Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2015

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 bildet schwerpunktmäßig die im Jahr 2015 polizeilich erfassten Fälle von Cybercrime im engeren Sinne ab. Es wird über die Entwicklungen im Jahr 2015 berichtet und das Gefahren- und Schadenspotenzial von Cybercrime und dessen Bedeutung für die Kriminalitätslage in Deutschland beschrieben.
Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Diese beinhaltet alle Straftaten, einschließlich der mit Strafe bedrohten Versuche, die polizeilich bearbeitet und an die Staatsanwaltschaft abgegeben wurden. Nicht berücksichtigt sind Cybercrime-Straftaten, bei denen von einer politischen oder nachrichtendienstlichen Motivation ausgegangen wird.

Seit dem Jahr 2014 findet eine PKS-Erfassung von Delikten der Cybercrime bundeseinheitlich ausschließlich in Fällen statt, in denen konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen. Dies zu erkennen gestaltet sich in diesem Phänomen jedoch häufig schwierig.
In Anbetracht der sehr großen Anzahl von Cybercrime-Straftaten, die der Polizei nicht zur Kenntnis gelangen (sogenanntes Dunkelfeld), bedarf es zur Einschätzung des Gefahrenpotenzials von Cybercrime auch der Einbeziehung nichtpolizeilicher Informationsquellen, z. B. Studien von Antivirensoftware-Herstellern oder behördlicher Einrichtungen, die die polizeilich bekanntgewordenen Straftaten (sogenanntes Hellfeld) ergänzen. Aussagen des Lagebildes zu den verschiedenen Erscheinungsformen von Cybercrime beruhen daher sowohl auf Erkenntnissen aus dem kriminalpolizeilichen Informationsaustausch zu Sachverhalten im Zusammenhang mit Cybercrime als auch auf polizeiexternen Quellen.

2 DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

2.1 POLIZEILICHE KRIMINALSTATISTIK

Die Zahl der unter Cybercrime im engeren Sinne in der PKS erfassten Straftaten ist im Jahr 2015 gegenüber dem Vorjahr um 8,3 % zurückgegangen; die Aufklärungsquote lag bei 32,8 % und damit 3,4 Prozentpunkte über der Vorjahresaufklärungsquote (2014: 29,4 %).
Die Fälle von Computerbetrug haben um 5,6 % zugenommen und bilden die überwiegende Mehrheit aller Cybercrime-Straftaten. Die Schadenssumme in diesem Bereich ist um 2,8 % gesunken.

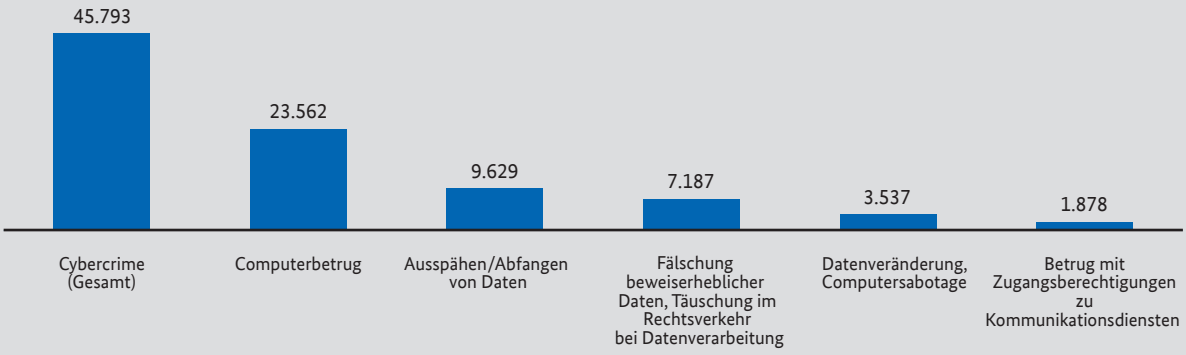
Die Fallzahlen zum Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten sind um 8,6 % gesunken. Die registrierte Schadenssumme in diesem Bereich ist von 2,5 auf 4,6 Mio. Euro (+84 %) angestiegen.[01]
Die für das Berichtsjahr erfasste Gesamtschadenssumme betrug 40,5 Mio. Euro. Dies entspricht einer Zunahme um 2,8 % gegenüber dem Vorjahr. Den gesunkenen Gesamtzahlen im Jahr 2015 steht somit eine steigende Qualität der erfassten Straftaten gegenüber.

01 Die Zahlen vor dem Jahr 2014 können aufgrund veränderter Erfassungsmodalitäten in der PKS nicht zum statistischen Vergleich herangezogen werden: Bis einschließlich 2013 erfasste die Mehrzahl der Bundesländer Cybercrimedelikte 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.
Ab dem Jahr 2014 werden Delikte der Cybercrime bundeseinheitlich nur noch in der PKS erfasst, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen.
Der Rückgang der Fallzahlen in 2015 wurde weiterhin durch die im Jahr 2014 eingeführte und noch laufende Umstellung der Erfassungsmodalitäten in den Bundesländern beeinflusst.
Um zukünftig auch die vom Ausland oder einem unbekannten Tatort aus begangenen Cybercrimedelikte und deren schädigende Auswirkung auf Deutschland zu erheben und in die Lagedarstellung aufzunehmen, ist eine gesonderte statistische Erfassung dieser Straftaten vorgesehen. Dies wird aufgrund von Umstellungen bei der Datenerfassung und -anlieferung voraussichtlich erst ab dem Jahr 2017 möglich sein.

Fallzahlen

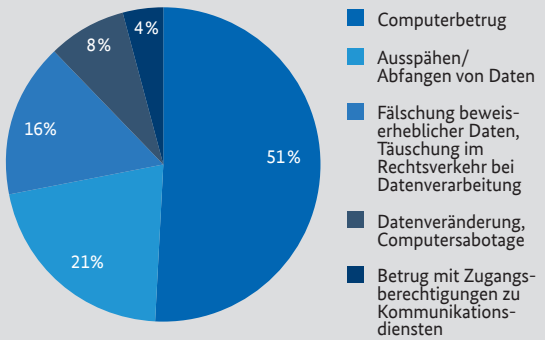
Für das Jahr 2015 registrierte die PKS insgesamt 45.793 Straftaten im Bereich Cybercrime im engeren Sinne.

Cybercrime im engeren Sinne 2015



Für die einzelnen Phänomenbereiche ergibt sich daraus folgende prozentuale Verteilung:

Cybercrime im engeren Sinne 2015 (prozentuale Verteilung)



Der **Computerbetrug** (§ 263a StGB) erfasst insbesondere die Verwertungshandlungen des Phishing (beispielhaft: Initiierung missbräuchlicher Transaktionen im Online-banking unter Nutzung von Schadsoftware), Trans-aktionen unter Nutzung missbräuchlich erlangter Kreditkartendaten und den Einsatz gestohlener oder gefälschter Zahlungskarten am Geldautomaten oder Point-of-Sale (POS)-Terminal.

