Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2016

Cybercrime-Straftaten in Deutschland

82.649 Fälle von Cybercrime im engeren Sinne (+80,5 %*)

253.290 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (+3,6 %)

972 Fälle von Ransomware (+94,4 %)

2.175 Fälle von Phishing im Onlinebanking (-51,4 %)

22 OK-Verfahren im Deliktsbereich Cybercrime (4 % aller OK-Verfahren)

Cybercrime ist transnationale Kriminalität

Zunehmende Professionalisierung der Täter, neue Tatgelegenheiten und Modi Operandi

Vermehrte Nutzung von Anonymisierungsdiensten

* Siehe hierzu Anmerkungen auf S. 5

Inhalt

1 Vorbemerkung

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

Das Bundeslagebild Cybercrime 2016 berichtet schwerpunktmäßig über die polizeilich bekannt gewordenen Entwicklungen von Cybercrime im engeren Sinne im Jahr 2016.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Das sogenannte polizeiliche Hellfeld umfasst alle Straftaten einschließlich der mit Strafe bewehrten Versuche, die polizeilich bearbeitet und an eine Staatsanwaltschaft abgegeben wurden. Aus den geänderten Erfassungsmodalitäten für die Delikte Computerbetrug und die missbräuchliche Nutzung von Telekommunikationsdiensten resultiert eine eingeschränkte Vergleichbarkeit der Zahlen des Jahres 2016 mit denen des Vorjahres.

In Anbetracht der überdurchschnittlich großen Anzahl von Cybercrime-Straftaten, die bei der Polizei nicht zur Anzeige gebracht werden (sogenanntes Dunkelfeld), werden zur umfassenden Einschätzung des Gefahrenpotenzials von Cybercrime auch nichtpolizeiliche Informationsquellen, z. B. Studien von Forschungseinrichtungen oder von behördlichen Einrichtungen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch von privaten Verbänden und Firmen, wie z. B. Antivirensoftware-Herstellern und IT-Sicherheitsdienstleistern, in dieses Lagebild einbezogen. Diese ergänzen das polizeiliche Hellfeld und tragen maßgeblich zu einer ganzheitlichen Lagebewertung bei.

Die Aussagen im vorliegenden Lagebild beruhen darüber hinaus auf Erkenntnissen aus dem kriminalpolizeilichen Informationsaustausch sowie anderen polizeilichen Quellen.

2 Darstellung und Bewertung der Kriminalitätslage

2.1 Statistische Erhebungen zu Cybercrime

2.1.1 Polizeiliche Kriminalstatistik (PKS)

Erfassungsmodalitäten und Dunkelfeld

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

Bis einschließlich 2013 erfasste die Mehrzahl der Länder Cybercrime-Delikte mit einem Schadensereignis in Deutschland (beispielsweise mit Schadsoftware befallener Rechner oder Betrugsopfer in Deutschland), auch wenn unbekannt war, ob sich die ursächliche kriminelle Handlung im In- oder Ausland ereignet hatte. Seit dem Jahr 2014 werden Delikte der Cybercrime bundeseinheitlich nur noch in der PKS erfasst, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen.

Zudem wird eine Tathandlung unabhängig von der Anzahl der Opfer nur einmal erfasst, wie beispielsweise im Fall der Softwaremanipulation auf ca. 1,2 Mio. DSL-Routern eines deutschen Internetproviders durch Malware im November 2016. Trotz einer siebenstelligen Anzahl von Opfern wird dieser Fall in der PKS als ein Fall der Computersabotage abgebildet.

Die Anzahl der tatsächlich begangenen Straftaten, die nicht polizeilich bekannt und erfasst werden, dürfte um ein Vielfaches höher liegen. Realistische Einschätzungen bzw. Hochrechnungen des Dunkelfelds sind jedoch nicht möglich.

Abgesehen von den Richtlinien gibt es für eine Nichterfassung von Straftaten in der PKS verschiedene Ursachen, u. a.:

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

- die betroffenen Personen erkennen nicht, dass sie Opfer 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),

- Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC),

- 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 Lösegeldes keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.

Eine Kenntnis von diesen Straftaten, auch der Versuche, ist für die Strafverfolgungsbehörden im Deliktsbereich Cybercrime von zentraler Bedeutung, da beispielsweise eine Analyse durchgeführter Angriffe Ansätze für eine effektive Bekämpfung eröffnet. Durch eine solche Analyse lassen sich nicht nur Angriffsvektoren (Angriffsweg/Angriffstechnik) und mögliche Tatzusammenhänge aufdecken, sie bietet auch die Möglichkeit, Ermittlungsansätze abzuleiten sowie insbesondere auch Präventionsmaßnahmen wie beispielsweise Patches[01] für betroffene Systeme oder Sicherheitshinweise für Nutzer zu entwickeln. Des Weiteren können Strafverfolgungsbehörden so schneller und zielgerichteter auf neue Entwicklungen reagieren.

Einzelne relevante Phänomene, wie z. B. Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch mit sogenannter Ransomware[02], werden in der PKS nicht unter dem Begriff Cybercrime im engeren Sinne, sondern gemäß PKS-Richtlinien unter den PKS-Schlüsseln der schwerwiegenderen bzw. speziellen Tat, z. B. der Erpressung, erfasst. Insofern finden diese Phänomene keine statistische Berücksichtigung im vorliegenden Lagebild. Derartige Fallkonstellationen sind lediglich in den Zahlen zum Tatmittel Internet enthalten.

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 Fallzahlen basiert, die im Rahmen von polizeilichen Ermittlungen erhoben wurden. Damit liefert sie eine qualitativ hochwertige Datenbasis trendprägender Straftaten für das Spektrum und die Entwicklung der in Deutschland begangenen Cybercrime-Delikte.

Cybercrime im engeren Sinne umfasst folgende Delikte:

Computerbetrug als Cybercrime im engeren Sinne; dieses Delikt wird seit 01.01.2016 in folgende Betrugsarten aufgeschlüsselt:

- 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)
- Betrügerisches Erlangen von Kfz 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

Das **Ausspähen und Abfangen von Daten** (§§ 202a, 202b, 202c StGB) umfasst den „Diebstahl“ digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden in der Regel als Handelsware in der „Underground Economy“[03] 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.

01 Ein Patch („Flicken“, „bugfix“) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen, Fehler korrigieren oder andere Verbesserungen integrieren.

02 Das Einbringen einer spezifischen Malware (Schadsoftware) bewirkt, dass der berechtigte Nutzer eines IT-Systems (z. B. Computer) dieses ganz oder teilweise nicht mehr nutzen und/oder auf die darauf gespeicherten Daten nicht mehr zugreifen kann. Für die (vermeintliche) Freigabe des IT-Systems oder der Daten wird ein Lösegeld (Englisch: ransom) gefordert.

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

Der Straftatbestand der **Fälschung beweiserheblicher Daten bzw. der Täuschung im Rechtsverkehr** (§§ 269, 270 StGB) erfasst 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. Mit überzeugenden Legenden soll das Opfer 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 dem Delikt **Datenveränderung/Computersabotage** (§§ 303a, 303b StGB) handelt es sich um eine Art digitale „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[04]), ebenso fällt darunter die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojanische Pferde, Viren, Würmer usw.).

Bei der **missbräuchlichen Nutzung von Telekommunikationsdiensten** handelt es sich um 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.

Fallzahlen

Die Zahl der als Cybercrime im engeren Sinne in der PKS erfassten Straftaten ist im Jahr 2016 gegenüber dem Vorjahr um 80,5 % auf 82.649 Straftaten gestiegen (2015: 45.793); die Aufklärungsquote lag bei 38,7 % (2015: 32,8 %).

Die Fälle von Computerbetrug haben um 148,8 % zugenommen und bilden fast drei Viertel aller Cybercrime-Straftaten (71 %)[05].

Der starke Anstieg im Bereich des Computerbetrugs dürfte insbesondere darauf zurückzuführen sein, dass Delikte, die in den Vorjahren noch als (allgemeiner) Betrug, jetzt wegen der eindeutigen Zuordnungsmöglichkeiten als Computerbetrug erfasst wurden. Insofern ist davon auszugehen, dass neben einem tatsächlichen Anstieg der Kriminalität teilweise eine Verschiebung der Fallzahlen vom klassischen Betrug hin zum Computerbetrug stattgefunden hat.

Die Fallzahlen zur missbräuchlichen Nutzung von Telekommunikationsdiensten gem. § 263a StGB sind um 84,1 % gesunken.

