigen wegen des Verdachts der Computersabotage und Erpressung in mehreren Fällen.

Der Deutsche, der bei seinen Taten unter dem Pseudonym „zzb00t“ gehandelt hat, ist dringend verdächtig gewesen, durch Inanspruchnahme von Diensten, die im Internet Serviceleistungen aus dem Cyberbereich anbieten, Webseiten von geschädigten Unternehmen mittels Überlastung (sog. DDoS-Angriffe) zum Erliegen gebracht zu haben. In der Folge bzw. im Verlauf der DDoS-Angriffe wurde eine Forderung von Lösegeld in Form von Bitcoins an die Unternehmen geschickt, damit die Cyber-Angriffe täterseits eingestellt werden. Zum Zeitpunkt der im Mai 2017 veranlassten Durchsuchungsmaßnahmen war der Täter bei mehreren Internet-Diensten eingeloggt, die sog. IP-Stresstests vermarkten. Die auf dem Täter-Computer einsehbaren Webseiten zeigten aktuell laufende (DDoS-)Angriffe dieser Anbieter, welche auf verschiedene IP-Adressen ausgerichtet waren. Offensichtlich nutzte der Täter mehrere dieser Service-Anbieter, um von ihm ausgewählte Webseiten mit massenhaften Anfragen zu überfluten, so dass diese nicht mehr erreichbar waren. Im Verlauf der Ermittlungen konnte festgestellt werden, dass von dem Täter bzw. den Internet-Diensten über ein sog. Botnetz – also eine Vielzahl gekaperter und zusammengeschlossener Rechner –die Online-Präsenzen namhafter deutscher Firmen lahmgelegt wurden. Der Täter handelte nach bisherigen Erkenntnissen ausschließlich aus finanziellen Motiven und wollte über die Erpressung der Unternehmen an Bitcoin gelangen.

Der Täter nutzte außerdem einen Anbieter von Wegwerf-E-Mail-Adressen („byom.de“).
Dort lässt sich mittels einer selbst gewählten ID eine gesicherte E-Mail Adresse generieren, die öffentlich verwendet werden kann. Ein Abrufen der E-Mails ist mit der generierten Adresse nicht möglich. Nach Angaben des Anbieters werden die E-Mails in den Standardeinstellungen nach einer Stunde gelöscht.

Der Täter wurde zwischenzeitlich vom Amtsgericht Bielefeld zu einem Jahr und zehn Monaten Haft verurteilt.

Kurzbewertung:
Die Durchführung von DDoS-Angriffen ist aufgrund des Angebots der im Netz vertretenen Dienstleister auch ohne größere eigene fachliche Expertise möglich. Das Internet bietet hier nicht nur die Möglichkeit entsprechende Angriffs-Tools anzumieten, sondern verfügt auch über Instrumente, welche die Identität des Täters verschleiern.

DDoS-Angriffe zeichnen sich durch rasant steigende Bandbreiten aus. Sie erreichen auch durch die Nutzung von IoT-Geräten neue Höchstwerte. Aufgrund der defizitären Sicherheitsstandards vieler IoT-Geräte lassen sich diese oftmals problemlos in Botnetze integrieren. Es ist davon auszugehen, dass diese Entwicklung weiter anhält und z. B. die mittels Botnetzen durchgeführten DDoS-Angriffe an Quantität und Qualität zunehmen.

3.4 MOBILE MALWARE

Hinsichtlich des Besitzes von Mediengeräten (Smartphones, PCs, Internetzugang, Fernseher) ist laut einer JIM-Studie (Jugend, Information und Multimedia) aus dem Jahr 2017 eine fast hundertprozentige Versorgung aller Haushalte erreicht.[20] Die Marktentwicklung von konventionellen Computern hin zu mobilen Endgeräten wie Smartphones und Tablets hält weiterhin an.

Mobile Endgeräte sind im Gegensatz zum klassischen PC in der Regel ständig online. Die Nutzer wickeln mittlerweile einen Großteil ihrer digitalen Aktivitäten über diese Geräte ab. Transaktionen im Onlinebanking, Zugriff auf E-Mail-Konten und Soziale Netzwerke oder auch Aktivitäten im Bereich des E-Commerce, oft über entsprechende Apps, machen Smartphones und Tablet-Computer zum attraktiven Angriffsziel für Kriminelle.

Aufgrund der vorherrschenden Update-Zyklen bleiben erkannte Sicherheitslücken in der Gerätesoftware oftmals längere Zeit ungeschlossen oder werden als Folge immer kürzerer Produktzyklen niemals geschlossen, weil der Supportzeitraum abgelaufen ist.

Schadprogramme gelangen meist durch die Nutzer selbst auf Mobilgeräte. Mangelnde Sensibilität für die Gefahren im Umgang mit mobilen Endgeräten, wie z. B. das Installieren von Apps aus nicht vertrauenswürdigen Quellen, hebelt technische Schutzmaßnahmen aus und ermöglicht Angreifern Wege in abgesicherte Netze.

Nutzer von mobilen Endgeräten und Geräten des Smart Home müssen weiter sensibilisiert werden.

Die wachsende Bedeutung mobiler Endgeräte für Cyberkriminelle spiegelt sich insbesondere in einer Zunahme von Malwareentwicklungen im Bereich mobiler Betriebssysteme wider. Laut eines Berichts des IT-Sicherheitsunternehmens Kaspersky zielt bekannte Schadsoftware weit überwiegend auf Android-Systeme ab.[21] Das G4C-Mitglied Symantec berichtet von einer Zunahme mobiler Malware um 54 % in 2017 im Vergleich zum Vorjahr und einer Gesamtzahl von 27.000 verschiedenen Varianten.[22]

Auch das BSI bestätigt in seinem Lagebericht 2017 diese Tendenzen und führt als Schwachstellen u. a. die unzureichende Verschlüsselung bei der Nutzung persönlicher Daten, den sicherheitskritischen Softwarestand bei den Mobilgeräten und das eigentliche Nutzerverhalten an. Darüber hinaus sieht das BSI im Falle fehlender Sicherheitsupdates eine Gefährdung durch den Missbrauch der Geräte (z. B. Einbindung in ein Botnetz) und ein hohes Risiko von Schadsoftware im mobilen Kontext.[23]

Aus polizeilichen Datenbeständen lassen sich aktuell kaum belastbare Zahlen zum Aufkommen mobiler Malware in Deutschland ableiten. Dies dürfte insbesondere auf das im Deliktsbereich Cybercrime schwach ausgeprägte Anzeigeverhalten und – daraus resultierend – das hohe Dunkelfeld zurückzuführen sein.[24]

---

[20] **Https://www.mpfs.de/fileadmin/files/Studien/JIM/2017/JIM_2017.pdf**.
[21] **Http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_Mobile-Report_GER_FINAL.pdf.**
[22] Vgl. Symantec ISTR: **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf.**
[23] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**
[24] Vgl. hierzu auch **https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**

Im Jahr 2017 führte das BKA eine Bund-Länder-Erhebung zu mobiler Malware durch. Demnach wurden 330 Fälle polizeilich bekannt. Dies entspricht einem Anteil von 6,4 % an allen polizeilich angezeigten Fällen von Malware-Infektionen im Jahr 2017.