Das **Ausspähen und Abfangen von Daten** (§§ 202a, 202b StGB) erfasst 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"[02] zum Kauf angeboten und täterseitig missbräuchlich einge-setzt. Die Verwertung erfolgt damit in zwei Stufen, dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

Der Straftatbestand der **Fälschung beweiserheblicher Daten bzw. der Täuschung im Rechtsverkehr** (§ 269 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-Informati-onen, 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. §§ 303a, 303b StGB umfassen typischer-weise die Denial of Service-Angriffe (DoS-, DDos-An-griffe[03]), ebenso fällt darunter die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojanische Pferde, Viren, Würmer usw.).

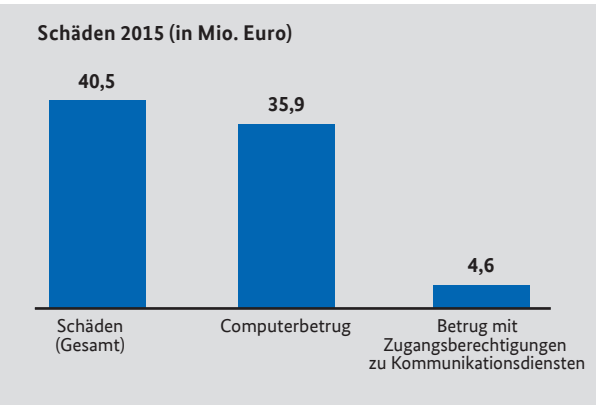
02 Überregionale Online-Schwarzmärkte, oft im sogenannten Darknet, über die Anbieter und Käufer ihre kriminellen Geschäfte rund um die digitale Welt anbahnen und abwickeln können.

03 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 (Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2015 - Glossar).

Ein Schwerpunkt beim **Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten** (§ 263a StGB) ist die Manipulation von Telekommunikationsanlagen. Unter Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen werden sowohl bei Firmen als auch bei Privathaushalten z. B. durch den unberechtigten Zugriff auf Router teure Auslandstelefonverbindungen angewählt oder gezielt Premium-bzw. Mehrwertdienste in Anspruch genommen.
Einzelne bzw. besonders relevante Phänomene, wie z. B. Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch die vielfältigen anderen Erscheinungsformen der digitalen Erpressung (z. B. die sog. „Ransomware“ [04]), werden in der PKS nicht unter dem Begriff Cybercrime im engeren Sinne, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen, also der Erpressung, erfasst. Insofern finden diese deliktischen Ausprägungen keine Berücksichtigung im vorliegenden Lagebild Cybercrime, bzw. sind lediglich in den Zahlen zum Tatmittel Internet enthalten.

Schäden

Bei Cybercrime werden in polizeilichen Statistiken nur bei den Delikten Computerbetrug und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten Schäden registriert. Die für 2015 erfasste Gesamtschadenssumme betrug hier 40,5 Mio. Euro. Dies entspricht einer Zunahme um 2,8 % (2014: 39,4 Mio. Euro).
Vom erfassten Gesamtschaden entfallen rund 35,9 Mio. Euro auf den Bereich Computerbetrug und rund 4,6 Mio. Euro auf den Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten. Die Tatsache, dass zu lediglich zwei Deliktsbereichen eine statistische Schadenserfassung erfolgt, lässt, bedingt durch das hohe Dunkelfeld, keine belastbaren Aussagen zum tatsächlichen monetären (Gesamt-) Schaden durch Cybercrime zu.



Fallbeispiele

Betrug mit Zugang zu Kommunikationsdiensten – Hacking von Telefonanlagen (Voice-Mailbox-Manipulation):
In einem Fall gelang es unbekannten Tätern im Oktober 2015, eine Telefonanlage einer Hochschule anzugreifen. Innerhalb eines Wochenendes wurden ca. 12.000 Telefon-Verbindungen in den Tschad und nach Ascension, Liberia und Guinea Bissau mit einer Verbindungsdauer von insgesamt ca. 80.000 Minuten über eine Nebenstellennummer aufgebaut und dadurch ein Schaden von ca. 120.000 Euro verursacht.

Gewerbsmäßiger Computerbetrug:
Im Jahr 2015 registrierten die Strafverfolgungsbehörden erneut steigende Fallzahlen bei betrügerischen Buchungen von Onlinetickets der Deutschen Bahn unter Verwendung widerrechtlich erlangter Kreditkartendaten, welche dann in Bereicherungsabsicht Reisenden deutlich unter Wert angeboten wurden. Entsprechende Angebote wurden über die Internetauftritte von Mitfahrzentralen, über Auktionsplattformen oder über eigens eingerichtete Webseiten platziert. Es entstand ein Schaden in Millionenhöhe.

Tatmittel Internet

Im Jahr 2015 wurden in der PKS insgesamt 244.528 Straftaten erfasst, bei denen das Internet als Tatmittel genutzt worden ist. Die Zahlen bewegen sich damit in etwa auf Vorjahresniveau (2014: 246.925 Fälle).
Überwiegend handelte es sich bei den mithilfe des Internets begangenen Delikten um Betrugsdelikte (Anteil: 74,5 %; 182.278 Fälle), darunter vor allem Fälle von Warenbetrug (Anteil 30,4 %; 74.421 Fälle), bei denen Täter über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder in minderwertiger Qualität lieferten. Den Tätern geht es allein darum, die Käufer/Opfer zu einer Zahlung zu veranlassen.
Spielt das Internet im Hinblick auf die Tatverwirklichung eine nur unwesentliche Rolle, wird die Sonderkennung „Tatmittel Internet“ nicht verwendet. Dies ist beispielsweise der Fall, wenn im Vorfeld der eigentlichen Tat Kontakte zwischen Täter und Opfer mittels Internet stattfanden.

04 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.

Polizeilich nicht bekanntgewordene Straftaten – Dunkelfeld

Im Deliktsfeld der Cybercrime muss von einem sehr großen Dunkelfeld ausgegangen werden. Untersuchungen[05] belegen, dass nur ein kleiner Teil der Straftaten in diesem Bereich zur Anzeige gebracht und damit den Strafverfolgungsbehörden bekannt wird.
Hinzu kommt, dass insbesondere in den Deliktsfeldern Computersabotage und Datenveränderung sowie Computerbetrug:

- eine große Anzahl der Straftaten aufgrund immer weiter verbreiteter technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinauskommt und von den Geschädigten gar nicht bemerkt wird,
- Straftaten durch Geschädigte nicht angezeigt werden, insbesondere so lange noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC),
- Geschädigte, insbesondere Firmen, erkannte Straftaten oft nicht anzeigen, um beispielsweise im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner“ nicht zu verlieren oder
- oftmals Geschädigte beispielsweise in Erpressungsfällen nur dann Anzeige erstatten, wenn trotz Zahlung eines Lösegeldes keine Dekryptierung des durch die Täterseite verschlüsselten Systems erfolgt.