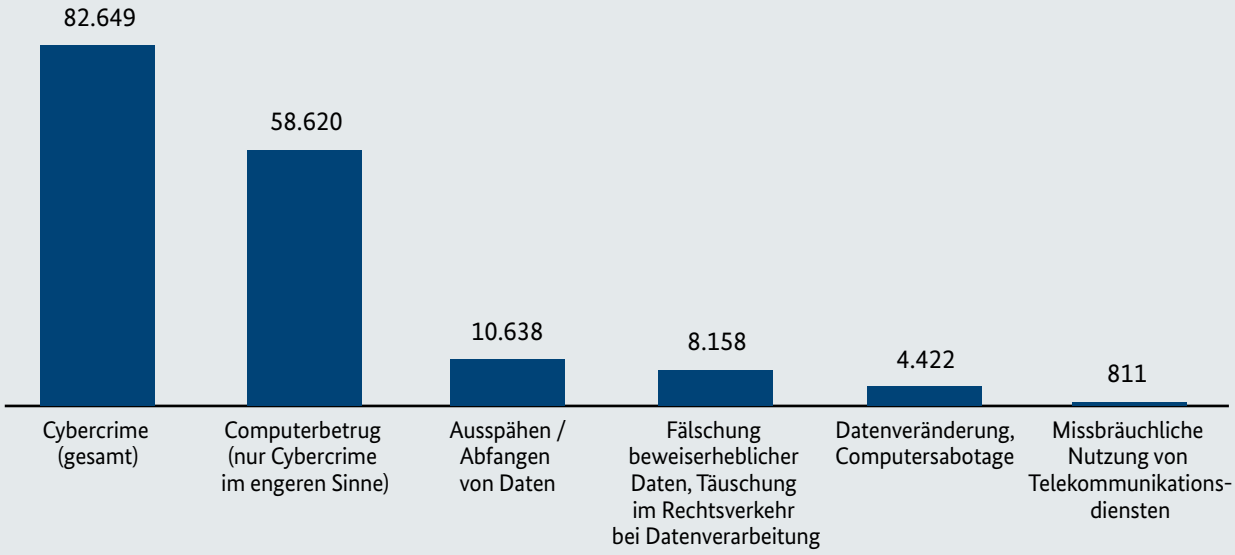
In diesem Zusammenhang ist zu berücksichtigen, dass seit Januar 2016 der Schlüsseltext der Straftatenschlüsselzahl 517 900 für den „Betrug mit Zugangsberechtigung zu Kommunikationsdiensten" in „Missbräuchliche Nutzung von Telekommunikationsdiensten" geändert worden ist. Zudem wurde die Erfassung auf Straftaten gem. § 263a StGB beschränkt, weil aufgrund einer weit auslegbaren Formulierung der Klartextbezeichnung des Erfassungsschlüssels eine im Ländervergleich uneinheitliche Erfassung erfolgte. War unter diesem Straftatenschlüssel ursprünglich ausschließlich eine Abbildung von Fällen der missbräuchlichen Nut-

04 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 sogenanntes Botnetz bilden.

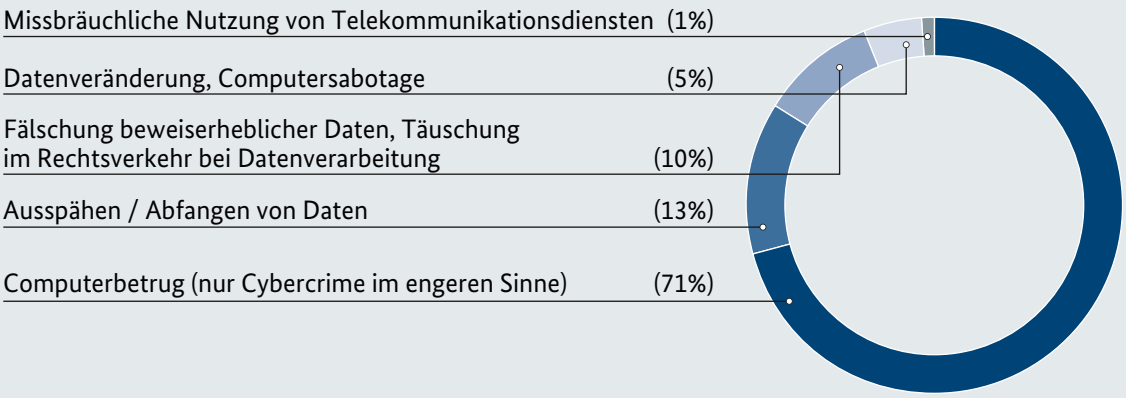
05 Es erfolgt seit Januar 2016 zur differenzierteren Abbildung eine Aufschlüsselung der Computerbetrugsarten, die zuvor als „sonstiger Computerbetrug" nach § 263a StGB (PKS-Schlüsselnummer 517 500) erfasst worden waren: Sonstiger Computerbetrug gem. § 263 Abs. 1 und 2 (PKS-Schlüssel 517 510) sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB (PKS-Schlüssel 517 520), betrügerisches Erlangen von Kfz gem. § 263a StGB (PKS-Schlüssel 511 120), weitere Arten des Kreditbetruges gem. § 263a StGB (PKS-Schlüssel 512 212), Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB (PKS-Schlüssel 516 520), Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB (PKS-Schlüssel 516 920), Leistungskreditbetrug gem. § 263a StGB (PKS-Schlüssel 517 220), Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB (PKS-Schlüssel 518 112), Überweisungsbetrug gem. § 263a StGB (PKS-Schlüssel 518 302).

zung von Telekommunikationsdiensten intendiert, wurden mit zunehmender Bedeutung des Internets im Wirtschaftsleben tatsächlich darunter auch viele andere Betrugsdelikte erfasst, bei denen Kommunikationsdienste zwar eine Rolle spielten, deren Nutzung alleine aber keine strafbare Handlung begründete und mithin ein anderer Erfassungsschlüssel einschlägig gewesen wäre.

Cybercrime im engeren Sinne (2016)



Cybercrime im engeren Sinne - prozentuale Verteilung (2016)



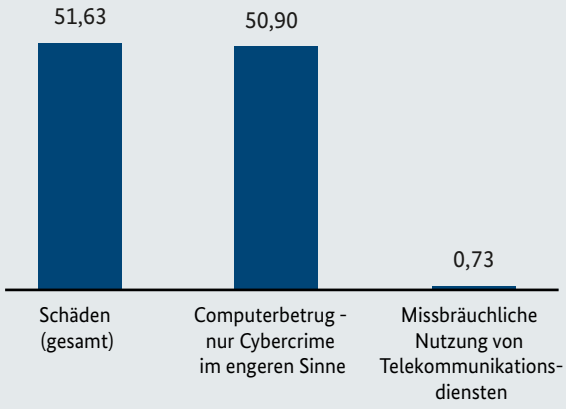
Schäden

Schäden im Deliktsbereich Cybercrime werden in polizeilichen Statistiken ausschließlich für Fälle des Computerbetrugs als Cybercrime im engeren Sinne und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen. Die für 2016 ausgewiesene Gesamtschadenssumme betrug 51,63 Mio. Euro. Vom erfassten Gesamtschaden entfielen rund 50,9 Mio. Euro (2015: 40,51 Mio. Euro) auf den Bereich Computerbetrug und rund 0,73 Mio. Euro (2015: 4,6 Mio. Euro) auf die missbräuchliche Nutzung von Kommunikationsdiensten.[06]

Da lediglich zu den Deliktsbereichen des § 263a StGB eine statistische Schadenserfassung erfolgt, sind keine belastbaren statistischen Aussagen zum tatsächlichen monetären (Gesamt-) Schaden durch Cybercrime möglich.

Oft sind finanzielle Schäden eines erfolgreichen Cyber-Angriffes nicht gänzlich bekannt oder können nicht beziffert werden. Reputationsverluste oder Imageschäden lassen sich in finanzieller Hinsicht nicht darstellen. Hinzu kommt, dass je nach Ausgestaltung des Angriffs oft nicht nur ein einzelnes System für einen bestimmten Zeitraum ausfällt, sondern teilweise gesamte Netzwerke lahmgelegt werden. Zur Darstellung des tatsächlichen Schadensausmaßes müssen demnach verschiedene Faktoren berücksichtigt werden.

Schäden in Mio. Euro (2016)



Tatmittel Internet

Die Sonderkennung „Tatmittel Internet“ wird verwendet, wenn das Internet im Hinblick auf die Tatverwirklichung eine wesentliche Rolle spielt, z. B. bei Abwicklung von Geschäften über das Internet bei Online-Versandhäusern. Die Sonderkennung wird somit nicht verwendet, wenn z. B. im Vorfeld der eigentlichen Tat bloße Kontakte zwischen Täter und Opfer über das Internet stattfanden.

Im Jahr 2016 wurden in der PKS insgesamt 253.290 Straftaten erfasst, bei denen das Internet als Tatmittel genutzt worden ist. Dies entspricht einer Steigerung von 3,6 % gegenüber dem Vorjahr (2015: 244.528 Fälle).

Überwiegend handelte es sich bei den mittels des Tatmittels Internet begangenen Straftaten um Betrugsdelikte (Anteil: 183.529 Fälle, 72,5 %), darunter vor allem Fälle von Waren- und Warenkreditbetrug (Anteil: 123.013 Fälle, 48,6 %), bei denen Täter über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder in minderwertiger Qualität lieferten bzw. Täter die Waren bestellten und nicht bezahlten.

Das Internet wurde zunehmend auch als Tatmittel beim Rauschgifthandel (2016: 2.048 Fälle), beim Waffenhandel bzw. bei Verstößen gegen das Waffengesetz (2016: 253 Fälle) und gegen das Kriegswaffenkontrollgesetz (2016: 15 Fälle) genutzt.

06 Aufgrund geänderter Erfassungsmodalitäten sind die Zahlen des Jahres 2016 nur eingeschränkt mit denen des Vorjahres vergleichbar.

Fallbeispiel Tatmittel Internet:

Im April 2016 erfolgte die Festnahme mehrerer Täter, die in verschiedenen deutschen Städten ansässig waren und deren Gruppierung seit mehreren Jahren über ein deutschsprachiges Forum sowie über einen eigenen Webshop Rauschgift und Medikamente vertrieben hatte. Der von den Tätern betriebene Webshop war im Clearnet[07] sowie im Darknet[08] erreichbar. Teilweise im Kilogrammbereich wurden u. a. Kokain und synthetische Drogen wie Ecstasy verkauft. Die Bezahlung des Rauschgifts erfolgt mittels digitaler Währungen. Die Täter verfügten über einen internationalen Kundenstamm und machten Umsätze in Millionenhöhe.