3.5 DIEBSTAHL DIGITALER IDENTITÄTEN/PHISHING IM ONLINE-BANKING

Nach wie vor ist die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte ein gängiges und lukratives Geschäftsmodell. Für Täter sind alle Daten bzw. Ausprägungen von digitalen Identitäten interessant, die für kriminelle Aktivitäten genutzt werden können. Hierzu zählen z. B. Zugangsdaten für Kommunikationsdienste, zu Bankportalen und Buchungssystemen sowie zu Onlineshops. Die erlangten digitalen Identitäten werden anschließend für kriminelle Zwecke missbraucht (vielfach Betrugsdelikte) oder meist über illegale Verkaufsplattformen der Underground Economy verkauft.

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.*

Um in den Besitz personenbezogener Informationen zu gelangen, setzen die Täter verschiedene Arten von Schadsoftware (Spyware[25], Trojaner[26] und Keylogger[27]), häufig aber auch Phishing-Mails, ein.

[25] 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.
[26] 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.

Hierzu werden die gestohlenen Identitäten mittels der eingesetzten Schadsoftware an spezielle Speicherorte im Internet (sog. Dropzones), auf welche die Täter bzw. deren Auftraggeber zugreifen können, ausgeleitet. Beim Einsatz von Phishing werden die Geschädigten zur Eingabe der relevanten Informationen auf täterseitig kontrollierte Server verleitet.

Im Rahmen von Open-Source-Recherchen auf einer Plattform der Underground Economy ist das BKA 2017 auf eine Aggregation von ca. 500 Mio. E-Mail-Adressen/Passwort-Kombinationen in strukturierter Form aufmerksam geworden, die aus unterschiedlichen Zeitfenstern und Quellen stammen dürften und mit hoher Wahrscheinlichkeit durch einen unbekannten „Sammler" zusammengestellt worden sind. Diese Datensammlung wird in der Underground Economy als „Anti Public Combo List" bezeichnet und kostenfrei zum Download angeboten. Die Zugangsdaten dürften aus einer Vielzahl von Hacks von Internetseiten über einen längeren Zeitraum stammen. Die aktuellsten ausgespähten Zugangsdaten in dieser Liste stammen aus Dezember 2016. Die Daten wurden vom BKA an die hierfür zuständige Sicherheitsbehörde (BSI) und das Hasso-Plattner-Institut (HPI) übermittelt, welches einen Webdienst „Identity Leak Checker" betreibt, in dem zum damaligen Zeitpunkt bereits 3,7 Mrd. kompromittierte Zugangsdaten gespeichert waren. Dieser Dienst kann von jedermann zur Überprüfung seiner etwaigen Betroffenheit genutzt werden.[28]

Das BSI hält in seinem Lagebericht für 2017 fest, dass die Verwendung von persönlichen Daten aus Datenabflüssen bei großen Dienstleistern derzeit immer häufiger beobachtet wird.[29] Dies wird von ENISA (European Union Agency for Network and Information Security) im „Threat-Landscape-Report" bestätigt, wonach im Jahr 2017 die Anzahl der Vorfälle von „Data Breaches" um 25 % gegenüber dem Vorjahr angestiegen ist und fortlaufend weitere Vorfälle zutage treten.[30]

---

[27] 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.

[28] **Https://sec.hpi.uni-potsdam.de.**

[29] Die Lage der IT-Sicherheit in Deutschland 2017, BSI.

[30] **Https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport**

Data Breaches:

Unter dem Begriff „Data Breach" werden sowohl bewusste als auch unbewusste Verluste sensibler Daten in eine als nicht vertrauenswürdig anzusehende Umgebung 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.

Die im Rahmen des iOCTA (Internet Organised Crime Threat Assessment) zitierte Webseite **www.breachlevelindex.com** weist eine Gesamtzahl von ca. 1,9 Mrd. gestohlenen Datensätzen in der ersten Hälfte des Jahres 2017 aus. Annähernd die Hälfte der Vorfälle von Data Breaches wurde in Europa registriert (49 %).[31]

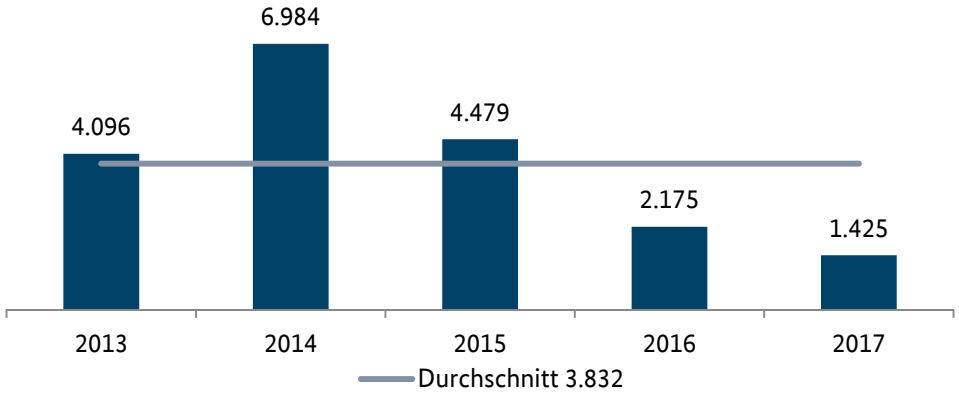
Der Fokus der medialen Berichterstattung lag im Jahr 2017 auf dem Verlust von Datensätzen von 148 Mio. US-Bürgern bei einer privatrechtlichen Auskunftsdatei. Bei dem zuvor erwähnten Breach, der sich zwischen Mai und Juli 2017 ereignete, gingen insbesondere Namen, Geburtsdaten, Adressen, Darlehens- und Kreditkarteninformationen sowie Führerschein- und Sozialversicherungsnummern verloren.[32] Diese Vorkommnisse führten in den USA zu einer öffentlichen Diskussion über verschärfte Cybersicherheitsgesetze, die weiterhin anhält.

Eine häufige Variante des digitalen Identitätsdiebstahls ist neben dem Massendiebstahl von digitalen Daten weiterhin das „Phishing im Zusammenhang mit Onlinebanking".

Im Jahr 2017 wurden dem BKA von den Polizeien der Länder 1.425 Sachverhalte zum Phänomen Phishing gemeldet. Im Vergleich zum Jahr 2016 (2.175) bedeutet dies einen Rückgang der Fallzahlen um 34,5 % auf den tiefsten Stand seit fünf Jahren und bestätigt die auch von Europol festgestellte rückläufige Tendenz bei diesem Phänomen.