Eine Kenntnis der versuchten und begangenen Straftaten ist für die Strafverfolgungsbehörden gerade im Deliktsbereich Cybercrime von Bedeutung, da beispielsweise die Analyse durchgeführter Angriffe zentral für eine effektive Bekämpfung ist. Durch eine solche Analyse lassen sich nicht nur Angriffsvektoren und mögliche Tatzusammenhänge erkennen, um daraus Ermittlungsansätze abzuleiten, sondern insbesondere auch Präventionsmaßnahmen entwickeln, wie bspw. Patches[06] für betroffene Systeme oder Sicherheitshinweise für Nutzer zu neuen Tatbegehungsweisen.
Ein möglichst umfassendes Bild zur Dimension dieses Deliktsbereiches und den Erscheinungsformen des kriminellen Missbrauchs von Internet und Informationstechnik sind Grundvoraussetzung dafür, dass Strafverfolgungsbehörden schnell und zielgerichtet auf neue Entwicklungen reagieren können. Es hilft, Nutzer informationstechnischer Systeme durch mittel- und langfristige Bekämpfungs- und Präventionsstrategien effektiv zu schützen.

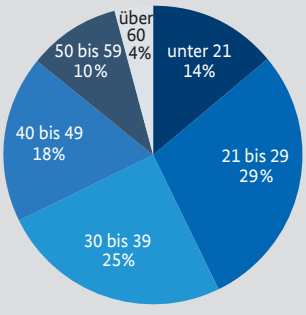
2.2 TÄTERSTRUKTUREN

Der überwiegende Teil der Cyberkriminellen handelt aus finanzieller Motivation. Dabei reicht das Spektrum vom klassischen Einzeltäter bis hin zu international organisierten Tätergruppierungen. Täter arbeiten im Bereich Cybercrime oftmals nicht mehr in den klassischen hierarchischen Strukturen, sie kennen sich teilweise nicht persönlich, sondern nutzen auch bei arbeitsteiliger Kooperation die Anonymität des Internets.

Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Services, die nicht selbst erbracht werden können, werden von anderen hinzugekauft. Das Angebot in der Underground Economy ist breit und reicht von für die Begehung von Straftaten erforderlicher Schadsoftware bis hin zu kompletten technischen Infrastrukturen.

Cybercrimedelikte werden vornehmlich von Männern begangen. Von 11.643 im Jahr 2015 in der PKS registrierten Tatverdächtigen waren lediglich 23 % Frauen.

Altersstruktur der Tatverdächtigen



05 Unter anderem „e-Crime Studie 2010 – Computerkriminalität in der deutschen Wirtschaft“ (KPMG, 2010), „Befragung zu Sicherheit und Kriminalität in Niedersachsen“ (Landeskriminalamt Niedersachsen, November 2013).

06 Ein Patch („Flicken“, „bugfix“) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen, Fehler korrigieren oder andere Verbesserungen integrieren (Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2015 – Glossar).

Bei Cybercrime im engeren Sinne handelt es sich entgegen der verbreiteten Annahme nicht um Kriminalität, die schwerpunktmäßig von Jugendlichen bzw. sogenannten „Script-Kiddies“ begangen wird. Die am stärksten vertretene Altersgruppe sind die 21 bis 29-Jährigen mit 29 % (3.360 festgestellte Tatverdächtige), danach folgen die 30 bis 39-Jährigen (2.880 festgestellte Tatverdächtige) mit 24,7 %, und schließlich die Gruppe der 40 bis 49-Jährigen mit 18 % (2.094 festgestellte Tatverdächtige).
Damit wird weit mehr als die Hälfte (57 %) der registrierten Delikte der Cybercrime im engeren Sinne von über 30-Jährigen begangen.

2.3 ORGANISIERTE KRIMINALITÄT

Im Deliktsfeld Cybercrime agieren zunehmend auch Tätergruppierungen, die der Organisierten Kriminalität (OK) zuzurechnen sind. Waren 2013 noch sechs OK-Gruppierungen im Kriminalitätsbereich Cybercrime erfasst worden, waren es im Jahr 2014 zwölf und 2015 bereits 22 Gruppierungen. Gemessen an der Gesamtzahl der im Jahr 2015 registrierten OK-Gruppierungen (566) bewegt sich der Anteil der im Bereich Cybercrime aktiven OK-Gruppierungen zwar immer noch auf einem relativ niedrigen Niveau, die Tendenz ist jedoch steigend.
Das Internet als Tatmittel wurde von OK-Gruppierungen in 89 (15,7 %) der insgesamt 566 der 2015 in Deutschland geführten OK-Verfahren genutzt.

2.4 AKTUELLE PHÄNOMENE

Digitale Erpressung unter Einsatz sogenannter Ransomware[07]

Digitale Erpressung mittels sogenannter „Ransomware“ ist ein in Deutschland weit verbreitetes Phänomen. Entsprechende Schadsoftware oder auch die gesamte „Dienstleistung“ (z. B. im sogenannten „Affiliate-Modell“[08]) kann z. B. in Foren der Underground Economy erworben werden, sodass mittlerweile kein besonderer IT-Sachverstand zur Durchführung digitaler Erpressungshandlungen erforderlich ist.

Im Jahr 2015 wurde ein neuartiger „digitaler Erpressungsdienst“ im Internet festgestellt. Die im sogenannten Darknet[09] verfügbare Dienstleistung ermöglicht selbst Anfängern im Bereich der IT, eine Ransomware ohne großen Aufwand kostenlos zusammenzustellen (sog. „Malware-Toolkit“). Die Anbieter des Dienstes erhalten bei einer erfolgreichen Lösegeldzahlung eine Umsatzbeteiligung, wobei die Lösegeldzahlung in der Regel in Form der digitalen Währung „Bitcoin“[10] über den Schadsoftwareanbieter selbst abgewickelt wird. Über eine vom Schadsoftwareanbieter zur Verfügung gestellte Kontrollplattform kann der Nutzer des Toolkits die von ihm hervorgerufenen Infektionen einsehen und seinen verbliebenen Anteil an den Lösegeldern an sich selbst auszahlen. Nur die Verbreitung der Ransomware muss durch den Kunden eigenständig und eigenverantwortlich durchgeführt werden.

07 Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld („ransom“) zu erpressen (Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2015 - Glossar).

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

09 Webseiten im Darknet (englisch für „Dunkles Netz“) werden nicht von den gängigen Internet-Suchmaschinen indiziert und können nicht über konventionelle Internettools (Internet-Browser) erreicht werden.

10 Bitcoin = englisch für „digitale Münze“. Weltweit verfügbares Zahlungssystem mit virtuellem Geld.

Grundsätzlich muss bei Ransomware zwischen zwei Varianten unterschieden werden:

a) Ransomware, die keine Verschlüsselung der Festplatte, sondern durch eine Manipulation lediglich den Zugriff auf das System im Sinne einer Sperrung verwehrt. Die wohl bekanntesten Ausprägungen sind Schadprogramme, bei denen bekannte Namen und Logos von Sicherheitsbehörden[11] missbraucht werden, um der kriminellen Zahlungsaufforderung einen offiziellen Charakter zu verleihen.[12]

b) Sogenannte 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 in den meisten Fällen keine andere Möglichkeit besteht, die verschlüsselten Daten wiederzuerlangen bzw. die verschlüsselten Daten trotz Zahlung des geforderten „Lösegeldes“ nicht wiedererlangt werden können.