Kurzbewertung:
Das Fallbeispiel zeigt die enormen Gewinnspannen bei Straftaten, die mittels Internet begangen werden. Für Kriminelle ergeben sich umfangreiche Tatgelegenheiten. Ein persönlicher Kundenkontakt ist häufig nicht erforderlich, was die Hemmschwelle für die Täter weiter senkt. Darüber hinaus erscheint die Nutzung des Internets durch eine vermeintliche Anonymität für den Anwender attraktiv.

2.1.2 Externe Quellen

Eine ganzheitliche Betrachtung und Bewertung der Lage ist auf der Grundlage von rein polizeilichen Daten nicht möglich. Daher müssen hier verstärkt Feststellungen und Lageprodukte externer Kooperationspartner aus Forschung, Privatwirtschaft und benachbarten Behörden einbezogen werden.

Eine im Oktober 2016 vom Digitalverband Bitkom in Auftrag gegebene repräsentative Umfrage unter 1.017 Internetnutzern kommt zu dem Ergebnis, dass nahezu jeder zweite Internetnutzer (47 %) in Deutschland innerhalb von 12 Monaten Opfer von Cybercrime geworden ist.[09]

Knapp die Hälfte der Betroffenen (45 %) hat nach eigenen Angaben infolge der Angriffe einen finanziellen Schaden erlitten, weil zum Beispiel Hard- und Software ersetzt werden musste, Leistungen nicht erbracht oder illegale Transaktionen durchgeführt wurden.

Lediglich 18 % von mittels Ransomware erpressten Unternehmen stellten laut einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cyber-Sicherheit zur Betroffenheit der deutschen Wirtschaft durch Ransomware eine Strafanzeige.[10]

Jedes fünfte Unternehmen wurde im Jahr 2016 Opfer eines erfolgreichen Cyberangriffs, so das Ergebnis einer Studie der Wirtschaftsprüfungs- und Beratungsgesellschaft Pricewaterhouse Coopers (PwC) unter 400 Firmen mit bis zu 1.000 Mitarbeitern. 2015 sei es noch jeder zehnte Betrieb gewesen. Hauptangriffsziele seien die Systemverfügbarkeit, gefolgt von Mitarbeiter- und Systemzugangsdaten. Trotz verschärfter Bedrohungslage reagierten die Firmen nur zögerlich. Die IT-Budgets seien zuletzt sogar gesunken.[11]

07 Als Clearnet wird das weitläufig bekannte Internet, welches mit normalen Browserprogrammen bedienbar und durch Suchmaschinen wie Google oder Yahoo einfach und intuitiv handhabbar ist, bezeichnet.

08 Webseiten im Darknet werden nicht von den gängigen Internet-Suchmaschinen indiziert und können nicht über konventionelle Internettools (Internet-Browser) erreicht werden.

09 https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html.

10 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ransomware-umfrage-2016-04.pdf%3bjsessionid=95F47CAD73CE017CF1040BC377F3AC03.2_cid091?__blob=publicationFile&v=4.

11 PwC-Studie: „Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand“ https://www.pwc.de/de/mittelstand/informationssicherheit-im-deutschen-mittelstand.html.

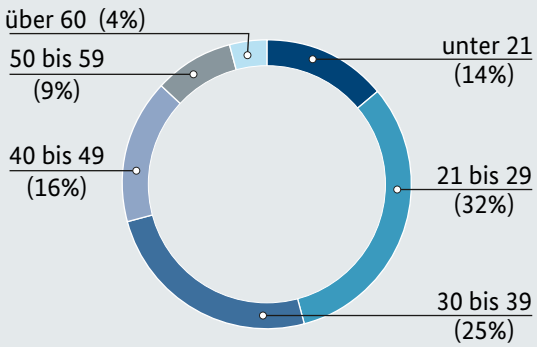
2.2 Täter

Cybercrime-Delikte wurden vornehmlich von Männern begangen. Von 20.920 im Jahr 2016 in der PKS registrierten Tatverdächtigen waren mit 30,3 % nur knapp ein Drittel Frauen.

Die am stärksten vertretene Altersgruppe blieben die 21 bis 29-Jährigen mit 31,9 % (6.664 festgestellte Tatverdächtige), danach folgten die 30 bis 39-Jährigen mit 25,4 % (5.321 festgestellte Tatverdächtige), und schließlich die Gruppe der 40 bis 49-Jährigen mit 16,2 % (3.394 festgestellte Tatverdächtige). Der Anteil der unter 21-Jährigen lag lediglich bei 13,99 % (2.926 festgestellte Tatverdächtige).
Mehr als die Hälfte (54,2 %) der registrierten Delikte der Cybercrime im engeren Sinne wurde somit von über 30-Jährigen begangen.
Insgesamt hatten 76 % der festgestellten 20.920 Tatverdächtigen die deutsche Staatsangehörigkeit, 5.024 Tatverdächtige waren Nichtdeutsche, wobei keine Nationalität signifikant in Erscheinung trat.

Das Täterspektrum reichte vom Einzeltäter bis hin zu international organisierten Tätergruppierungen. Gemeinsam agierende Täter arbeiteten im Bereich Cybercrime nur selten in hierarchischen Strukturen.

Altersstruktur der Tatverdächtigen (2016)



Sie kannten sich häufig gar nicht persönlich und nutzten auch bei arbeitsteiliger Kooperation die Anonymität des Internets.
Der überwiegende Teil der Cyberkriminellen handelte aus finanzieller Motivation.

Die Täterseite reagierte flexibel und schnell auf neue technische Entwicklungen und passte ihr Verhalten entsprechend an. Dienste, die nicht selbst erbracht werden konnten, wurden von anderen hinzugekauft (Stichwort: Cybercrime-as-a-Service).

2.3 Organisierte Kriminalität

Cybercrime ist auch im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität von Bedeutung. In den Jahren 2015 und 2016 wurden jeweils 22 OK-Gruppierungen im Kriminalitätsbereich Cybercrime erfasst. Gemessen an der Gesamtzahl der im Jahr 2016 registrierten OK-Gruppierungen (563) bewegte sich der Anteil der im Bereich Cybercrime aktiven OK-Gruppierungen zwar immer noch auf einem relativ niedrigen Niveau, über mehrere Jahre betrachtet ist die Tendenz jedoch steigend. 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.

Als Tatmittel wurde das Internet 2016 in 54 (9,6 %) der 2016 in Deutschland geführten OK-Verfahren genutzt. Damit ist der Anteil einschlägiger Fälle gegenüber dem Vorjahr um 6,1 Prozentpunkte gesunken (2015: 89 Verfahren, 15,7 % der OK-Verfahren).

2.4 Digitale Währungen

Sogenannte Digitale Währungen wie z. B. Bitcoin (BTC), Litecoin oder Ethereum, sind virtuelle Geldeinheiten deren Herstellung und Verwendung auf mathematischen Berechnungen und kryptografischen Verfahren beruhen . Die Nutzung einer digitalen Währung erfordert jedoch zumeist lediglich die Installation einer „Wallet"-Software. Die Verwendung digitaler Währungen ist nicht illegal. Erwerb und Veräußerung, also die Umwandlung von/in gesetztliche Zahlungsmittel, sind z.B. auf zahlreichen Online-Börsen möglich. Darüber hinaus kann bereits in zahlreichen Online-Shops sowie einigen Geschäften und Cafés mit BTC bezahlt werden. BTC ist die aktuell am stärksten verbreitete digitale Währung. Aktuell entspricht 1 BTC ca. 2.250 Euro (Stand 3.7.2017).

Virtuelle Währungen existieren rein digital und werden mittels kryptografisch abgesicherter Protokolle direkt zwischen den Nutzern ohne Einbindung von Notenbanken oder Kreditinstituten gehandelt. Damit sind sie staatlichen Eingriffsmöglichkeiten weitgehend entzogen. Transaktionen laufen anonym ab, solange Quell- und Zieladressen keinem Besitzer zugeordnet werden können. Digitale Währungen stellen somit ein attraktives digitales Zahlungsmittel für Kriminelle dar. Verwendung finden sie in fast allen Deliktsbereichen, besonders häufig bei Cybercrime-Delikten, Erpressung und Betrug mit Tatmittel Internet. Eine besondere Gefahr besteht darin, dass digitale Währungen insbesondere für Geldwäschehandlungen und Finanzierung terroristischer Aktivitäten missbraucht werden könnten.[12]

2.5 Aktuelle Phänomene

Schadprogramme (Malware)

Schadprogramme führen unerwünschte oder schädliche Funktionen auf einem digitalen System aus.
Die Verbreitung und der Einsatz von Schadprogrammen auf Opfer-Systemen 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).
Laut dem BSI Bericht „Die Lage der IT-Sicherheit in Deutschland 2016" wird die Gesamtzahl der Schadprogrammvarianten für Computersysteme auf über 560 Mio. geschätzt (2015 über 439 Mio.).

12 https://www.interpol.int/News-and-media/News/2017/N2017-002 und https://www.europol.europa.eu/newsroom/news/global-conference-countering-money-laundering-and-misuse-of-digital-currencies.