[31] **Http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf.**
[32] **Https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.846d59ae8dde.**

Fälle von Phishing im Onlinebanking



Da Banken im Falle eines festgestellten Phishing-Vorfalls beim Onlinebanking die Erstattung des beim Kunden entstandenen Schadens regelmäßig nur bei polizeilicher Anzeigenerstattung des Vorfalls vornehmen, dürfte das Dunkelfeld in diesem Deliktsbereich sehr gering sein.[33]

Die Täter setzen bei Phishing nicht nur auf rein technische Lösungen, sondern versuchen mittels des sog. Social Engineerings[34] an die notwendigen Kundeninformationen zu gelangen. So wird durch die Täter der Versuch unternommen, die in Deutschland verwendeten Autorisierungsmechanismen im Onlinebanking, die ein aktives Handeln des Kontoberechtigten erfordern (unter Nutzung eines zweiten Kommunikationskanals[35]), auszuhebeln.

Seit 2014 lässt sich ein rückläufiger Trend bei den Fallzahlen von Phishing im Onlinebanking feststellen. Als Erklärungsansatz hierfür kann die konsequente Weiterentwicklung und Verfeinerung der Mechanismen zur bankenseitigen Detektion derartiger Angriffe, einschließlich der Erkennungsmöglichkeit malwarebasierter Abgriffe beim Online-Banking, gesehen werden.

Darüber hinaus sieht das G4C in 2017 eine rückläufige Tendenz beim malwarebasierten Ansatz bei Betrug im Online-Banking, u. a. da täterseitig der malwarebasierte Ansatz beim Phishing im Onlinebanking gegenüber dem Abgriff von Kontoinformationen durch den Einsatz von Phishing-Mails mit einem wesentlich höheren technischen Aufwand verbunden ist.

Als Beispiel für eine von den Tätern betriebene Anpassung des E-Mail-basierten Phishings kann die Ausleitung von Vermögenswerten aus kompromittierten Konten über virtuelle Geldbörsen (z. B. Bitcoin-Wallets) angeführt werden. Nach Erkenntnissen des G4C-Mitglieds Commerzbank werden dabei die für Transaktionen von Geldkonten auf Wallets erforderlichen Informationen (im Regelfall der abfotografierte Personalausweis des rechtmäßigen Kontoinhabers) zur Identitätsverifizierung beim Phishing mit abgegriffen.

---

[33] Für die Banken ihrerseits besteht ab 2019/2020 eine Meldeverpflichtung gegenüber der European Banking Authority (EBA), so dass in der Folge dort ein umfangreiches Lagebild zu Phishing vorliegen dürfte.
[34] Soziale Manipulation – Beeinflussung einer Person zur Preisgabe vertraulicher Informationen. Bei Cyber-Angriffen mittels Social Engineering versuchen Kriminelle die Geschädigten dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadcodes auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.
[35] Sog. two-factor authentication.

Trotz der quantitativ rückläufigen Entwicklung bleibt Phishing im Hinblick auf die vorhandenen Möglichkeiten und die zu erzielenden kriminellen Erträge weiterhin ein lukratives und damit attraktives Betätigungsfeld für die Täterseite. So betrug die durchschnittliche Schadenssumme im Bereich „Phishing im Zusammenhang mit Onlinebanking“ im Jahr 2017 rund 4.000 Euro pro Fall. Dies ergibt eine Gesamtschadenssumme in Höhe von 5,7 Mio. Euro, welche indes deutlich unter der durchschnittlichen Schadenssumme der vergangenen fünf Jahre lag (Durchschnitt 2013-2017: 15,3 Mio. Euro).

3.6 CYBERCRIME-AS-A-SERVICE

„Cybercrime-as-a-Service“ (CaaS), illegale Foren und inkriminierte Handelsplattformen der Underground Economy befördern dynamische Entwicklungen in nahezu allen Kriminalitätsfeldern und haben sich als erfolgreiche Geschäftsmodelle etabliert. Digitale Marktplätze spielen auch bei der Begehung von Straftaten im Bereich Cybercrime eine weiter ansteigende Rolle. Hier werden einerseits kriminelle Dienstleistungen angeboten bzw. gesucht, andererseits tauschen sich die Cyberkriminellen in entsprechenden Foren über ihr kriminelles Know-How (z. B. über das Ausnutzen von Sicherheitslücken) aus.

In der Underground Economy werden Produkte und Services zu folgenden Phänomen aus dem Cyberbereich angeboten:

- Ransomware,
- Botnetze für kriminelle Aktivitäten,
- DDoS Attacken,
- Malware-Herstellung und -Verteilung,
- Datendiebstahl,
- Verkauf/Angebot sensibler Daten (Zugangs- oder Zahlungsdaten),
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität,
- Portale zum Test der erworbenen bzw. hergestellten Schadsoftware auf Detektierbarkeit und
- Dropzones zum Ablegen illegal erlangter Informationen und/oder Waren.

Ein aktueller Trend ist die Professionalisierung der Täter im Bereich CaaS. So kann durch die kriminellen Dienstleistungen in Form einer Auftragsarbeit der gesamte Prozess - von der Beratung des „Kunden“ über die Auswahl einer Sicherheitslücke, der Anpassung der Schadsoftware, der Einbringung der Malware auf dem Zielsystem bis hin zur Organisation der inkriminierten Geldströme - an spezialisierte Dienstleister abgegeben werden. Eigene technische Fähigkeiten des „Kunden“, also des Kriminellen, der diese Werkzeuge dann beispielsweise für Cyber-Angriffe nutzt, sind kaum mehr erforderlich. Dadurch öffnet sich das Phänomen Cybercrime für eine breite Nutzerschicht ohne tiefgehende technische Kenntnisse.

Zahlen zum Phänomen CaaS liegen nicht vor. Es dürfte nach hiesiger Einschätzung aber weiter von einer großen Zahl der Marktplätze (sowohl im Clear- bzw. Visible Web, als auch im Darknet) und einer damit verbundenen großen Angebotspalette auszugehen sein.

3.7 UNDERGROUND ECONOMY – DIGITALE SCHWARZMÄRKTE

Illegale Foren oder Marktplätze im Clearnet, Deepweb[36] und im Darknet spielen eine weiterhin größer werdende Rolle bei der Begehung von Cybercrime.

Es werden weiterhin die unter dem Punkt CaaS aufgeführten Dienstleistungen angeboten. Allerdings dienen die Foren auch unverändert der Kommunikation von Cyberkriminellen, dem Transfer von kriminellem Know-how sowie dem Austausch über das Ausnutzen von Sicherheitslücken und insofern der Tatvorbereitung der Cyber-Straftaten.