Wirksame Schutzmaßnahmen reduzieren das Risiko einer Infektion. Solche Maßnahmen bestehen u. a. in der Nutzung professionell aufgebauter Netzwerkstrukturen mit umfassenden Sicherungsmaßnahmen (Antiviren-Software, Firewall etc.) sowie der Durchführung regelmäßiger Datenbackups, die anschließend getrennt (offline) vom Netzwerk vorgehalten werden.
Für das Jahr 2015 wurden dem BKA lediglich 400 Fälle von digitaler Erpressung gemeldet, was einen Rückgang um 26,6 % gegenüber dem Vorjahr (545 Fälle) entspricht. Die Erkenntnislage des Bundesamts für Sicherheit in der Informationstechnik (BSI) steht im Widerspruch zu dieser Entwicklung. Gemäß den Feststellungen des BSI verbreitete sich Ransomware im Jahre 2015 stärker als 2014.[13]
Seit Mitte September 2015 hat sich die Bedrohungslage durch Ransomware noch deutlich verschärft.[14] Dies spiegelte sich zugleich in einer vertieften Medienberichterstattung wider. Weil der Druck für die Betroffenen, ihre Daten wieder zu erlangen, sehr hoch ist, zahlen viele das geforderte Lösegeld. Laut einer Umfrage eines Anbieters von Sicherheitssoftware haben 33 % der in Deutschland von Ransomware Betroffenen Lösegeld gezahlt und sind 36 % der Internetnutzer in Deutschland grundsätzlich bereit, die Forderungen von Erpressern zu erfüllen, sollten sie Opfer von Ransomware werden. In Deutschland liegt demnach der Betrag, bis zu dem eine Zahlungsbereitschaft besteht, bei durchschnittlich 211 Euro.[15] Dieser Erfolg der Täter führe dazu, dass mittlerweile Kapazitäten aus dem „Banking-Trojaner-Geschäft“ abgezogen werden und Botnetze nun Ransomware verteilen.[16]
Seit Dezember 2015 werden große Spam-Wellen festgestellt, über die massenhaft Ransomware verteilt wird. Es handelt sich in über 95 % um Ransomware mit Verschlüsselungsfunktionen. Einfache Sperrbildschirme im Desktop-Bereich haben heute keine Relevanz mehr.[17]

Fallbeispiel

In einer süddeutschen Klinik ist im Jahr 2015 Verschlüsselungsschadsoftware (Ransomware) in Form eines sogenannten „CryptoLockers“ durch Öffnen eines E-Mail-Anhangs durch einen Mitarbeiter in das Datenverarbeitungssystem gelangt. Die Malware verschlüsselte anschließend alle Dateien und Verzeichnisse, für die der Mitarbeiter Schreib- und Leserechte besaß. Dazu zählten auch sensible Daten wie z. B. Arztbriefe. Ziel des Angriffs war die Verschlüsselung von Dateien zur Erpressung eines nicht näher bekannten Geldbetrages in Bitcoin, wobei nicht von einem zielgerichteten Angriff auf den Klinikverbund ausgegangen werden kann. Auf den Erpressungsversuch wurde seitens der Klinik nicht eingegangen.

Bisher haben sich keine konkreten Hinweise ergeben, dass gezielt Angriffe auf bestimmte Unternehmenssparten durchgeführt wurden. Diese Feststellung wird auch dadurch gestützt, dass bislang verschiedenste Unternehmensarten bzw. Behörden infiziert wurden.

11 Bekannte Beispiele sind der sogenannte „BKA-Trojaner“ und der „GVU-Trojaner“.

12 Bundeslagebilder Cybercrime 2012 und 2013 (www.bka.de).

13 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2015“.

14 BSI (2016): Ransomware, Bedrohungslage, Prävention & Reaktion, S. 5.

15 http://www.crn.de/security/artikel-109549.html?tweet.

16 Genutzt wird vermehrt das Dridex-Botnetz, vgl. BSI (2016): Ransomware, Bedrohungslage, Prävention & Reaktion, S. 5.

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

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

Das Geschäftsmodell „Cybercrime-as-a-Service“ gewinnt weiter an Bedeutung. Die digitale Underground Economy stellt eine große Bandbreite an Dienstleistungen zur Verfügung, welche die Durchführung jeder Art von Cybercrime ermöglichen bzw. erleichtern. Das Angebot an solchen illegalen Dienstleistungen 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,
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität,
- sog. Dropzones zum Ablegen illegal erlangter Informationen und/oder Waren.

Diese Beispiele zeigen, dass interessierte Kriminelle auch ohne eigene technische Kenntnisse und mit vergleichsweise geringem Aufwand Zugang zu hochentwickelten Cyber-Werkzeugen erhalten können, mit denen alle Formen von Cybercrimeangriffen ausgeführt werden können. Mittlerweile wird – analog zu legalen Software-Verträgen – häufig sogar Support für die Kunden/Bezieher der Leistungen des Cybercrime-as-a-Service angeboten. Dieser Support beinhaltet beispielsweise Updates für Schadsoftware, Beratungsdienste, Anti-Erkennungsmechanismen sowie die Hilfestellung bei technischen Problemen.
Darüber hinaus werden als weitere Dienstleistungen auch die „Infection on Demand“ (Verteilung von Schadsoftware auf Anforderung/Abruf) sowie Test-Portale angeboten, 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.

Fallbeispiel

Im Jahr 2015 wurde unter Federführung des FBI und Europols ein sogenanntes Underground Economy-Forum zerschlagen, über das die Täter diverse inkriminierte Dienstleistungen angeboten hatten.
Bei diesem Forum handelte es sich um das zum damaligen Zeitpunkt bedeutendste englischsprachige Forum der Underground Economy, in dem auch zahlreiche deutsche bzw. deutschsprachige Nutzer aktiv waren. Deren kriminelle Aktivitäten richteten sich gegen deutsche Unternehmen bzw. Geschädigte. Der Server dieses Forums befand sich zeitweise in Deutschland.
Die zwischen den beteiligten Strafverfolgungsbehörden in 17 Staaten organisierten strafprozessualen Maßnahmen im Zusammenhang mit dem sogenannten „Takedown“ (Stilllegung) des Forums erfolgten im Juli 2015. Die Maßnahmen umfassten, neben Festnahmen und Hausdurchsuchungen bei den ca. 50 identifizierten Forumsmitgliedern, die Beschlagnahme der Forums-Domain sowie die Sicherstellung des entsprechenden Servers.

Digitale Schwarzmärkte – Underground Economy

Die illegalen Foren oder Marktplätze der digitalen Underground Economy spielen eine zunehmend zentrale Rolle bei der Begehung von Straftaten im Bereich Cybercrime. Die Foren dienen 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.
Zusätzlich werden insbesondere im Darknet kriminelle Marktplätze betrieben, auf denen illegale Waren erworben werden können. Die Angebote umfassen u. a. Drogen, Waffen, Falschgeld, gefälschte Ausweise, gestohlene Kreditkartendaten oder gefälschte Markenartikel. Der Handel mit Kinderpornografie erfolgt in der Regel über eigens dafür geschaffene Plattformen.
Zur Bezahlung der gehandelten Waren werden ausschließlich digitale Kryptowährungen akzeptiert, die ein pseudoanonymes Bezahlen ermöglichen. Darüber hinaus bieten diese kriminellen Marktplätze zum Schutz der Verkäufer und Käufer oftmals auch ein Treuhandsystem an. Je nach Ausgestaltung dieses Systems ermög-

licht es den als „Treuhändern“ agierenden Kriminellen, das ihnen anvertraute Geld aus allen laufenden Transaktionen des Marktplatzes zu unterschlagen und danach „unterzutauchen“.
Die Zunahme von Aktivitäten in der Underground Economy verdeutlicht eine zunehmende Verlagerung von Delikten aus der analogen in die digitale Welt. Ausschlaggebend für diese Entwicklung dürfte nicht nur die mögliche Anonymität sein, sondern auch der Umstand, dass über illegale Online-Marktplätze weltweit unzählige potenzielle Kunden erreicht werden können, auch weil diese Foren und Marktplätze im Darknet ohne tiefergehende Computerkenntnisse erreichbar sind.