Digitale Erpressung unter Einsatz sogenannter Ransomware [13]

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[14] missbraucht werden, um der kriminellen Zahlungsaufforderung einen offiziellen Charakter zu verleihen.

b) Sogenannte Krypto-Ransomware, die die Daten auf den infizierten Endsystemen und aktuell auch mittels Netzwerk verbundenen Systemen (Server, Dateiablagen etc.) tat-sächlich verschlüsselt. Diese Variante ist weitaus gefährlicher, da die genutzten Verschlüsselungen nicht in allen Fällen überwunden werden können. Die Zahlung des geforderten Lösegeldes führt darüber hinaus häufig nicht zur Entschlüsselung des infizierten Systems.

Digitale Erpressung mittels sogenannter Ransomware ist ein in Deutschland und darüber hinaus weltweit vermehrt 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 der Erpressung gem. § 253 StGB.

Der Einsatz der Ransomware führt zur Verschlüsselung einzelner Daten eines digitalen Systems und in vielen Fällen auch zur Verschlüsselung erreichbarer Netzwerkkomponenten (andere Endgeräte innerhalb eines Firmennetzwerks u. ä.).
In den meisten Fällen fordern die Täter ein Lösegeld vom Opfer, das in Form von digitaler Währung zu zahlen ist. Nach Zahlung der geforderten Summe sollen die Opfer einen Freischaltcode erhalten, mit dem sie das blockierte System entsperren und anschließend wieder nutzen können.

Seit Dezember 2015 beobachtet das BSI große Spam-Wellen, über die massenhaft Ransomware verteilt wird. Gegenüber Oktober 2015 wurde im Februar 2016 mehr als zehn Mal so häufig Ransomware durch Virenschutzprogramme in Deutschland detektiert.[15] Europol stellt in seinem Cybercrime-Lagebericht 2016 fest, dass Ransomware zwischenzeitlich alle anderen Arten von Malware (inklusive Bankingtrojaner) eingeholt hat.[16]

Infizierte Systeme werden oftmals vollverschlüsselt 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 Geschäftsbetriebes.

Laut BSI verfügen mittlerweile mehr als 95 % der Ransomware über Verschlüsselungsfunktionen.[17] Einfache Sperrbildschirme im Desktop-Bereich ohne das Verschlüsseln der Festplatten wurden im Jahr 2016 weiterhin als Modus Operandi festgestellt.

Im Rahmen einer im April 2016 durchgeführten anonymen Umfrage des BSI bei deutschen Wirtschaftsunternehmen zu ihrer Betroffenheit durch Ransomware wurde festgestellt, dass nahezu ein Drittel (32 %) der befragten Institutionen in den vorhergegangenen sechs Monaten von Ransomware betroffen war.

13 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.

14 Bekannte Beispiele sind der sogenannte BKA-Trojaner und der GVU-Trojaner.

15 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html.

16 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

17 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016): Ransomware, Bedrohungslage, Prävention & Reaktion, S. 8.

Entsprechende Schadsoftware oder auch die gesamte „Dienstleistung“ (z. B. im sogenannten Affiliate-Modell[18]) kann z. B. in Foren der Underground Economy erworben werden, so dass kein besonderer IT-Sachverstand zur Durchführung digitaler Erpressungshandlungen erforderlich ist.

Mit Hilfe von im Darknet verfügbaren „Malware-Toolkits“ können sich die Täter Ransomware ohne großen Aufwand selbst zusammenstellen.

Die Anbieter des Toolkit-Dienstes erhalten bei einer erfolgreichen Lösegeldzahlung eine Umsatzbeteiligung, in der Regel in digitaler Währung.

Beim illegalen Geschäftsmodell mit Ransomware hat sich zwischenzeitlich sogar ein Wettbewerb zwischen den Vertreibern etabliert. So werden erfolgreiche Ransomwarevarianten schlichtweg kopiert, wobei die Nachahmerprodukte häufig schlechter kodiert sind und auf weniger professionelle Art und Weise weiterverbreitet werden. Das „Geschäftsmodell Ransomware“ beruht letztlich auf der erfolgenden Entschlüsselung eines Systems nach Zahlung des geforderten Lösegeldes. Andere Straftäter wenden das Modell an, ohne dass sie willens oder in der Lage sind, eine Entschlüsselung vorzunehmen. Weiterhin sabotieren sich Tätergruppierungen gegenseitig, indem Entschlüsselungstools für „rivalisierende“ Varianten im Netz veröffentlicht werden. Es hat sich eine regelrechte Industrie entwickelt.[19]

Für das Jahr 2016 wurden dem BKA im Rahmen des polizeilichen Meldedienstes 972 Fälle von digitaler Erpressung gemeldet, was einem Anstieg um 94,4 % gegenüber dem Vorjahr (500 Fälle) entspricht und den vom BSI und privaten IT-Sicherheitsdienstleistern festgestellten Trend widerspiegelt.

Fallbeispiel Verschlüsselungssoftware

Im Dezember 2016 wurde erstmalig eine Verschlüsselungssoftware festgestellt, die sich innerhalb von wenigen Stunden in Deutschland verbreitete. Hatte das potenzielle Opfer Excel-Dateien, die per E-Mail übersandt wurden, geöffnet, fand es ein offiziell aussehendes Dokument mit der Bitte, die Makro-Funktionen des Tabellenkalkulationsprogramms zu aktivieren. Kam der Nutzer der Bitte nach, fügte das infizierte Dokument mit Hilfe von VBScript zwei EXE-Dateien mit Schadcode zusammen und führte sie aus. Anschließend wurden Dateien verschlüsselt, die Originale gelöscht sowie die System-Partition so manipuliert, dass der PC nicht mehr gestartet werden konnte.

Es zeigte sich, dass die Angriffe fast ausschließlich gegen deutsche Opfer gerichtet waren, da es sich um in deutscher Sprache verfasste angebliche Bewerbungs-E-Mails handelte, die gezielt an Personalabteilungen von Firmen gerichtet waren.

Was die Software besonders gefährlich machte, waren die zu Beginn der Angriffe äußerst niedrigen Erkennungsraten der gängigen Virenscanner. Die Angreifer änderten die Malware-Dateien im Stundentakt, um eine Erkennung der präparierten E-Mails durch die Virenscanner der Opfer zu verhindern.

18 Affiliate beschreibt das Verhältnis zwischen dem Hersteller eines Produktes (beispielsweise Ransomware) und dem Käufer, der das Produkt als Dienstleistung entgegennimmt. Durch den Hersteller wird eine technische Betreuung gewährleistet (wie Updates, Wartung, Nutzung von Servern). Die konkrete Verteilung der Ransomware liegt im Zuständigkeitsbereich des Kunden.

19 Vgl. https://threatpost.com/petya-sabotages-rival-ransomware-chimera-leaks-decryption-keys/119543/ sowie https://de.securelist.com/analysis/kaspersky-security-bulletin/72252/kaspersky-security-bulletin-2016-story-of-the-year/.

Massenhafte Fernsteuerung von Computern (Botnetze)

Sogenannte Botnetze spielten als zentrale Angriffsressource im Bereich Cybercrime auch im Jahr 2016 eine bedeutende Rolle. Bei Botnetzen handelt es sich um zahlreiche, per Schadcode infizierte Computer, die ohne Wissen ihrer Besitzer über „Command & Control-Server“ (C&C-Server) ferngesteuert werden können.

Wie entstehen Botnetze?

Die Installation der Schadsoftware auf den Opfer-PCs erfolgt für die Besitzer unbemerkt auf verschiedene Art und Weise, sei es durch Öffnung eines infizierten E-Mail-Anhangs oder auch mittels „Drive-by-Infection[20]“.
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. In der Folge hat der Täter durch die zuvor installierte Schadsoftware einen nahezu vollständigen Zugriff auf den infizierten Computer des Opfers.
Weitere Verbreitungskanäle sind das Usenet[21] und Tauschbörsen/P2P (Peer to Peer)-Netze[22], in denen die Schadsoftware meist als Video- oder Sounddatei getarnt zum Download angeboten wird.

Botnetze und ihre Kapazitäten sind nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy. Die Betreiber der Botnetze, sogenannte Bot-Herder[23], vermieten Bots, durch die beispielsweise mittels DDoS-Attacken gezielte Angriffe auf Unter-nehmensserver durchgeführt werden, massenweise Spam-Mails versendet werden oder auch gezielte Datendiebstähle erfolgen können.

Valide Angaben zur Gesamtzahl der in Deutschland bzw. weltweit in Botnetzen zusammengeschlossenen Rechner sind kaum möglich.

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) und EUROPOL gehen davon aus, dass Deutschland an der Spitze der Staaten, die Command & Control-Server hosten, steht.

20 Sogenannte Drive-By-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware wie Trojanische Pferde unbemerkt auf dem PC zu installieren.

21 Weltweites, elektronisches Netzwerk, das einen eigenen selbstständigen Dienst des Internets neben dem World Wide Web darstellt. Es entstand lange vor dem World Wide Web. Es stellt fachliche Diskussionsforen aller Art in reiner Textform zur Verfügung, an denen grundsätzlich jeder teilnehmen kann (sogenannte Newsgroups).

22 Als „Peer-to-Peer“ (oft auch „P2P“ abgekürzt) wird ein Informationsaustausch bezeichnet, der zwischen gleichberechtigten IT-Systemen („Peers“) durchgeführt wird. Jedes IT-System kann hierbei Dienste anbieten oder nutzen. Über die hierfür aufgebaute Kommunikationsverbindung können sich mehrere IT-Systeme Ressourcen dezentral untereinander teilen. Somit werden die typischen Funktionen eines Servers und eines Clients auf einem IT-System vereint.