Neben diesen CaaS zuzurechnenden Sachverhalten ist weiterhin eine zunehmende Verlagerung der anderen, klassischen Kriminalitätsphänomene in den virtuellen Raum festzustellen.
Im Clear Web, aber insbesondere auch im Darknet, werden illegale Waren wie Drogen, Waffen, Falschgeld, gefälschte Ausweise, gestohlene Kreditkartendaten oder gefälschte Markenartikel angeboten. Vermeintliche Anonymität, ein mutmaßlich geringeres Entdeckungsrisiko und die Möglichkeit, über die Marktplätze Kunden weltweit zu erreichen, dürften hier als Erklärungsansätze dienen. Selbst die Foren und Marktplätze im Darknet stehen jedem Internetnutzer offen. Eine tiefergehende technische Expertise ist auch hierfür nicht erforderlich.

Während es für die vorgenannten Delikte keine spezifischen Plattformen gibt, erfolgt demgegenüber der Handel mit Kinderpornografie in der Regel über eigens dafür geschaffene Plattformen.

Die Administratoren der Foren partizipieren häufig über ein Treuhand-System an den Erlösen aus dem Verkauf der illegalen Waren.

Zur Bezahlung der gehandelten Waren werden ausschließlich digitale Kryptowährungen[37] akzeptiert, die ein anonymes bzw. pseudonymes Bezahlen ermöglichen.

[36] Das Deepweb ist jener Teil des Internet, der nicht durch allgemeine Suchmaschinen auffindbar ist. Inhalte sind beispielsweise Datenbanken, Intranets oder Fachwebseiten.
[37] Alternative Bezeichnungen: virtuelle, alternative oder digitale Währungen, Geld oder Devisen.

Fallbeispiel: Digitale Schwarzmärkte – Underground Economy

Das BKA führte unter der Sachleitung der Generalstaatsanwaltschaft Frankfurt/M. in enger Kooperation mit der High Tech Crime Unit der niederländischen Polizei seit Januar 2017 die polizeilichen Ermittlungen gegen die verantwortlichen Betreiber der über das Tor-Netzwerk erreichbaren Darknet-Handels-/Verkaufsplattform „HANSA Market“, welche zuletzt die zweitgrößte Plattform war.

Die Ermittlungen richteten sich insbesondere gegen zwei 30- und 31-jährige Administratoren wegen des Verdachts des Verstoßes gegen das Betäubungsmittelgesetz. Zielrichtung des Verfahrens der niederländischen Polizei war die technische Übernahme des Marktplatzes, um sog. Powerseller identifizieren zu können.

Im Juni 2017 erfolgten die Durchsuchungen mehrerer Objekte und die Festnahme der Beschuldigten. Gleichzeitig wurde der Marktplatz von der niederländischen Polizei übernommen und anschließend vom Netz genommen.

Sichtbar wurden die Maßnahmen für die Underground Economy-Szene durch die Platzierung des „Seizure-Banners“:

Die polizeilichen Maßnahmen gegen diese Plattform in der Underground Economy bestätigen erneut den illegalen Handel von Betäubungsmitteln im Internet.

Außerdem konnte durch die polizeilichen Ermittlungen ein hochgradig professionelles und arbeitsteiliges Vorgehen der Beschuldigten nachgewiesen und das Täternetzwerk zerschlagen werden.

Neben HANSA Market wurde 2017 das größte über das Tor-Netzwerk erreichbare deutschsprachige Forum „Deutschland im Deep Web“ (DiDW) von den Sicherheitsbehörden vom Netz genommen.

Fallbeispiel: Digitale Schwarzmärkte – Underground Economy

DiDW wurde von einem 30-jährigen deutschen Staatsangehörigen administriert und betrieben, welcher im Juni 2017 in Untersuchungshaft genommen wurde. Im Rahmen der Ermittlungen wurde der Vollzugriff auf das Produktivsystem des Forums erlangt, die dazugehörige Datenbank gesichert und im Anschluss die Plattform im Juni abgeschaltet. Zum Zeitpunkt der Abschaltung dieser Darknet-Plattform waren dort über 20.000 User registriert. Auf „DiDW" wurden Betäubungs-/Arzneimittel, erlaubnispflichtige Schuss-/Kriegswaffen, Falschgeld und gefälschte Ausweisdokumente gehandelt.

In die medienöffentliche Wahrnehmung trat das Forum „DiDW", da der 18-jährige Schütze des Amoklaufs am Münchener Olympia-Einkaufszentrum im Juli 2016 die Tatwaffe, eine Pistole Glock 17, über diese Plattform gekauft hatte. Beim Amoklauf tötete er neun Menschen sowie sich selbst.

Im Rahmen der weiteren Auswertung der Führungsebene des Forums „DiDW" wurden Ermittlungsverfahren gegen zwei Moderatoren und einen Powerseller eingeleitet. Alle drei User waren neben ihrer Rolle im Forum aktive Verkäufer von illegalen Betäubungsmitteln, rezeptpflichtigen Arzneimitteln und weiteren inkriminierten Waren bzw. Dienstleistungen.

3.8 ANGRIFFE AUF WIRTSCHAFTSUNTERNEHMEN/ CYBERSPIONAGE

Wirtschaftsunternehmen stehen weiterhin im Zielspektrum von Cyberkriminellen. Auch eine 2017 durchgeführte Studie der KPMG AG belegt eine große Betroffenheit von Unternehmen im Bereich der Computerkriminalität.[38]

Die aufgeführten Phänomene wie Ransomware, Malware, DDoS-Angriffe und Botnetz-Tätigkeiten stellen auch für Unternehmen am Wirtschaftsstandort Deutschland eine Bedrohung mit hohem Schadenspotenzial dar. Die in Deutschland ansässigen Unternehmen bieten auch lohnenswerte Angriffsziele für Cyber-Spionage.

Laut BSI steigt die Zahl der Cyber-Spionage-Angriffe auf Wirtschaftsunternehmen nach einem Rückgang in 2015/2016 mittlerweile wieder an.[39] Insbesondere bei den Unternehmen, die sich umfangreich im Ausland engagieren, sind Angriffe staatlicher bzw. staatlich gesteuerter Akteure feststellbar.

Typisch für staatlich gesteuerte Cyber-Attacken sind sog. APT-Angriffe (Advanced Persistent Threat).

[38] **Https://home.kpmg.com/de/de/home/themen/2017/04/ecrime-studie.html.**
[39] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**

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.

Das BKA sieht folgende Befunde im Bereich der Cyberspionage:

- Cyber-Angriffe gegen Deutschland sind als eine wichtige Methode der Informationsgewinnung für ausländische Nachrichtendienste etabliert.
- Weltweit werden bei Cyberspionage-Angriffen immer wieder dieselben Serverinfrastrukturen und Schadsoftwarekomponenten verwendet.
- Hauptangriffsvektor ist häufig der Versand von Spear-Phishing-E-Mails[40], sowohl mit maliziösen Links als auch mit Schadanhang, mittels derer der Geschädigte bzw. dessen Systeme infiziert werden. Den Cyberspionage-Angriffen gehen in der Regel professionelle Abklärungen der Geschädigten über Social Engineering, aber auch klassische Aufklärung vor Ort voraus.
- Diverse Veröffentlichungen zahlreicher IT-Sicherheitsunternehmen weisen regelmäßig auch auf eine deutsche Betroffenheit bei Cyberspionage-Angriffen hin. Eine konkrete und tatsächlich fass- und belastbare Attribution ist bei diesen Angriffen allerdings nicht bzw. kaum möglich.