Diebstahl digitaler Identitäten und Identitätsmissbrauch

Die digitale Identität als Ganzes oder zumindest Teile der digitalen Identität sind begehrtes Diebesgut von Cyberkriminellen, sei es, um die erlangten Informationen für die eigenen kriminellen Zwecke einzusetzen oder um die gestohlenen Daten meist über illegale Verkaufsplattformen der Underground Economy zu veräußern.
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[18].

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) Bestandteil der digitalen Identität.
Um in den Besitz dieser Informationen zu gelangen, werden täterseitig häufig neben sog. „Trojanischen Pferden“[19] auch andere Methoden unter Nutzung des Internets eingesetzt, wie z. B.:

- Installation von Schadprogrammen über Drive-By-Exploits[20],
- Phishing,
- Einbruch auf Servern und Kopieren der Anmeldeinformationen,
- Einsatz von Keyloggern[21] oder Spyware[22].

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

Fallbeispiel

Im Rahmen eines 2015 geführten Ermittlungsverfahrens gegen die Betreiber einer Plattform, die mit ausgespähten digitalen Identitäten handelte, konnten über 7,4 Millionen Datensätze sichergestellt werden, die User-Accounts diverser Diensteanbieter enthielten. In den Datensätzen befanden sich u. a. Informationen zu hinterlegten Kreditkarten und Bankkonten. Die Ermittlungen ergaben, dass ein überwiegender Teil der Zugangsdaten zum Zeitpunkt der Sicherstellung valide war.
Im internationalen Zusammenwirken der Sicherheitsbehörden mit weltweit aktiven Diensteanbietern wurden umgehend präventive Maßnahmen zum Schutz der User umgesetzt.

18 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.

19 Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) 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 (sog. Hintertür) zum Computer öffnen (Quelle: BSI-Gefährdungskataloge).

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 (Quelle: www.bsi-fuer-buerger.de).

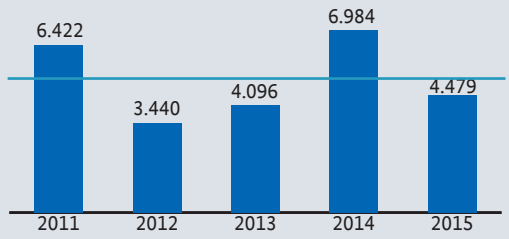
21 Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnet alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern (Quelle: www.bsi.bund.de, Glossar).

22 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 (Quelle: www.bsi.bund.de, Glossar).

Phishing im Onlinebanking

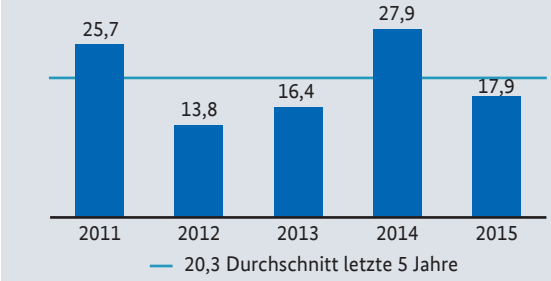
Die bekannteste Variante des digitalen Identitätsdiebstahls ist das sog. „Phishing im Zusammenhang mit Onlinebanking“. Für das Jahr 2015 wurden dem Bundeskriminalamt im Rahmen des polizeilichen Meldedienstes 4.479 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2014 (6.984) bedeutet dies eine Abnahme der Fallzahlen um 35,9 %. Die Zahl der Fälle liegt im Jahre 2015 unter dem Durchschnitt der Fallzahlen der vergangenen fünf Jahre (5.084).

Fälle – Phishing im Onlinebanking 2011-2015



Nachdem u. a. durch verschiedene Schutzmaßnahmen die verstärkte Nutzung des mTAN-Verfahrens (u. a. auch bezeichnet als smsTAN)[23] als Sicherungsmethode im Onlinebanking sowie eine noch intensivere Sensibilisierung der Anwender ein deutlicher Rückgang der Fallzahlen im Jahr 2012 erreicht werden konnte, haben die Fallzahlen bis 2014 wieder deutlich zugenommen.
Dies zeigt, dass sich die Täterseite den veränderten Rahmenbedingungen technisch angepasst und neue oder bessere Schadsoftware entwickelt hat, um dieses bisher als relativ sicher geltende Transaktionsverfahren zu umgehen.
Dazu zählen auch aktuelle „Trojanische Pferde“, die speziell auf den deutschen Bankensektor ausgerichtet sind und über das technische Potenzial verfügen, sowohl das iTAN- als auch das mTAN-Verfahren mittels sog. Echtzeitmanipulation (Man-In-The-Middle-/Man-In-The-Browser-Attacken[24]) erfolgreich anzugreifen.
Die Täter setzen dabei aber nicht nur auf rein technische Lösungen, sondern versuchen mittels sogenannten Social Engineerings[25] an die notwendigen Kundeninformationen zu gelangen, um die mittlerweile weitgehend in Deutschland verwendeten Autorisierungsmechanismen im Onlinebanking, die ein aktives Handeln des Kontoberechtigten erfordern (unter Nutzung eines zweiten Kommunikationskanals[26]), auszuhebeln. Bekanntestes Beispiel ist der Versand von E-Mails in vertrauenerweckender Aufmachung mit der Aufforderung, aus bestimmten Gründen vertrauliche Informationen preiszugeben.
Eine der Ursachen für den Rückgang der Fallzahlen im Jahre 2015 dürfte darin liegen, dass die Banken auf die Angriffe der Täterseite reagiert haben und weiter an der Verbesserung der Sicherheitsstandards im Bereich Online-Banking arbeiten.
Erfahrungsgemäß ist es aber nur eine Frage der Zeit, bis sich die Täterseite auf die neuen Sicherheitsstandards eingestellt hat und die Fallzahlen wieder ansteigen.
Phishing bildet im Hinblick auf die vorhandenen Möglichkeiten und die zu erzielenden kriminellen Erträge weiterhin ein lukratives 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. Auf dieser Berechnungsgrundlage wurden im Jahr 2015 Schäden in Höhe von 17,9 Mio. Euro verursacht, deutlich weniger als der durchschnittliche Schaden in den vergangenen fünf Jahren (20,3 Mio. Euro). Demzufolge ergeben sich unter Berücksichtigung der dem Bundeskriminalamt in den zurückliegenden fünf Jahren gemeldeten Fallzahlen[27] folgende Schadenssummen:

Schäden – Phishing im Onlinebanking 2011-2015 (in Mio. Euro)



23 mTAN (mobile Transaktionsnummer): Anders als beim iTAN-Verfahren (mit einer vorab erstellten nummerierten TAN-Liste) wird für jede Online-Überweisung eine eigene Transaktionsnummer generiert und per SMS an den Kunden übermittelt.