23 Herder (englisch) – Hirte.

Fallbeispiel Botnetze:

Anfang Dezember 2016 konnte durch eine zeitgleich erfolgte Beschlagnahme von 39 Servern und mehreren Hunderttausend Domains nach mehr als vier Jahren intensiver Ermittlungsarbeit von Cyber-Experten aus Polizeien und anderen Behörden in 41 Staaten die wohl weltweit größte Infrastruktur zum Betrieb sogenannter Botnetze aufgedeckt und analysiert werden. Dadurch ist Cyberkriminellen allein in Deutschland die Kontrolle über mehr als 50.000 infizierte Computer entzogen worden.

Mindestens seit 2009 haben Täter die weltweit vernetzte Botnetz-Infrastruktur „Avalanche“ für das Versenden von E-Mails, die schadhaften Code enthalten haben, genutzt. In 180 Staaten wurden Opfer festgestellt. Bei „Avalanche“ handelte es sich nach bisheriger Einschätzung um die weltweit größte Infrastruktur zum Betrieb eines Botnetzes.

Allein auf der Führungsebene dieser kriminellen Vereinigung konnten 16 Beschuldigte identifiziert werden. Gegen sieben Tatverdächtige in Deutschland wurden Haftbefehle wegen des Verdachts der Bildung einer kriminellen Vereinigung, des banden- und gewerbsmäßigen Computerbetrugs und anderer Straftaten erlassen.

Die Exekutivmaßnahmen wurden von den deutschen Dienststellen koordiniert und durch Eurojust und Europol zeitgleich in zehn Staaten unterstützt. An den Ermittlungen beteiligt waren neben dem US-amerikanischen Federal Bureau of Investigation (FBI) weitere US-amerikanische sowie europäische und außereuropäische Behörden.

Kurzbewertung:
Die quantitative wie qualitative Ausgestaltung von kriminellen Infrastrukturen erreicht ein immer größeres Ausmaß. Der Fall verdeutlicht die Erforderlichkeit von internationalen Kooperationen im Phänomenbereich Cybercrime, um derartige Infrastrukturen erfolgreich bekämpfen zu können.

Angriffe auf die Verfügbarkeit von Webseiten, Internetdiensten und Netzwerken (DDoS-Angriffe[24])

Eng verknüpft mit der Thematik Botnetze sind die „DDoS-Angriffe“. Die in einem Botnetz zusammengeschlossenen Rechner sind die zentrale Ressource zur Durchführung von DDoS-Angriffen. Ziel dieser ist es, die Verfügbarkeit von Webseiten, einzelner Dienste oder auch von ganzen Netzen in der Regel zu sabotieren.

DDoS-Angriffe gehören zu den am häufigsten beobachteten Sicherheitsvorfällen im Cyber-Raum. Kriminelle haben hieraus entsprechende Geschäftsmodelle entwickelt und vermieten Botnetze verschiedener Größen.

Statistische Daten zu Anzahl und Dauer von DDoS-Angriffen in Deutschland liegen im BKA nicht vor. Das BSI berichtet in seinem Jahresbericht 2016, dass sich die maximale Bandbreite von Einzelangriffen gesteigert hat[25].

Die Nichterreichbarkeiten von Vertriebsportalen wie beispielsweise Online-Shops in Folge eines DDoS-Angriffs kann gerade im wettbewerbsintensiven Marktsegment Internet erhebliche wirtschaftliche Schäden nach sich ziehen. Die Motivlagen der Täterseite reichen von rein monetären Interessen (Erpressung) oder dem Erlangen von Wettbewerbs-

24 Vgl. Fußnote 5.

25 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2016“.

vorteilen über Rache bis hin zu politischen bzw. ideologischen Motiven.

Die durch DDoS-Angriffe verursachten Schäden für den Geschädigten lassen sich schwer errechnen, 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.

Prognose

DDoS-Angriffe, die mittels Mirai-Botnetzen begangen werden, zeichnen sich aufgrund der Nutzung von zahlreichen zusätzlichen Geräten des Internets der Dinge (Internet of Things – IoT) durch rasant steigende Bandbreiten aus. Die erreichbaren Bandbreiten nehmen hier Größenordnungen an, die mittels vormaliger Infektionen von insbesondere Desktop-PCs nicht hätten erreicht werden können. Hierdurch erhöht sich das Gefahrenpotenzial auch für große Internetdienstleister, deren Infrastrukturen vormals Angriffen standhielten.

Es ist davon auszugehen, dass künftig vermehrt die Einbeziehung von Geräten des Internets der Dinge in Botnetze stattfinden wird. Ein Anstieg von Quantität und Qualität von DDoS-Angriffen mittels Miraibasierten und vergleichbaren Botnetzstrukturen ist anzunehmen.[28]

Fallbeispiel DDoS-Angriffe:

Im Oktober 2016 kam es unter Beteiligung des Botnetzes „Mirai“ zu großangelegten DDoS-Angriffen auf einen großen Internetdienstleister, so dass viele Webseiten stundenlang nicht erreichbar waren.

Auch für den Ausfall von DSL-Routern eines großen deutschen Internetproviders im November 2016 zeichnete ein „Mirai“-basiertes Botnetz verantwortlich.

Das Botnetz „Mirai“ nutzt aus, dass Alltagsgegenstände wie Router, Überwachungssysteme, Fernseher oder Kühlschränke mit dem Internet verbunden sind (IoT = Internet of Things). Die Software scannt über das Internet derartige Geräte auf Sicherheitslücken und infiziert diese dann ggf. mittels eines Schadcodes. Das ursprüngliche Bot-Netz „Mirai“ umfasste 2016 rund 500.000 kompromittierte „Internet of Things“-Geräte weltweit, zwischenzeitlich waren bis zu drei Millionen Geräte in das Botnetz eingebunden.[26]

Kurzbewertung:
Anhand des Fallbeispiels wird deutlich, dass Geräte der Internets der Dinge[27] oft Sicherheitslücken aufweisen, da sie vom Endnutzer mangels Konfigurationsmöglichkeiten nicht selbst geschützt werden können und so anfällig für Cybercrime-Straftaten sind.

Auch für IoT-Geräte muss herstellerseitig ein technischer Sicherheitsstandard etabliert werden, um vor Cyber-Angriffen zu schützen. Durch Schnittstellen zum Internet sind IoT-Geräte analog zu Laptops oder Smartphones zahlreichen Angriffsszenarien ausgesetzt.

26 https://www.heise.de/security/meldung/Kriminelle-bieten-Mirai-Botnetz-mit-400-000-IoT-Geraeten-zur-Miete-an-3504584.html.

27 Siehe Gliederungspunkt 3.2 für weitere Erläuterungen.

28 Diese Prognose wird vom German Competence Centre against Cybercrime e.V. (G4C) bestätigt und mitgetragen. Darüber hinaus stellt das G4C den Trend zu sogenannten BrickerBots fest und führt dazu folgendes aus: „Diese Bricker Bots werden für sogenannte PDOS Angriffe verwendet. PDOS steht für Permanent Denial-of-Service, d. h. angegriffene Geräte werden, gemessen am Reparaturaufwand, effektiv zerstört („Bricked“). Die BrickerBots werden zwar sicher einige IoT Geräte eliminieren und Mirai-basierte Botnetze etwas schwächen, aber trotzdem werden auch künftig noch einige IoT-DDoS Attacken zu beobachten sein.“

Angriffe auf Kritische Infrastrukturen (KRITIS)

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden[29].

KRITIS-Betreiber verlassen sich zur Steuerung ihrer Produktionsstätten und Dienstleistungen zunehmend auf moderne Informations- und Kommunikationstechnologien. Grundsätzlich sind KRITIS-Betreiber dabei den gleichen Gefahren ausgesetzt wie alle andere Unternehmen. Das Risiko liegt bei KRITIS-Betreibern jedoch meist auf deutlich höherem Niveau, da Betriebsstörungen schnell zu Ausfällen führen, die schwerwiegende Auswirkungen auf große Teile der Bevölkerung haben können.

Wegen des hohen Schadenspotenzials, sind KRITIS potenzielle Ziele für politisch motivierte Straftäter. Cyber-Vorfälle, von denen sowohl Unternehmen als auch staatliche Stellen wie beispielsweise der Deutsche Bundestag betroffen waren, haben zugenommen. Festgestellte Angriffe auf TV-Sender, Energieversorger und weitere KRITIS-Branchen häuften sich in der Vergangenheit, von einer weiteren Zunahme der Angriffe muss ausgegangen werden.

Typisch für staatlich gesteuerte Cyber-Attacken sind sogenannte APT-Angriffe (Advanced Persistent Threat). Auch Cyber-Vorfälle, von denen sowohl Unternehmen als auch staatliche Stellen wie beispielsweise der Deutsche Bundestag betroffen waren, haben zugenommen.

Auch allgemeinkriminelle Hacker schrecken vor Angriffen auf KRITIS-Unternehmen nicht zurück. Erpressungen mittels DDoS-Attacken und Ransomware fanden in 2016 wiederholt statt. Betroffen waren neben Krankenhäusern u. a. Fernsehanstalten und Energieversorger. Einzukalkulieren ist, dass solche, auch nicht politisch motivierte Angriffe, weiter zunehmen werden.

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.

Digitale Schwarzmärkte - Underground Economy

Illegale Foren oder Marktplätze finden sich sowohl im Clearnet, im Deepweb[30] sowie auch im Darknet. Sie spielen eine weiter zunehmende zentrale Rolle bei der Begehung von Straftaten im Bereich Cybercrime.

Die Foren dienen unverändert hauptsächlich der Kommunikation von Cyberkriminellen, dem Transfer von kriminellem Know-how und dem Austausch über das Ausnutzen von Sicherheitslücken. Darüber hinaus werden die unter „Cybercrime-as-a-Service“ dargestellten Dienstleistungen gehandelt.