Auch im Bereich der Cyberspionage ist von einer hohen Dunkelziffer durch nicht erkannte bzw. nicht angezeigte Angriffe auszugehen.

3.9 ANGRIFFE AUF KRITISCHE INFRASTRUKTUREN (KRITIS)

KRITIS sind Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen. Ein Ausfall oder eine Beeinträchtigung kann zu nachhaltig wirkenden Versorgungsengpässen bzw. erheblichen Störungen der öffentlichen Sicherheit führen.[41]

Grundsätzlich sind KRITIS-Betreiber dabei den gleichen Gefahren ausgesetzt wie alle anderen Unternehmen. Allerdings ist das Schadenspotenzial wesentlich höher. Deshalb gilt dieser Bereich nicht nur als Ziel für finanziell motivierte Täter, sondern potenziell auch für Täter mit politischer Motivation. Der Bereich Staat und Verwaltung liegt per se im Angriffsspektrum dieser Täter.

[40] Verfeinertes Phishing mit einem gezielteren persönlichen Ansatz („spear" – steht für Speer).
[41] **Http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Flyer.pdf**.

Für die KRITIS-Unternehmen besteht bei festgestellten Vorfällen eine Verpflichtung zur Meldung an das BSI nach dem IT-Sicherheitsgesetz. In seinem Lagebericht 2017[42] weist das BSI für den Zeitraum seit Inkrafttreten dieses Gesetzes (Juli 2015) bis zum 30.06.2017 insgesamt 34 Meldungen aus. Dabei lag der Schwerpunkt im Sektor Informationstechnik und Telekommunikation.

Die grundsätzliche Verwundbarkeit von KRITIS-Unternehmen wurde in der jüngeren Vergangenheit exemplarisch durch die Cyber-Attacken auf die Deutsche Telekom AG (Mirai) und die Deutsche Bahn AG (WannaCry) deutlich.

Es bleibt festzustellen, dass der Wirtschaftsstandort Deutschland aufgrund der vergleichsweise hohen Konkurrenzfähigkeit und technologischen Expertise ein interessantes Ziel für Cyber-Spionage oder allgemeinkriminelle Hacker darstellt. Dementsprechend stehen auch die Betreiber kritischer Infrastrukturen im Fokus von Cyber-Angriffen. In 2017 weltweit festgestellte Cyber-Angriffe auf den Energiesektor, die Hacker-Angriffe auf das Netz der Bundesverwaltung sowie auf KRITIS-Unternehmen abzielende Ransomware-Angriffe veranschaulichen das Bedrohungspotenzial auch für Deutschland.

[42] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**

4 Schäden durch Cybercrime

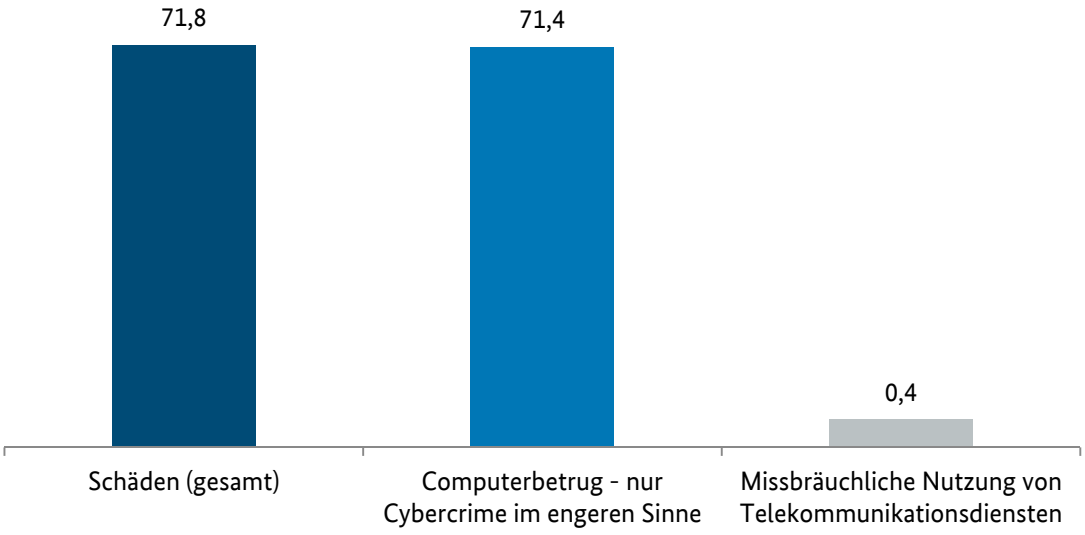
Cybercrime verursacht bei Bürgern, Behörden und Wirtschaftsunternehmen hohe materielle und immaterielle Schäden. Medienberichte über millionenfachen Datendiebstahl oder Manipulationen einer Vielzahl von technischen Geräten führen zu einer deutlichen Beeinträchtigung des Sicherheitsgefühls der Bürger.

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 wiederum als Angriffsziele krimineller Hacker dienen und missbraucht werden können. Gemäß einer ARD/ZDF-Onlinestudie ist 2017 die Zahl der Onlinenutzer auf insgesamt 62,4 Mio. gestiegen. Dies entspricht einem Anteil von 89,8 % an der deutschsprachigen Bevölkerung ab 14 Jahren und einem Zuwachs gegenüber 2016 von 4,4 Mio. Menschen[43].

Jedoch werden Schäden im Deliktsbereich Cybercrime in polizeilichen Statistiken ausschließlich für Fälle des Computerbetrugs als Cybercrime im engeren Sinne und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen. Die für 2017 ausgewiesene Gesamtschadenssumme betrug 71,8 Mio. Euro (2016: 51,6 Mio. Euro). Vom erfassten Gesamtschaden entfielen rund 71,4 Mio. Euro (2016: 50,9 Mio. Euro) auf den Bereich Computerbetrug und über 0,4 Mio. Euro (2016: 0,7 Mio. Euro) auf die missbräuchliche Nutzung von Kommunikationsdiensten.

Da lediglich in den genannten Deliktsbereichen eine statistische Schadenserfassung erfolgt, sind auf Basis der PKS keine belastbaren Aussagen zum tatsächlichen monetären Gesamtschaden durch Cybercrime möglich.

Schäden durch Cybercrime in Mio. Euro (2017)[44]



[43] **Http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2017/**.
[44] Bei Fällen mit unbekannter Schadenshöhe wird ein symbolischer Schaden von einem Euro erfasst.