24 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 (Quelle: BSI Gefährdungskataloge G 5.143). 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.

25 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 (Quelle: BSI - Die Lage der IT-Sicherheit in Deutschland 2015).

26 Sogenannte „Two-factor authentication“.

27 Auf Grundlage des polizeilichen Meldedienstes.

Massenhafte Fernsteuerung von Computern (Botnetze)

Sogenannte Botnetze spielten im Jahr 2015 im Bereich Cybercrime erneut eine bedeutende Rolle. Dabei werden zahlreiche, per Schadcode infizierte Computer ohne Wissen ihrer Besitzer über sogenannte Command & Control-Server (C&C-Server) ferngesteuert. Die Installation der dafür erforderlichen 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".
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. Wenn diese aufgrund des mutmaßlich bestehenden Freundschaftsverhältnisses gutgläubig geöffnet oder entsprechende Links aktiviert werden, führt dies zur Infektion des Computers. In der Folge hat der Täter durch die Installation von Schadsoftware einen nahezu vollständigen Zugriff auf den infizierten Computer des Opfers.
Weitere Verbreitungskanäle sind das Usenet[28] und Tauschbörsen/P2P (Peer to Peer)-Netze[29], in denen die Schadsoftware meist als Video- oder Sounddatei getarnt zum Download angeboten wird.
Botnetze und ihre Kapazitäten stellen nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy dar. Die Betreiber der Botnetze, sogenannte „Bot-Herder"[30], vermieten Bots, durch die beispielsweise mittels DDoS-Attacken gezielte Angriffe auf Unternehmensserver durchgeführt werden können, 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 nur sehr schwer möglich:

- In seinem Jahresbericht 2015 spricht das BSI davon, dass allein in der ersten Jahreshälfte 2015 von Sicherheitsforschern täglich bis zu 60.000 Infektionen deutscher Systeme registriert und über das BSI an die deutschen Internetanbieter gemeldet worden sind.
- Der Verband der deutschen Internetwirtschaft e. V. (ECO)[31] berichtet in seiner Jahresstatistik, dass im Jahr 2015 bei den vom Anti-Botnetz-Beratungszentrum[32] gescannten Rechnern der Anteil der mit Botnetz-Schadsoftware infizierten Systeme bei 38 % lag (2014: 40 %)[33].

Fallbeispiel

Im Februar 2015 wurde die Infrastruktur eines Botnetzes sichergestellt und abgeschaltet, welches weltweit 3,2 Mio. infizierte Rechner umfasste. In Europa attackierte die dem Botnetz zugrunde liegende Malware in erster Linie gezielt britische Finanzinstitutionen und Telekommunikationsprovider.
Die Malware gelangte auf verschiedene Weise auf die Computer, etwa über infizierte Links in E-Mails oder z. B. beim Besuch von infizierten Webseiten. Nach einer Infektion spähte die Malware digitale Identitäten der Anwender der kompromittierten Systeme aus, darunter auch Zugangsdaten zum Online-Banking, zu sozialen Netzwerken und zu E-Mail-Providern. Auch Rechner in Deutschland waren betroffen. Deutsche Opfer wurden in Zusammenarbeit mit dem BSI von ihren Providern informiert.
Das Botnetz wurde unter internationaler polizeilicher Koordinierung und in Kooperation mit der Privatwirtschaft abgeschaltet. Zur Durchführung der Maßnahme arbeiteten polizeiliche Vertreter aus vier Staaten und Europol gemeinsam mit Repräsentanten aus mehreren IT-Firmen zusammen.

28 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 (sog. Newsgroups).

29 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 (Quelle: BSI-Maßnahmenkatalog M 5.152).

30 Herder (englisch) – Hirte.

31 www.eco.de.

32 www.botfrei.de.

33 https://www.eco.de/2016/pressemeldungen/botfrei-de-jahresstatistik-2015-zahl-der-zombierechner-weiter-bedrohlich.html.

Angriffe auf die Verfügbarkeit von Webseiten, Internetdiensten und Netzwerken (DDoS-Angriffe[34])

Eng verknüpft mit der Thematik Botnetze ist das Themenfeld der sogenannten DDoS-Angriffe, da diese Angriffe auf die Verfügbarkeit von Webseiten, einzelnen Diensten oder auch ganzen Netzen in der Regel unter Einsatz von zu einem Botnetz zusammengeschlossenen Computern erfolgen.
DDoS-Angriffe gehören zu den am häufigsten beobachteten Sicherheitsvorfällen im Cyber-Raum. Kriminelle haben hieraus bereits entsprechende Geschäftsmodelle entwickelt und vermieten Botnetze verschiedener Größen.
Statistische polizeiliche Daten (Anzahl, Dauer usw.) liegen nicht vor. Das BSI berichtet in seinem Jahresbericht von 29.437 registrierten DDoS-Angriffen im ersten Halbjahr 2015, gegenüber 25.113 Angriffen im ersten Halbjahr 2014 (+ 17 %).
Gerade im wettbewerbsintensiven Marktsegment Internet können Nichterreichbarkeiten von Vertriebsportalen zu erheblichen wirtschaftlichen Schäden führen. Die Motivlagen der Täterseite reichen von politischen/ideologischen Motiven über Rache oder das Erlangen von Wettbewerbsvorteilen bis hin zu rein monetären Interessen (Erpressung).
Die durch DDoS-Angriffe verursachten Schäden für den Geschädigten lassen sich schwer beziffern, da Folgewirkungen der Angriffe wie:

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

oftmals nur sehr schwer abschätzbar sind.

Fallbeispiel

Im Jahr 2015 erfolgten polizeiliche Ermittlungen in einem Fall der (digitalen) Erpressung wegen Distributed-Denial-of-Service (DDoS)-Angriffen gegen Server (Webdienste) größerer Unternehmen in Deutschland und 17 weiteren Ländern weltweit. In Deutschland wurden in diesem Zusammenhang 16 Fälle bekannt. International wurden Fallzahlen im hohen dreistelligen Bereich festgestellt.
Eine Tätergruppierung hatte zuletzt im Juli 2015 in Deutschland Onlinepräsenzen größerer E-Commerce-Unternehmen und Firmen mit DDoS-Attacken angegriffen und von den betroffenen Unternehmen Zahlungen in der digitalen Währung Bitcoin (BTC) gefordert, um die Angriffe einzustellen. Die Forderungen beliefen sich dabei jeweils auf ca. umgerechnet 10.000 Euro.
Im Dezember 2015 erfolgte im Rahmen einer koordinierten Maßnahme unter Mitwirkung von Strafverfolgungsbehörden der Staaten USA, Großbritannien, Deutschland, Österreich, Bosnien-Herzegowina sowie von Europol die Festnahme eines Tatverdächtigen im Ausland. Anschlussermittlungen im Ausland haben ferner zum Auffinden wichtiger Sachbeweise und zur Identifizierung eines weiteren Tatbeteiligten geführt. Der inhaftierte Hauptverdächtige konnte mit einzelnen in Deutschland begangenen Erpressungen direkt in Verbindung gebracht werden.