Das Angebot auf den kriminellen Marktplätzen erscheint grenzenlos. Es umfasst illegale Drogen, Waffen, Falschgeld, gefälschte Ausweise, gestohlene Kreditkartendaten oder gefälschte Markenartikel. Der Handel mit Kinderpornografie erfolgt in der Regel über eigens dafür geschaffene Plattformen.

29 http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Flyer.pdf.

30 Das Deepweb ist jener Teil des Internet, der nicht durch allgemeine Suchmaschinen auffindbar ist. Inhalte sind beispielsweise Datenbanken, Intranets oder Fachwebseiten.

Die Marktplätze haben teils mehr als 100.000 unter sogenannten Nicknames registrierte Mitglieder und umfassen bis zu einer Million Mitteilungen bzw. Veröffentlichungen.

Zur Bezahlung der gehandelten Waren werden ausschließlich digitale Kryptowährungen[31] akzeptiert, die ein pseudoanonymes Bezahlen ermöglichen. Durch Treuhand-Systeme, die genutzt werden, um die Transaktionen abzuwickeln, sichern sich oftmals die Administratoren der kriminellen Online-Marktplätze einen Teil des Umsatzes vom Verkauf der illegalen Waren.

In den zunehmenden Aktivitäten in der Underground Economy spiegelt sich eine fortschreitende Verlagerung von Straftaten in den virtuellen Raum wider. Ausschlaggebend für diese Entwicklung dürfte nicht nur ein Maximum an Anonymität sein, welches das subjektive Entdeckungsrisiko enorm verringert, sondern auch der Umstand, dass über illegale Online-Marktplätze unzählige potenzielle Kunden weltweit erreichbar werden.

Die Foren und Marktplätze im Darknet stehen jedem Internetnutzer offen, da sie ohne tiefergehende Computerkenntnisse erreichbar sind.

Fallbeispiel Digitale Schwarzmärkte – Underground Economy:

Gegen die Betreiber und Mitglieder von zwei Underground Economy-Foren hat das Bundeskriminalamt seit Ende 2014 ein Ermittlungsverfahren wegen des Verdachts des gewerbsmäßigen Handels mit Betäubungsmitteln, des Ausspähens von Daten, der Datenveränderung, des gewerbsmäßigen Computerbetruges, der Geldwäsche sowie weiterer Straftaten geführt.

Im Verlauf der europaweit geführten Ermittlungen konnten die für die illegalen Marktplätze verantwortlichen Administratoren sowie weitere Mitglieder der Führungs- und Verkäuferebenen identifiziert und schließlich im Februar 2016 festgenommen werden.
Sichtbar wurden die Maßnahmen für die Underground Economy-Szene durch die Platzierung des „Seizure-Banners“.

Die Sicherstellung einer erheblichen Menge von Betäubungsmitteln bestätigte die im Zuge der Ermittlungen gewonnenen Erkenntnisse hinsichtlich einer zunehmenden Verlagerung des Rauschgifthandels ins Internet.

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

31 Alternative Bezeichnungen: virtuelle, alternative oder digitale Währungen, Geld oder Devisen.

Bereitstellung von Software und Dienstleistungen zur Begehung von Straftaten (Cybercrime-as-a-Service)

Das Geschäftsmodell „Cybercrime-as-a-Service“ wird in der kriminellen Szene weiter ausgebaut. Die digitale Underground Economy hält heute ein breites Spektrum von Dienstleistungen zur Durchführung jeder Art von Cybercrime bereit. Das Angebot umfasst z. B.:

- Ransomware (-toolkits),
- Bereitstellung von Botnetzen für verschiedene kriminelle Aktivitäten,
- DDoS-Attacken,
- Malware-Herstellung und -Verteilung,
- Datendiebstahl,
- Verkauf/Angebot sensibler Daten, z. B. Zugangs- oder Zahlungsdaten,
- Vermittlung von Finanz- oder Warenagenten, die die Herkunft der durch Straftaten erlangten Finanzmittel oder Waren gegen Bezahlung verschleiern,
- Kommunikationsplattformen zum Austausch von kriminellem Know-how, wie beispielsweise Foren der Underground Economy,
- „Infection on Demand“ (Verteilung von Schadsoftware auf Anforderung/Abruf),
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität,
- Test-Portale, in denen Cyberkriminelle erworbene oder erstellte Schadsoftware auf Detektierbarkeit durch aktuelle Cyber-Sicherheitsprodukte testen können, um durch Änderungen die Erfolgsaussichten für eine „Verteileroffensive“ zu verbessern,
- sogenannte Dropzones zum Ablegen illegal erlangter Informationen bzw. Waren.

Die Beispiele zeigen, dass interessierte Kriminelle sich auch ohne eigene technische Kenntnisse Zugang zu hochentwickelten illegalen Cyber-Werkzeugen verschaffen können und sich so mit vergleichsweise geringem Aufwand in die Lage versetzen können, zahlreiche Formen von Cyberangriffen auszuführen. Mittlerweile wird – ähnlich wie bei legalen Softwareangeboten – häufig sogar ein „Kundendienst“ angeboten. Dieser Support beinhaltet beispielsweise Updates für Schadsoftware, Beratungsdienste, Anti-Erkennungsmechanismen sowie Hilfeleistung bei technischen Problemen.

Fallbeispiel Cybercrime-as-a-Service:

Im Jahr 2016 wurde in Rheinland-Pfalz ein Ermittlungsverfahren wegen des Ausspähens von Daten gem. § 202a StGB und der Vorbereitung des Ausspähens von Daten gem. § 202c StGB geführt. Der in Deutschland ansässige Beschuldigte bot als Infrastrukturdienstleister für Cybercrime mindestens seit 2012 diverse Software national und international zum Kauf an. Diese Schadsoftware wurde vom Beschuldigten entwickelt und versetzt den Käufer/Lizenzinhaber in die Lage, jede beliebige Schadsoftware, z. B. Viren oder Trojaner, speziell zu tarnen. Die Viren und Trojaner bleiben in der Folge von Antivirenprogrammen unerkannt und infizieren dann den Computer des Opfers.

Zudem bot der Beschuldigte gegen Bezahlung einen sogenannten Counter-Anti-Virus-Dienst (CAV) an. Der Nutzer hat hiermit online die Möglichkeit, Schadsoftware mit einer großen Auswahl an Antivirenprogrammen auf deren Unerkennbarkeit testen zu lassen. Als Ergebnis erhält der Nutzer eine Auflistung der Antivirenprogramme, die seine getarnte Datei als Schadsoftware erkennen.

Im Rahmen der Ermittlungen wurden bundesweit im April 2016 über 175 Durchsuchungsbeschlüsse bei 171 Tatverdächtigen vollstreckt.

Zudem konnten ca. 500.000 Muster von Malware festgestellt werden. National und international wurden durch die Ermittlungen 4.785 Kaufvorgänge belegt. Insgesamt wurde die Schadsoftware in 16.000 Fällen benutzt.

Kurzbewertung:
Der Sachverhalt beschreibt nur ein Beispiel vielfältiger Produkte, die auf kriminellen Online-Marktplätzen im Internet angeboten werden. Im Erfolgsfall können hohe kriminelle Erträge erzielt werden. Anbieter gehen dabei oft arbeitsteilig vor und bieten neben der Bereitstellung des Produktes auch weitere Dienste wie Kundensupport oder spezielle Software-Lösungen an. Cybercrime-as-a-Service stellt dabei eine Infrastruktur für die Begehung von Straftaten durch technisch wenig versierte Täter dar und ist Bestandteil der Entwicklungen im Bereich Cybercrime.

Diebstahl digitaler Identitäten und Identitätsmissbrauch

Digitale Identitäten als Ganzes oder zumindest Teile digitaler Identitäten sind ein begehrtes Diebesgut im Cyberspace, sei es, um die erlangten Informationen für kriminelle Zwecke zu missbrauchen oder um sie, meist über illegale Verkaufsplattformen der Underground Economy, zu verkaufen.

Um in den Besitz dieser Informationen zu gelangen, setzen die Täter häufig neben „Trojanischen Pferden“[33] auch andere Methoden ein, wie z. B.:

- Installation von Schadprogrammen über Drive-By-Exploits[34],
- Phishing,
- Einbruch auf Server und Kopieren der Anmeldeinformationen,
- Einsatz von Keyloggern[35] oder Spyware[36].

Die gestohlenen Identitäten werden mittels der eingesetzten Schadsoftware meist automatisch an speziellen Speicherorten im Internet (sogenannte Dropzones) gesammelt, auf welche die Täter bzw. deren Auftraggeber zugreifen können.

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 (Onlinebanking, 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*[32].

32 Bereitstellung von IT-Infrastrukturen, wie z. B. Datenspeicher oder auch fertiger Software, über ein Netzwerk, ohne dass diese auf dem lokalen PC installiert sein müssen.

33 Ein Trojanisches Pferd, oft auch kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Es verbreitet sich nicht selbst, sondern wirbt mit der angeblichen Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen, z. B. könnte ein Trojanisches Pferd einem Angreifer eine versteckte Zugriffsmöglichkeit (sogenannte Hintertür) zum Computer bieten.

34 Sogenannte Drive-By-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware wie Trojanische Pferde unbemerkt auf dem PC zu installieren.

35 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.

36 Wortschöpfung aus Spy (spionieren) und Software. Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, 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.