Finanzielle Schäden eines erfolgreichen Cyber-Angriffs sind oft nicht gänzlich bekannt oder bezifferbar. 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 lahmgelegt werden. Zur Darstellung des tatsächlichen Schadensausmaßes müssen demnach mehrere Faktoren berücksichtigt werden. Hierzu liegen Studien privater Firmen vor: Beispielsweise stellten 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 mache laut der Untersuchung etwa ein Viertel des Schadens aus.[45]

In der Studie des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) haben Befragungen von Internetnutzern ergeben, dass in 54 % der Fälle ein finanzieller Schaden entstanden sei.[46]

Große Diskrepanz zwischen Schadenserhebungen in der polizeilichen Statistik und den Feststellungen der Privatwirtschaft.

BITKOM bemisst in einer Studie den finanziellen Schaden für die deutsche Wirtschaft durch Delikte der Cybercrime für das Jahr 2017 mit 55 Mrd. Euro.[47] Grundlage dieser Zahl sind Angaben von betroffenen Unternehmen, die im Rahmen einer Umfrage 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.

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

Fallbeispiel: Schaden durch Cybercrime

Das Landgericht Köln verurteilte im Juli 2017 den Verursacher der Ausfälle der Router eines Telekommunikationsanbieters zu einer Freiheitsstrafe von einem Jahr und acht Monaten. Bei der Betrachtung der Kosten machte das betroffene Unternehmen einen Schaden von zwei Mio. Euro geltend, wobei das Gericht ca. 50 % tatsächlich (als durch den Cyberangriff entstandene Kosten) anerkannte. So wurden z. B. zusätzliche Kosten für das bei der Störungsbeseitigung eingesetzte Personal nicht berücksichtigt.[48]

Kurzbewertung:
Die von Security-Dienstleistern in ihren Studien aufgeführten teilweise enormen Schadenssummen im Bereich Cybercrime müssen auch vor dem Hintergrund der aufgeführten Gerichtsentscheidung bewertet werden.

[45] **Https://www.csis.org/analysis/economic-impact-cybercrime.**
[46] **Https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**
[47] **Https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.**
[48] **Https://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2017/118_KLs_4_17_Urteil_20170728.html.**

5 Trends und Ausblick

Neben den Entwicklungen in den aufgeführten Kriminalitätsphänomenen dürften nachfolgend aufgeführte Themen Einfluss auf die Entwicklung des Querschnittsphänomens Cybercrime auch über die Landesgrenzen hinweg haben. Die Strafverfolgungsbehörden müssen auch auf diese Bereiche ihre Aufmerksamkeit richten.

5.1 DIGITALE WÄHRUNGEN

Digitale Währungen, wie z. B. Bitcoin (BTC), Litecoin (LTC) oder Ethereum (ETH), sind virtuelle Geldeinheiten, deren Herstellung und Verwendung auf mathematischen Berechnungen und kryptografischen Verfahren beruhen und deren Nutzung zumeist lediglich die Installation einer „Wallet"-Software erfordert.

Die Verwendung digitaler Währungen ist nicht illegal. Erwerb und Veräußerung, also die Umwandlung von gesetzlichen Zahlungsmitteln/in gesetzliche Zahlungsmittel, sind z. B. auf zahlreichen Online-Börsen möglich. BTC ist die aktuell am stärksten verbreitete digitale Währung. In zahlreichen Online-Shops sowie einigen Geschäften und Cafés kann bereits mit BTC bezahlt werden.

Virtuelle Währungen werden mittels kryptografisch abgesicherter Protokolle direkt zwischen den Nutzern ohne Einbindung von Notenbanken oder Kreditinstituten gehandelt. Insoweit sind sie staatlichen Eingriffsmöglichkeiten weitgehend entzogen. Transaktionen laufen anonym ab, solange Quell- und Zieladressen keinem Besitzer zugeordnet werden können.

Kryptowährungen stellen somit ein attraktives digitales Zahlungsmittel für Kriminelle dar. Verwendung finden sie in fast allen dargestellten Phänomenbereichen der Cybercrime. Eine besondere Gefahr besteht darin, dass digitale Währungen insbesondere für Geldwäschehandlungen und zur Finanzierung terroristischer Aktivitäten missbraucht werden können.

Weitere Anreize für Kriminelle bestehen im Diebstahl dieser Währungen sowie dem Inkriminieren der Blockchain[49]. Beispielsweise geschah dies, indem die Täter Zugriff auf einen sog. Seedgenerator zu Bitcoin-Wallets erlangten. Mit diesem ist es für die Nutzer möglich, einen „Generalschlüssel" für ihre Wallets zu erstellen. Durch Zugriff auf den Generalschlüssel konnten die Täter beispielsweise Kryptowährung im Wert von ca. vier Mio. US-Dollar erbeuten. Außerdem wurde bekannt, dass von einer anderen Plattform virtuelle Währungen in Höhe von 430 Mio. Euro gestohlen wurden.[50]

Anfang 2018 wurden von Forschern der Rheinisch-Westfälischen Technischen Hochschule Aachen und der Goethe-Universität Frankfurt am Main in der Blockchain einer digitalen Währung mehrere illegale Inhalte entdeckt, die aufgrund der Funktionsweise dieser Technologie nicht mehr löschbar sind. Es handelte sich hierbei um nicht direkt zur Transaktion gehörende Informationsfragmente, die täterseitig in der Blockchain abgelegt wurden. Insgesamt haben die Forscher mehr als 1.600 Dateien gefunden, darunter zwei Linklisten, die auf kinderpornografische Inhalte verweisen.

---

[49] Blockchain bezeichnet die zugrundeliegende Technologie für Kryptowährungen, u. a. Bitcoin. Bei der Blockchain handelt es sich um ein öffentliches oder privates, dezentral geführtes, digitales Buchführungssystem (Distributed Ledger Technology) zur kontinuierlichen Aufzeichnung von Transaktionen. Starke kryptografische Verkettung der Transaktionen in Blöcken gewährleistet Fälschungssicherheit und Pseudonymität.

[50] **Https://iota-deutschland.de/timeline/iotas-im-wert-von-mehreren-millionen-durch-seed-scam-gestohlen/.**

Bislang wurden konkrete Fälle der Verbreitung, des Besitzes oder der Drittbesitzverschaffung kinderpornografischen Materials nicht bekannt. Allein die bestehende technische Möglichkeit, illegale Inhalte in die Blockchain zu programmieren, stellt die Sicherheitsbehörden jedoch vor große Herausforderungen.

5.2 INTERNET DER DINGE

Der Begriff „Internet der Dinge“ (Internet of Things; IOT) beschreibt den Trend, dass neben den standardmäßig genutzten Geräten (Computer, Smartphone, Tablet) zunehmend auch sog. intelligente Endgeräte an das Internet angeschlossen werden und durchgängig online sind. Dazu zählen Haushaltsgeräte wie beispielsweise Kühlschränke, Fernseher oder Router, aber auch Sensoren, über die andere Geräte via Internet per Smartphone oder Tablet gesteuert werden. Diese Geräte verfügen in der Regel über eine eigene Rechenleistung und sind mit entsprechenden Betriebssystemen ausgestattet, welche oftmals eigens für die Geräte durch den Hersteller auf Basis von Open-Source-Codes entwickelt werden.