34 Vgl. Fußnote 5.

Mobile Endgeräte – zunehmend beliebtes Angriffsziel

Mobile Endgeräte, wie Smartphones und Tablets, gewinnen weiterhin Marktanteile. Gemäß einer repräsentativen Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM), nutzten Anfang des Jahres 2015 rund 44 Mio. Bundesbürger (ab 14 Jahren) ein Smartphone, was einer Zunahme von rund zwei Mio. innerhalb der zurückliegenden sechs Monate entspricht[35]. Neben klassischen Funktionen wie Telefonieren und der Verwendung als Foto- oder Videokamera, werden dabei u. a. meist folgende Anwendungen genutzt:

- Surfen im Internet (93 %),
- zusätzliche Apps (74 %),
- soziale Netzwerke (70 %).

Das Abspeichern persönlicher Informationen und das Abwickeln sensibler Vorgänge über die mobilen Geräte (u. a. das Abspeichern von Daten in der Cloud) macht sie zu einem lohnenden Angriffsziel für Kriminelle. Hinzu kommt ein langsames Update-Verhalten der Gerätehersteller, so dass bekannte Sicherheitslücken oftmals monatelang ungeschlossen bleiben bzw. auf zahlreichen Geräten sogar niemals geschlossen werden.
Die steigende Verbreitung sowie die teilweise immer noch mangelnde Sensibilität der Nutzer hinsichtlich der Gefahren im Umgang mit mobilen Endgeräten sorgen für eine weiterhin hohe Attraktivität für die Täterseite.
Ein wesentlicher Aspekt ist, dass mobile Endgeräte im Gegensatz zum klassischen PC in der Regel ständig online sind und die jeweiligen Nutzer mittlerweile einen Großteil ihrer digitalen Aktivitäten über diese Geräte abwickeln, wie z. B. Transaktionen im Onlinebanking, Zugriff auf E-Mail-Konten und Soziale Netzwerke oder auch Aktivitäten im Bereich des E-Commerce, oft über entsprechende Apps.
Dieser Trend steigert die Bedeutung und Attraktivität mobiler Endgeräte für Cyberkriminelle, was insbesondere durch die Zunahme von Malwareentwicklungen im Bereich mobiler Betriebssysteme unterstrichen wird. Die Anzahl der Varianten von Schadsoftware für mobile Plattformen nimmt laut BSI weiterhin rasant zu. Rund 96 % der Schadsoftware trifft aufgrund seines Verbreitungsgrads das Betriebssystem Android[36]. Insgesamt 59 % der laut BSI bis September 2015 von Antivirus-Produkten detektierten schadhaften Android-Apps sind Trojanische Pferde, 2014 lag ihr Anteil bei 51 %[37].

Fallbeispiel

Im Oktober 2015 wurden die Wohnungen von 13 Tatverdächtigen in Hessen, Baden-Württemberg, Bayern, Bremen, Niedersachsen und Nordrhein-Westfalen durchsucht. Den Betroffenen wurde vorgeworfen, über das Internet Smartphone-Schadsoftware, die gezielt Android Geräte angreift, erworben und eingesetzt zu haben. Die Koordination der Ermittlungen auf internationaler Ebene erfolgte durch Europol und Eurojust. Neben den Durchsuchungen in Deutschland erfolgten auch Maßnahmen in Großbritannien, Frankreich, Belgien und der Schweiz.
Die Schadsoftware eröffnet die Möglichkeit, die Kontrolle über das infizierte Smartphone vollständig zu übernehmen. Mit der Schadsoftware können unter anderem der Datenverkehr überwacht, Telefon- und Umgebungsgespräche heimlich abgehört sowie mit der Smartphone-Kamera heimlich Bildaufnahmen gefertigt werden. Des Weiteren können von dem infizierten Gerät Telefonate initiiert sowie SMS versandt, Daten eingesehen und verändert sowie der Standort des Smartphones lokalisiert werden. Die Schadsoftware ist insbesondere beim sog. „Phishing“ im Online-Banking von erheblicher Bedeutung, da sie das Erlangen der „mTAN“ ermöglicht. Sie ist derart konzipiert, dass sie auch von versierten Smartphone-Nutzern nicht ohne weiteres entdeckt werden kann.

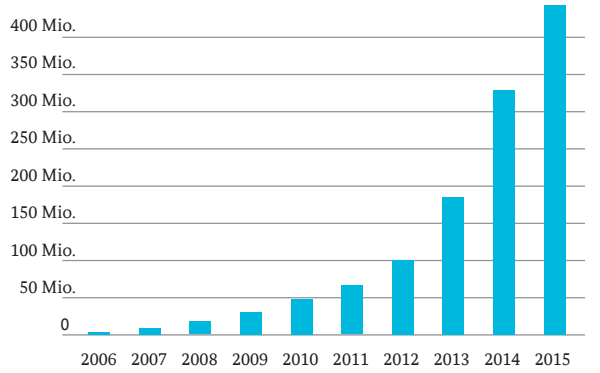
35 www.bitkom.org; Umfrage vom Februar 2015.

36 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.

37 BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2014 und 2015“.

Schadprogramme (Malware) im Allgemeinen

Schadprogramme, die unerwünschte oder schädliche Funktionen auf einem infizierten System ausführen, spielen die zentrale Rolle bei der Begehung von Straftaten im Bereich Cybercrime.
Die Verbreitung und der Einsatz von Schadprogrammen auf Opfer-Systemen ist die wesentliche Basis für die Begehung von Straftaten der Cybercrime.
Die häufigsten Verbreitungswege von Schadprogrammen sind Anhänge in Spam-Mails sowie die vom Anwender unbemerkte Infektion beim Besuch von Webseiten (Drive-by-Exploits).
Es liegen kaum valide Daten zur Verbreitung von Schadprogrammen vor. Laut BSI liegt nach Schätzungen die Gesamtzahl der Schadprogrammvarianten für PCs bei derzeit über 439 Mio. (2014 über 250 Mio.).[38]



Grafik: BSI – Bericht
„Die Lage der IT-Sicherheit in Deutschland 2015“,
Abbildung der Anzahl bekannter Windows-Schadprogrammvarianten

3 GEFAHREN- UND SCHADENSPOTENZIAL

3.1 INTERNETNUTZUNG IN DEUTSCHLAND

Die 2016 aktualisierte ARD-ZDF-Onlinestudie[39] hat für das Jahr 2015 ergeben, dass 79,5 % der Personen ab 14 Jahren in Deutschland (2014: 79,1 %) online sind. Dies entspricht 56,1 Mio. Personen (2014: 55,6 Mio.). Während bei den 14 bis 49-Jährigen die Zahlen weitgehend konstant geblieben sind, gibt es die höchsten Zuwachsraten bei den über 50-Jährigen. Bei den 50 bis 59-Jährigen nutzen 83,2 % das Internet, bei den über 60-Jährigen inzwischen 50,4 %.
Zugenommen hat auch die mobile Nutzung: Mittlerweile greifen 30,7 Mio. Nutzer (55 %) unterwegs auf Netzinhalte zu, fünf Prozent mehr als im Vorjahr. Die mobilen Internetnutzer sind im Schnitt an 6,3 Tagen pro Woche im Internet, die ausschließlich stationären Nutzer an durchschnittlich 5,1 Tagen pro Woche.