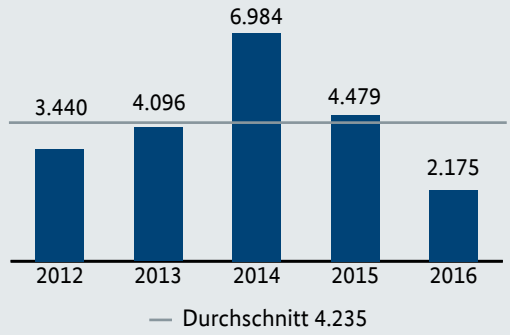
Fallbeispiel Diebstahl digitaler Identitäten bzw. Identitätsmissbrauch:

Hintergrund eines im Zuständigkeitsbereich des LKA NW 2016 geführten Ermittlungsverfahrens war ein durch die Täter begangener Diebstahl von Zugangsdaten eines Online-Shops, der über die Marketplace-Plattform von Amazon Waren anbietet. In kürzester Zeit boten die Täter hochwertige Produkte in diesem Shop zum Kauf an und unterboten mit Dumpingpreisen alle Wettbewerber. Sie setzten dabei auf den Wunsch der Kunden, Schnäppchen zu machen. Der Bestellprozess wurde kurz vor Beendigung abgebrochen und den Käufern dieser Produkte eine E-Mail zugestellt. Abweichend vom üblichen Zahlungsweg des Online-Shops erhielten die Kunden darin Bankdaten (meist von ausländischen Banken), an die sie den Kaufpreis überweisen sollten. Trotz Zahlung erhielten die Kunden die Ware nie.

Phishing im Onlinebanking

Die häufigste Variante des digitalen Identitätsdiebstahls ist neben dem Massendiebstahl von digitalen Daten weiterhin das sogenannte „Phishing im Zusammenhang mit Onlinebanking". Für das Jahr 2016 wurden dem Bundeskriminalamt von den Polizeien der Länder 2.175 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2015 (4.479) bedeutet dies eine Abnahme der Fallzahlen um rund 51 %. Die Zahl der Fälle befindet sich im Jahr 2016 damit auf dem tiefsten Stand seit fünf Jahren und bestätigt die auch von Europol festgestellte rückläufige Tendenz in diesem Phänomenbereich.

Fälle – Phishing im Onlinebanking



Beim Phishing zum Nachteil deutscher Bankkunden werden in der Regel „Trojanische Pferde" eingesetzt, die speziell auf den deutschen Bankensektor ausgerichtet sind und über das technische Potenzial verfügen, sowohl das iTAN- als auch das mTAN-Verfahren mittels sogenannte Echtzeitmanipulation (Man-In-The-Middle-/Man-In-The-Browser-Attacken[37]) erfolgreich anzugreifen.

Die Täter setzen bei Phishing aber nicht nur auf rein technische Lösungen, sondern versuchen mittels des sogenannten Social Engineerings[38] an die notwendigen Kundeninformationen zu gelangen. So werden die mittlerweile weitgehend in Deutschland verwendeten Autorisierungsmechanismen im Onlinebanking, die ein aktives Handeln des Kontoberechtigten erfordern (unter Nutzung eines zweiten Kommunikationskanals[39]), ausgehebelt.

37 Ziel bei einem Man-In-The-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. Bei „Man-In-The-Browser-Attacken" manipuliert die auf dem Rechner mittels eines Trojaners installierte Malware die Kommunikation innerhalb des Webbrowsers, wodurch andere Informationen weitergegeben werden, als der Nutzer eingibt.

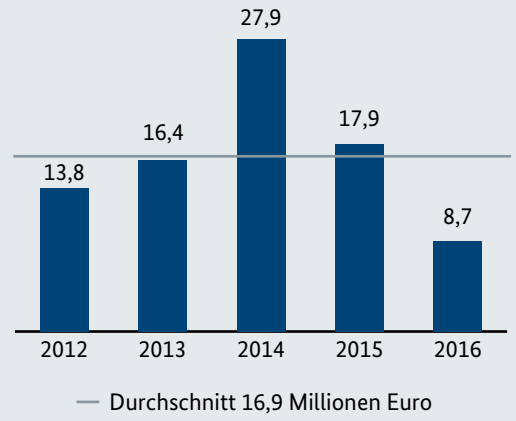
38 Soziale Manipulation – Beeinflussung einer Person zur Preisgabe vertraulicher Informationen. Bei Cyberangriffen mittels Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadcodes auf ihren Systemen 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.

39 Sogenannte „Two-factor authentication".

Bekanntestes Beispiel ist der Versand von E-Mails in vertrauenerweckender Aufmachung, z. B. mit einem bekannten Firmen- oder Behördenlogo, mit der Aufforderung, aus bestimmten Gründen vertrauliche Informationen preiszugeben.

Trotz der 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“ auch im Jahr 2015 rund 4.000 Euro pro Fall. Dies ergibt eine Gesamtschadenssumme in Höhe von 8,7 Mio. Euro für das Jahr 2016. Die Gesamtschadenssumme lag damit jedoch deutlich unter der durchschnittlichen Schadenssumme der vergangenen fünf Jahre (16,9 Mio. Euro).

Schäden – Phishing im Onlinebanking (in Mio. Euro)



Mobile Endgeräte – zunehmend beliebtes Angriffsziel

Mobile Endgeräte wie Smartphones und Tablets verdrängen insbesondere in den privaten Haushalten zunehmend konventionelle Computer und gewinnen kontinuierlich Marktanteile. Gemäß einer repräsentativen Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) nutzten Anfang des Jahres 2016 rund 51 Mio. Bundesbürger (rund drei Viertel der Deutschen ab 14 Jahren, also 74 %) ein Smartphone. 2014 waren es noch rund zwei Drittel (65 %) und 2012 gerade einmal etwas mehr als ein Drittel (36 %). Der Nutzeranteil hat sich damit innerhalb von vier Jahren mehr als verdoppelt.[40]

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 lohnenden Angriffsziel für Kriminelle.

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

40 https://www.bitkom.org/Presse/Presseinformation/Umsatz-mit-Smartphones-knackt-10-Milliarden-Marke.html.

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.

Die zunehmende Bedeutung und Attraktivität mobiler Endgeräte für Cyberkriminelle spiegelt sich insbesondere in einer Zunahme von Malwareentwicklungen im Bereich mobiler Betriebssysteme wider. Die Anzahl der Varianten von Schadsoftware für mobile Plattformen nimmt laut BSI weiter zu. Hauptangriffsziel im Bereich der mobilen Plattformen ist laut BSI nach wie vor fast ausschließlich das Betriebssystem Android[41].

Fallbeispiel Angriff auf Mobile Endgeräte:

In dem Ermittlungsverfahren des LKA NW (siehe Fallbeispiel zum Diebstahl digitaler Identitäten bzw. Identitätsmissbrauch, S. 24) konnten durch die Ermittlungen auch Angriffe auf mobile Endgeräte festgestellt werden. Durch die Ermittlungen wurde deutlich, dass neben dem Diebstahl von persönlichen Daten die Täter durch Phishing auch an Zugangsdaten zum Onlinebanking gelangten. Zur Ausführung von Überweisungen benötigten die Täter noch die notwendigen Transaktionsnummern (TAN).

Die Einführung neuer Sicherheitsvorkehrungen wie mTAN und TAN-Generatoren zur Autorisierung von Finanztransaktionen erschweren den Tätern zwar den Zugriff auf die nur kurzzeitig verwendbaren Transaktionsnummern, die zunehmende Verbreitung von Smartphones und Tablets bietet jedoch neue Angriffsvektoren. Die Täter greifen mobile Endgeräte gezielt mit spezieller Schadsoftware an. Gelingt es den Tätern, Zugriff auf die Konten der Geschädigten zu erhalten sowie deren mobile Endgeräte zu kompromittieren, können mTAN auf Mobilgeräte der Täter umgeleitet und Überweisungen durchgeführt werden.

Kurzbewertung:
Die Möglichkeit der Abwicklung von Bankgeschäften über mobile Endgeräte eröffnet neue Tatgelegenheiten für Cybercrime-Straftaten. Der meist geringe Schutz, das nicht zeitgerechte Schließen von Sicherheitslücken in den Betriebssystemen durch die Hersteller sowie die dauernde Internetverbindung erleichtern den Zugriff durch Kriminelle auf diese Geräte.

41 Mobiles Betriebssystem, das von Google entwickelt worden ist. Android kommt hauptsächlich auf Smartphones und Tablets zum Einsatz. Offiziell ist Android seit dem 21. Oktober 2008 verfügbar.

3 Gefahren- und Schadenspotenzial

Cybercrime verursacht bei Bürgern, Behörden und Wirtschaftsunternehmen hohe materielle und immaterielle Schäden.

Öffentlichkeitswirksame Schlagzeilen zu millionenfachem Datendiebstahl oder Manipulationen von technischen Geräten im sechs- bis siebenstelligen Bereich führen zu einer deutlichen Beeinträchtigung des Sicherheitsgefühls der Bürger. Gemäß einer ARD/ZDF-Onlinestudie ist 2016 die Zahl der Onlinenutzerinnen und -nutzer auf insgesamt 58 Mio. gestiegen. Dies entspricht einem Anteil von 83,8 % an der deutschsprachigen Bevölkerung ab 14 Jahren und einem Zuwachs gegenüber 2015 von 3,4 % bzw. 1,9 Mio. Menschen[42]. Jedermann, 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 über Netzwerke gesteuert. Auch der stationäre Handel speichert zunehmend die Daten seiner Kunden in Datenbanken, die wiederum als Angriffsziel krimineller Hacker dienen und missbraucht werden können.