Ein wesentlicher Aspekt der Sicherheit beim Internet der Dinge betrifft die Netzwerktechnik. Die Verbindungen beim IoT basieren nicht nur auf WLAN, sondern z. B. auch auf Bluetooth, Near Field Communication (NFC) und Radio-Frequency Identification (RFID[51]). Die Absicherung muss daher viele verschiedene Verbindungsarten und Schnittstellen berücksichtigen.

Smart Home eröffnet unzählige neue Möglichkeiten zur Begehung von Straftaten.

Viele IoT-Geräte sind leicht angreifbar: Offene Ports ohne Authentifizierung, voreingestellte Standard-Login-Daten oder fehlende Security-Updates sind nur einige Schwachstellen. Viele Hersteller, die ihre Produkte internetfähig machen wollen, haben noch keine Erfahrung mit der Entwicklung sicherer Software. Sie stehen unter Zeitdruck, wollen keine Verzögerungen bei der Markteinführung in Kauf nehmen und scheuen zusätzliche Kosten, um das nötige Know-how aufzubauen oder einzukaufen. Herstellerseitig wäre jedoch eine fortlaufende Aktualisierung der Firmware zum Schutz der Anwender notwendig.

DDoS-Angriffe zeichnen sich aufgrund der Nutzung von zahlreichen zusätzlichen Geräten des Internets der Dinge durch rasant steigende Bandbreiten aus. Die erreichbaren Bandbreiten nehmen hier Größenordnungen an, die mittels vormaliger Infektionen von insbesondere Desktop-PCs nicht erzielt werden konnten. Hierdurch erhöht sich das Gefahrenpotenzial auch für große Internetdienstleister, deren Infrastrukturen vormals Angriffen standhielten. Beispiel hierfür waren die 2016 durchgeführten Angriffe mittels des Mirai-Botnetzes. Mittlerweile gibt es eine Vielzahl von Mirai-Nachfolgern und -Varianten.

Forscher warnen beispielsweise davor, dass sich „IoTroop/IoT_reaper“ zu einem der größten Botnetze der vergangenen Jahre entwickeln könnte.[52] Es soll sich deutlich schneller vergrößern als das Mirai-Botnetz. Nach aktuellem Stand soll IoTroop/IoT_reaper fast zwei Mio. Webcams, Sicherheitskameras und digitale Videorecorder kontrollieren.

[51] „Identifizierung mit Hilfe elektromagnetischer Wellen“.
[52] **Https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/iot_reaper/**.

Während Mirai insbesondere auf die Erzeugung von Web-Traffic für DDoS-Angriffe ausgerichtet war, ist die Funktion von IoTroop/IoT_reaper noch unklar.

Das Botnetz „Satori“ hingegen hat es besonders auf Heimrouter und IoT-Geräte abgesehen, um Kryptowährungen zu schürfen. Das Botnetz missbraucht hierzu eine Schwachstelle in der Schürf-Software Claymore. Der Schadcode tauscht die Wallet-Adresse der Geschädigten gegen eine eigene aus, was dazu führt, dass die Geräte unbemerkt für die Drahtzieher des Botnetzes schürfen.[53]

Das Botnetz „Hide’n Seek“ (HNS) fokussiert sich indes überwiegend auf IP-Kameras. Die aktuellen Erkenntnisse bei der Untersuchung des „Hide’n Seek“ Bots zeigen, dass dieser eine größere Komplexität ausweist und neue Fähigkeiten hat. Mit HNS ist Informationsdiebstahl möglich und der Bot ist potenziell für Spionage oder Erpressung geeignet.[54]

Darüber hinaus wurde bekannt, dass Kriminelle IoT-Geräte mittels eines weiteren Mirai-Abkömmlings („OMG“-Botnet) kapern und diese als Proxy missbrauchen. Ziel der Drahtzieher ist es, den Datenverkehr ihrer illegalen Aktivitäten, wie beispielsweise Hack-Versuche von Netzwerken oder Datendiebstahl, zu tarnen.[55]

Da sich der Trend zum sog. Smart Home, d. h. die Vernetzung von Haustechnik und Haushaltsgeräten (z. B. Jalousien, Heizung, Garagentor etc.) und die gezielte Fernsteuerung der Funktionen über das Heimnetzwerk und das Internet, zunehmend verbreitet, eröffnen sich unzählige neue Möglichkeiten zur Begehung von Straftaten (z. B. Deaktivierung der häuslichen Alarmanlage zur Vorbereitung von Einbrüchen, Manipulation von Kraftfahrzeugen).

Das Gefahrenpotenzial wächst zunehmend: Nach Angaben des Marktforschungsunternehmens Gartner waren im Jahr 2017 8,3 Mrd. vernetzte Geräte im Gebrauch; 31 % mehr als im Vorjahr. Im Jahr 2020, so Schätzungen, werden es bereits 25 Mrd. Geräte (Maschinen, Fahrzeuge etc.) sein. In dieser Zahl seien Smartphones, Tablets und Computer nicht berücksichtigt. Der Prognose zufolge entfallen 5,2 Mrd. vernetzte Geräte auf Verbraucher und 3,1 Mrd. Geräte auf Unternehmen.[56]

Die größten Zuwächse beim Endverbraucher erwartet Gartner neben Smart-TVs und digitalen Set-Top-Boxen im Bereich der vernetzten Fahrzeuge (auch i. Z. m. dem autonomen Fahren). Die Möglichkeiten hier seien vielfältig und reichten von automatischen Schadensmeldungen und internetgestützter Navigation bis hin zum Datenaustausch mit Dritten wie Versicherungen. Bei Unternehmen sieht Gartner die größten Zuwächse im Bereich der smarten Stromzähler und Überwachungskameras.

Gartner erwartet bis 2020 einen Schwarzmarkt von fünf Mrd. Euro für gefälschte Sensoren sowie Videodaten, die Kriminelle nutzen könnten. Mit dem IoT seien Informationen über Geolocation, Temperatur, Luftdruck, Lichtverhältnisse, Anwesen- oder Abwesenheit von Menschen, Identitäten der Menschen, Veränderungen in der Umgebung usw. verfügbar.

---

[53] **Https://www.heise.de/security/meldung/Satori-Botnetz-hat-es-auf-Ethereum-Miner-abgesehen-3946840.html.**
[54] **Https://www.heise.de/security/meldung/Hide-n-Seek-IoT-Botnetz-mit-Spionage-Skills-3950938.html**.
[55] **Https://www.heise.de/security/meldung/OMG-Botnet-macht-aus-IoT-Geraeten-Proxys-3982037.html.**
[56] **Https://www.gartner.com/newsroom/id/3598917.**

5.3 INDUSTRIE 4.0

Mit einer zunehmenden Vernetzung von Maschinen und Geräten sowie einer steigenden Tendenz von elektronischen und webbasierten Steuerungsprozessen steigt auch das Bedrohungspotenzial in diesem Bereich. Unternehmen werden abhängiger von einer funktionierenden Informationstechnik und dürften demzufolge auch weiterhin im Fokus von Cyberkriminellen bleiben.