Anwender mit mobilem Internetzugang weisen die höchste Nutzungsintensität auf. Während die Gesamtbevölkerung dem Internet durchschnittlich 108 Minuten pro Tag widmet, sind es bei den Nutzern mobiler Endgeräte, wie Smartphones und Tablets, mit insgesamt 158 Minuten zurzeit 50 Minuten mehr. Gleiches gilt für die Nutzungsfrequenz: So liegt die tägliche Internetnutzung bei den mobilen Anwendern mit rund 90 % deutlich höher als bei den stationären Anwendern mit 59 %.
Diese Entwicklungen verdeutlichen, dass die Anzahl der Tatgelegenheiten und der potenziellen Opfer von Cybercrime gerade bei den Nutzern mobiler Endgeräte kontinuierlich zunimmt.

38 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2015“.

39 www.ard-zdf-onlinestudie.de.

3.2 INTERNET DER DINGE

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 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 beachtliche Rechenleistung und sind mit entsprechenden Betriebssystemen ausgestattet, welche oftmals eigens für die Geräte durch den Hersteller auf Basis von Open Source Code[40] entwickelt werden.
Oftmals 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. Lampen, Jalousien, Heizung, Garagentor etc.) und die gezielte Fernsteuerung der Funktionen, verbreitet sich ebenfalls fortwährend. Hierdurch eröffnen sich vielfältige neue Möglichkeiten zur Begehung von Straftaten (z. B. Deaktivierung der häuslichen Alarmanlage zur Vorbereitung von Einbrüchen).
Auch die fortschreitende Vernetzung in und von Kraftfahrzeugen eröffnet neue Angriffsgelegenheiten für Cyberkriminelle, z. B. durch die Manipulation interner Steuerbefehle von Kraftfahrzeugen. Erpressungen könnten ein Ziel solcher Manipulationen sein, indem Kraftfahrzeuge beispielsweise verschlossen oder sogar gestoppt werden und erst nach Zahlung von Lösegeld wieder freigegeben werden. Immer mehr Kraftfahrzeuge sind mittlerweile auch internetfähig und verfügen über handelsübliche Internetbrowser, die oft analog zu den intelligenten Endgeräten über keine oder nur unzureichende Schutzmechanismen verfügen und häufig veraltete Betriebssysteme/Software mit Sicherheitslücken nutzen.
Eine Studie geht davon aus, dass bis zum Jahr 2020 mehr als eine Billion internetfähiger Endgeräte weltweit mit dem Internet verbunden sein werden.[41]

3.3 INDUSTRIE 4.0

Die Entwicklung hin zum „Internet der Dinge“ beeinflusst auch die Entwicklungen im Unternehmenssektor. Die Nutzung privater mobiler Endgeräte („Bring your own device“[42])und Sozialer Netzwerke im Arbeitskontext nimmt stetig zu.
Der Trend des „Bring your own device“ birgt erhebliche Risiken. Die Vereinigung von privaten und beruflichen Internet- und Computeraktivitäten auf einem privaten Endgerät erleichtert es Cyberkriminellen, aufgrund der teilweise schwächeren Absicherung dieser Geräte auch auf Unternehmensdaten zuzugreifen. Hier werden Einfallstore für z. B. den Diebstahl geistigen Eigentums oder Wirtschaftsspionage geöffnet.
Ebenso gewinnt die elektronische und webbasierte Steuerung von Prozessen in Unternehmen 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 zum 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. Insbesondere die Gefahr der digitalen Erpressung dürfte für Unternehmen kontinuierlich zunehmen.

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

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

42 Mit Bring Your Own Device (BYOD) wird die Nutzung privater Endgeräte für berufliche Zwecke sowie deren Einbindung in Unternehmensnetze bezeichnet (Quelle: BSI - Die Lage der IT-Sicherheit in Deutschland 2014).

4 GESAMTBEWERTUNG UND AUSBLICK

Cybercrime ist ein transnationales Kriminalitätsphänomen. Das von Cybercrime ausgehende Gefährdungs- und Schadenspotenzial steigt. Mit der weiter zunehmenden Bedeutung der IT im privaten sowie professionellen Bereich erhöhen sich die Manipulations- und Angriffsmöglichkeiten.

Im Bereich von Cybercrime wird von einem stark ausgeprägten Dunkelfeld ausgegangen. Die polizeilichen Statistiken können lediglich einen kleinen Ausschnitt der tatsächlichen Dimension von Cybercrime abbilden und sind derzeit noch nicht im Stande, das Gesamtphänomen und das daraus resultierende Gefährdungspotenzial vollständig zu beschreiben. Trotz insgesamt rückläufiger registrierter Fallzahlen in der PKS kann deshalb nicht auf eine rückläufige Gefährdung durch Straftaten der Cybercrime geschlossen werden. Ermittlungsergebnisse deuten zudem darauf hin, dass Täter im Bereich Cybercrime sich zunehmend professionalisieren, indem sie ihre Vorgehensweise ständig verfeinern und aktuellen Gegebenheiten anpassen.

Wiederholte Datendiebstähle spektakulären Ausmaßes und die tägliche Betroffenheit jedes einzelnen Users, z. B. durch ständige Spam-Mails, bergen die Gefahr der Abstumpfung und Resignation und letztlich fehlender Sensibilität für die zwingende Notwendigkeit verstärkter, eigenverantwortlicher Präventivmaßnahmen zum Selbstschutz. Wo die Präventionsmaßnahmen versagen, ist eine konsequente Strafverfolgung Cyberkrimineller notwendig.

Eine effektive Prävention sowie nachhaltige ganzheitliche Bekämpfung von Cybercrime muss im Verbund der zuständigen Sicherheitsbehörden und in Kooperation mit den Wirtschaftsunternehmen erfolgen. Hierbei kommt der internationalen Zusammenarbeit eine zentrale Rolle zu.

Die bereits in den Vorjahren festgestellte Veränderung der Täterstrukturen 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 Einzeltäter mit umfassenden IT-Kenntnissen, sondern zunehmend auch Kriminelle ohne spezifische Fachkenntnisse, die für eine Tatbegehung erforderliches Know-how und Ressourcen käuflich erwerben bzw. für die Begehung der Straftaten in heterogenen Gruppen arbeitsteilig zusammenwirken.

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

Die von Cybercrime ausgehenden Gefahren für den Privat- und Wirtschaftsbereich sowie die Gesellschaft insgesamt werden weiter zunehmen.

Aktuelle Technologietrends, wie z. B. das „Internet der Dinge“, „Industrie 4.0“ oder auch die weiter ansteigende Nutzung des Internets durch den Privatanwender, dürften diese Entwicklung deutlich fördern, weil sie aus Täterperspektive neue Tatgelegenheiten und neue Tatgelegenheitsstrukturen eröffnen.

IMPRESSUM

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2015

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de