3.1 Datenpannen großen Ausmaßes – Data Breaches

Unter dem Begriff „Data Breach“ werden sowohl beabsichtigte als auch unbeabsichtigte 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, weil z. B. das Kreditkartenkonto von Kriminellen bis zum Limit ausgeschöpft wurde, oder in Form von persönlichen Nachteilen wie Imageschäden, weil z. B. 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 ursächlich ein nicht hinreichend gesicherter Umgang von Unternehmen mit Daten. Zumeist stehen aber technisch versierte Täter, sogenannte Hacker, hinter den Angriffen.

42 http://www.ard-zdf-onlinestudie.de/.

Data Breach/Bedrohungslage:

ENISA bezeichnete bereits das Jahr 2014 als „Jahr der Datenpannen". Dennoch ist in den Fallzahlen für 2016 im Vergleich zu 2014 ein weiterer signifikanter Anstieg um 45 % (im Vergleich zu 2015 um 25 %) zu verzeichnen[43].
Europol listet im iOCTA 2016 nur 15 der beobachteten Databreaches aus der ersten Jahreshälfte 2016 auf und kommt dabei bereits auf eine Summe von über 43 Mio. kompromittierten Datensätzen. Bei dem wesentlichen Teil der kompromittierten Daten handelt es sich um Nutzerdaten und insbesondere Anmeldeinformationen, was Kriminellen Tür und Tor für weitere Straftaten wie z. B. Phishing-Kampagnen öffnet oder eine Monetisierung über das Darknet ermöglicht. Im September 2016 wurde bekannt, dass es Angreifern gelungen war, bereits in 2014 erfolgreich Kundenkonten von Yahoo zu hacken und seitdem Daten von über 500 Mio. Kunden zu stehlen. Hierunter sollen Namen, E-Mail-Adressen, Telefonnummern sowie verschlüsselte Passwörter gewesen sein.
Die im Rahmen des iOCTA zitierte Webseite breachlevelindex.com kommt auf eine Gesamtzahl von ca. 1,4 Mrd. gestohlenen Datensätzen in 2016.[44]

3.2 Internet der Dinge (IoT)

Der Begriff „Internet der Dinge" beschreibt den Trend, dass neben den standardmäßig genutzten Geräten (Computer, Smartphone, Tablet) zunehmend auch sogenannte intelligente Endgeräte an das Internet angeschlossen 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 Code[45] entwickelt werden.

Zu oft verfügen diese sogenannten intelligenten Endgeräte über keine oder nur unzureichende Schutzmechanismen und nutzen häufig veraltete Betriebssysteme/Software mit Sicherheitslücken. Für Cyberkriminelle sind solche Geräte leicht angreifbar, wobei Infektionen für die Benutzer kaum feststellbar sind.

Der Trend zum sogenannten 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, verbreitet sich zunehmend. Hierdurch eröffnen sich vielfältige neue Möglichkeiten zur Begehung von Straftaten (z. B. Deaktivierung der häuslichen Alarmanlage zur Vorbereitung von Einbrüchen, Manipulation von Kraftfahrzeugen).

Eine Studie der Allianz Global Corporate & Specialty (AGCS) geht davon aus, dass bis zum Jahr 2020 mehr als eine Billion internetfähiger Endgeräte weltweit mit dem Internet verbunden sein werden.[46]

43 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

44 http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf.

45 Software, deren Quellcode (englisch: source code) offen liegt und in der Regel frei verfügbar ist.

46 Studie der Allianz Global Corporate & Specialty (AGCS) mit dem Namen „A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity".

3.3 Industrie 4.0

Auch die elektronische und webbasierte Steuerung von Prozessen in Industrieunternehmen gewinnt weiter an Bedeutung. Die zunehmende Vernetzung, die Abhängigkeit vernetzter, sich selbst steuernder Produktionsprozesse und Logistikketten von der Verfügbarkeit der Netze und die Problematik der sicheren Trennung und Abschottung dieser Netze vom Internet stellen dabei eine große Herausforderung dar.

Die Folge all dieser Entwicklungen ist eine steigende Abhängigkeit der Unternehmen von der Informationstechnik, einhergehend mit einem sehr hohen Gefährdungspotenzial. Angriffe auf die IT-Infrastruktur von Unternehmen führen mittlerweile nicht mehr alleine zur Störung der Kommunikation, sondern bergen vielmehr die Gefahr eines kompletten Produktionsstillstands mit allen damit verbundenen Folgen.

Von einer weiteren Zunahme der Angriffe mittels Ransomware, also der digitalen Erpressung auf Unternehmen muss bei der geschilderten aktuellen Lageentwicklung ausgegangen werden.

Bewertung der eigenen Sicherheitssituation versus tatsächliche Bedrohungslage

Laut einer Studie von PricewaterhouseCoopers (PwC) zur Informationssicherheit in mittelständischen Unternehmen in Deutschland klaffen die Bedrohungslage und die Bewertung der eigenen Sicherheitssituation auseinander. Ein „IT-Sicherheitsruck" bei mittelständischen Unternehmen wurde jedenfalls nicht erkannt. Damit gingen diese Unternehmen ein hohes Risiko ein. Als „Hidden Champions" seien sie hochinnovativ, im Vergleich zu Kapitalgesellschaften jedoch oft ungenügend gesichert und damit ein besonders beliebtes Angriffsziel. Außerdem setze der Mittelstand mehr und mehr auf die digitale Transformation seiner Geschäfts- und Produktionsprozesse. Das Ergebnis seien hochkomplexe IT-Infrastrukturen, die eine intakte Informationssicherheit im eigenen Unternehmen zu einer umso größeren Herausforderung werden lassen." [47]

47 PwC-Studie: „Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand" https://www.pwc.de/de/mittelstand/informationssicherheit-im-deutschen-mittelstand.html.

4 Gesamtbewertung und Ausblick

Auch wenn die im Jahre 2016 signifikant angestiegenen Fall- und Schadenszahlen im Bereich von Cybercrime im engeren Sinne zu einem wesentlichen Teil auf eine Änderung der Erfassungsrichtlinien in der PKS zurückgeführt werden können, sind sie dennoch ein Indiz für das weiter gestiegene Gefährdungs- und Schadenspotenzial von Cybercrime.

Mit der weiter zunehmenden Bedeutung der IT im privaten sowie professionellen Bereich steigen die Manipulations- und Angriffsmöglichkeiten. Polizeiliche Ermittlungsergebnisse deuten zudem darauf hin, dass Täter im Bereich Cybercrime sich zunehmend professionalisieren, indem sie ihre Vorgehensweise ständig verfeinern und flexibel aktuellen Gegebenheiten anpassen.

Wiederholte Datendiebstähle spektakulären Ausmaßes und die tägliche Betroffenheit jedes einzelnen Users, z. B. durch ständige Spam-Mails, bergen die Gefahr der Resignation oder auch letztlich fehlender Sensibilität für die zwingende Notwendigkeit verstärkter, eigenverantwortlicher Präventivmaßnahmen zum Selbstschutz.

Cybercrime ist ein transnationales Kriminalitätsphänomen – eine entgrenzte Kriminalität.

Die bereits in den Vorjahren festgestellte Erweiterung des Täterspektrums hat sich im Berichtsjahr fortgesetzt. Die Täter begehen heute nicht mehr ausschließlich Cybercrime-Straftaten im engeren Sinne, sondern bieten vielmehr die zur Begehung von Straftaten erforderliche Schadsoftware oder gar komplette technische Infrastrukturen in der Underground Economy an. Diese Werkzeuge eröffnen aufgrund ihrer einfachen Handhabung auch Tätern ohne fundierte IT-Spezialkenntnisse die Möglichkeit, Straftaten über das Internet zu begehen. Es agieren daher nicht mehr ausschließlich hoch spezialisierte Täter mit umfassenden IT-Kenntnissen, sondern zunehmend auch Kriminelle ohne spezifische Fachkenntnisse, die für eine Tatbegehung erforderliches Know-how und Ressourcen käuflich erwerben bzw. ihre individuellen Fähigkeiten für die Begehung der Straftaten in heterogene Gruppen einbringen und arbeitsteilig zusammenwirken.

Organisierte Täterstrukturen haben im Phänomenbereich Cybercrime in den vergangenen Jahren an Bedeutung gewonnen. Es muss davon ausgegangen werden, dass sich diese Entwicklung fortsetzt.

Aufgrund der noch stärker zunehmenden Bedeutung der weltweiten digitalen Vernetzung in allen Lebensbereichen steigt die Gefahr für jedermann und jedes Unternehmen Opfer von Cybercrime zu werden. Die digitale und analoge Welt sind kaum noch zu trennen. Die Übergänge u. a. durch Nutzung von mobilen Geräten, das „Internet der Dinge“ und die zunehmende Technisierung von Industrie und Handel („Industrie 4.0“) sind fließend.

Aktuelle Technologietrends eröffnen aus Täterperspektive neue Tatgelegenheiten und dürften die Bedrohungslage weiter verschärfen.

Eine nachhaltige ganzheitliche Bekämpfung von Cybercrime einschließlich einer effektiven Prävention kann nur im nationalen (z. B. Gemeinsames Cyber-Abwehrzentrum) und internationalen Verbund (z. B. Europol, Interpol) der zuständigen Sicherheitsbehörden und in enger Kooperation mit der Wirtschaft (z. B. German Competence Centre against Cybercrime e.V. - G4C) erfolgen.

Impressum

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2016

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de