Da Angriffe auf die IT-Infrastruktur von Unternehmen mittlerweile nicht mehr alleine zur Störung der Kommunikation führen, sondern vielmehr die Gefahr eines kompletten Produktionsstillstands beinhalten, dürften auch die mit den Cyber-Angriffen in diesem Bereich verbundenen Schäden als ansteigend prognostiziert werden. Generell dürfte bei der geschilderten Lageentwicklung von einer weiteren Zunahme der Angriffe auf Unternehmen mittels Malware ausgegangen werden.

5.4 KÜNSTLICHE INTELLIGENZ

Die Automatisierung intelligenten Verhaltens und das Maschinenlernen sowie ihre kommerzielle Nutzung gewinnen weiterhin an Bedeutung. Diese Entwicklungen werden auch von Cyberkriminellen beobachtet. Die wurmartige Verbreitung von Malware ist ein Indiz dafür, dass malwarebasierte Cyber-Angriffe zunehmend professioneller ausgeführt werden. Durch die Integration intelligenter und lernender Schwachstellenscanner wird die selbstständige, wurmartige Verbreitung von Malware zusätzlich gefördert.

Vorhersagen hinsichtlich technischer Neuerungen und ihrer Missbrauchspotenziale sind aus polizeilicher Sicht grundsätzlich zurückhaltend zu bewerten. Dennoch sollte in 2018 aufgrund der konkreten Erfahrungswerte aus den Vorjahren von einer Fortführung des oben beschriebenen Trends der zunehmenden Professionalisierung von Cyber-Angriffen ausgegangen werden.

Verstärkt wird dies dadurch, dass das Themenfeld Künstliche Intelligenz auch nach Ansicht des G4C mehr Anwendungsmöglichkeiten für Cyber-Angriffe als für die Cyber-Abwehr eröffnet.

6 Gesamtbewertung und Ausblick

Die Fallzahlen im Bereich Cybercrime stiegen im Jahr 2017 moderat an. Schätzungen zum Dunkelfeld und aktuelle Forschungsergebnisse unterstreichen das hohe Gefährdungs- und Schadenspotenzial von Cybercrime. Die zunehmende Bedeutung der IT für Unternehmen, Behörden und für den privaten Bereich steigert die Manipulations- und Angriffsmöglichkeiten. Aktuelle Technologietrends eröffnen neue Tatgelegenheiten und dürften die Bedrohungslage weiter verschärfen.

Weiter steigende Quantität und Qualität von Cyber-Angriffen.

Polizeiliche Ermittlungsergebnisse deuten zudem darauf hin, dass sich Täter im Bereich Cybercrime zunehmend professionalisieren, indem sie flexibel auf aktuelle technische Rahmenbedingungen reagieren. Cybercrime-Täter begehen heute nicht mehr ausschließlich Straftaten im digitalen Raum, sondern bieten auch die zur Begehung von Straftaten erforderliche Schadsoftware oder komplette technische Infrastrukturen in der im Internet bestehenden kriminellen Schattenwirtschaft an. Diese Werkzeuge eröffnen aufgrund ihrer einfachen Handhabung auch Tätern ohne fundierte IT-Spezialkenntnisse die Möglichkeit, Straftaten mittels des Internets zu begehen.
Es werden daher zunehmend auch Kriminelle ohne spezifische Fachkenntnisse in die Lage versetzt, sich das für eine Tatbegehung erforderliche Know-how anzueignen und entsprechende Tools käuflich zu erwerben. Das Spektrum potenzieller Täter weitet sich dementsprechend aus. Daher ist generell eine steigende Quantität und Qualität von Cyber-Angriffen zu erwarten.

Die vermeintliche Anonymität, die das Darknet jedem Nutzer bieten kann, macht diesen Bereich des Internets für Kriminelle besonders attraktiv. Dies gilt auch für Gruppierungen der Organisierten Kriminalität. Generell kann ein arbeitsteiliges Zusammenwirken von Cyber-Kriminellen bei der Tatbegehung festgestellt werden. Für eine erfolgreiche Bekämpfung von Cybercrime sollte daher der Aspekt einer möglichen organisierten Tatbegehung im Fokus der Strafverfolgungsbehörden stehen.

Schadensausmaß und Strafandrohung stehen in einem Ungleichgewicht.

Im Bereich Cybercrime wurden Deliktsfelder identifiziert, in welchen Schadensausmaß und Strafandrohung in einem Ungleichgewicht zu stehen scheinen. Dies betrifft beispielsweise den Betrieb von illegalen Verkaufsplattformen der Underground Economy oder auch den Aufbau und Betrieb von Botnetzen, z. B. für die Durchführung von DDoS-Angriffen z. N. von Unternehmen oder Kritischen Infrastrukturen. Auf internationaler Ebene besteht u. a. Handlungsbedarf zur Schaffung eines abgestimmten Rechtsrahmens für die Erhebung von elektronischen Beweismitteln bei Internet-Service-Providern, die oftmals im Ausland ansässig sind und Daten in weiteren Staaten speichern. Da sich der Datenstandort aufgrund von Cloud-Algorithmen ständig ändern kann, können Rechtshilfemaßnahmen zur Erhebung beweisrelevanter Daten nicht immer zielgerichtet durchgeführt werden.

Der engen, auch institutionellen Kooperation zwischen den Sicherheitsbehörden und der Wirtschaft – ein weiteres Kernelement einer erfolgreichen Bekämpfung von Cybercrime – kommt eine besondere Bedeutung zu. Eine ganzheitliche Prävention und Bekämpfung von Cybercrime im nationalen (z. B. Gemeinsames Cyber-Abwehrzentrum) und internationalen Kontext (z. B. Europol, Interpol) ist auch deshalb unentbehrlich, da es sich bei Cybercrime in der weit überwiegenden Zahl der Fälle um transnationale Kriminalität handelt.

Wiederholte Datendiebstähle großen Ausmaßes und die tägliche Betroffenheit jedes einzelnen Anwenders, z. B. durch Spam-Mails, bergen die Gefahr nachlassender Sensibilität für zwingend notwendige eigenverantwortliche Präventivmaßnahmen zum Selbstschutz. Dabei rücken mobile Endgeräte, deren Schutz von den Nutzern oftmals vernachlässigt wird, besonders in den Fokus.
Die derzeitigen Entwicklungen im Bereich der synthetischen Abbildungen von Stimmen oder Personen lassen ein hohes Potenzial bei der missbräuchlichen Nutzung dieser Technologien z. B. im Zusammenhang mit der Online-Legitimation oder der stimmgesteuerten Manipulation von Smart Home prognostizieren. Aus den genannten Gründen müssen die Nutzer von Smartphones, Tablets und Smart Home-Technologien weiter sensibilisiert werden.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Juli 2018

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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