Bundeskriminalamt

Cybercrime

Bundeslagebild 2014

INHALT

1 VORBEMERKUNG

Das Lagebild informiert zu den Entwicklungen im Berichtszeitraum und beschreibt das Gefahren- und Schadenspotenzial von Cybercrime und deren Bedeutung für die Kriminalitätslage in Deutschland. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder mittels dieser Informationstechnik begangen werden.
Grundlage für den statistischen Teil des Lagebildes sind die Daten aus der Polizeilichen Kriminalstatistik (PKS). Das beinhaltet alle Straftaten, einschließlich der mit Strafe bedrohten Versuche, die polizeilich abschließend bearbeitet und an die Staatsanwaltschaft abgegeben wurden.
Mit Blick auf das sehr große Dunkelfeld in diesem Deliktsbereich bedarf es zur Einschätzung der Bedrohungslage auch der Einbeziehung externer Erkenntnisse, die das polizeilich-statistische Hellfeld anreichern. Phänomenologische Aussagen des Lagebildes 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

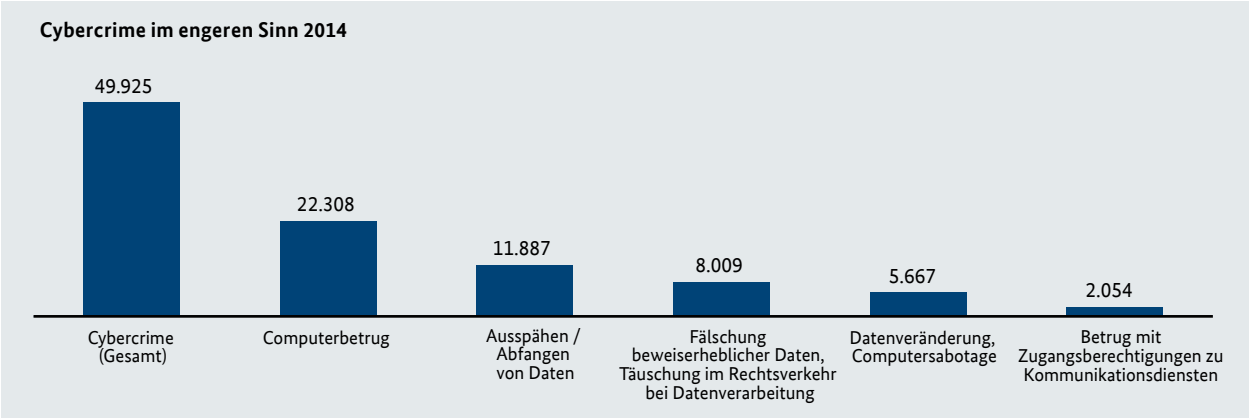
2.1 POLIZEILICHE KRIMINALSTATISTIK

In der PKS ist die Anzahl der auf Cybercrime entfallenden Straftaten für das Jahr 2014 gegenüber den Vorjahren im Bundesdurchschnitt deutlich geringer; zugleich sind die Aufklärungsquoten gestiegen.
Diese statistischen Aussagen sind auf veränderte Erfassungsmodalitäten in der PKS zurückzuführen: 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 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.
Die Zahlen der PKS bis 2013 zum Phänomen Cybercrime bilden insofern keine Bezugsgröße und keinen Vergleichsmaßstab für die Jahre ab 2014. Daher kann auf Grundlage der für das Jahr 2014 ausgewiesenen Zahlen nicht auf eine rückläufige Bedrohung durch Straftaten der Cybercrime geschlossen werden.
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 in zwei Jahren möglich sein.
Das Bundeslagebild Cybercrime stellt schwerpunktmäßig die im Jahr 2014 erfassten Fälle von Cybercrime im engeren Sinn dar. Diese umfassen alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten[01].

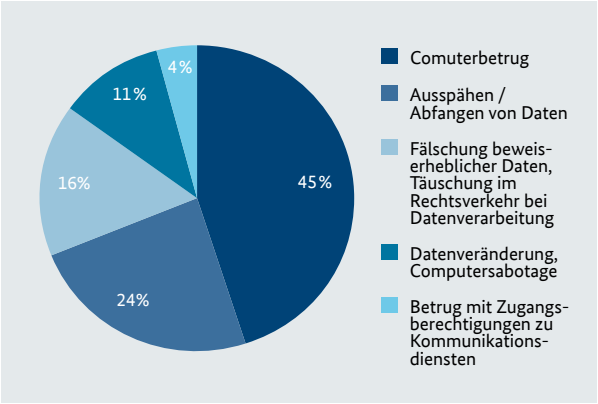
01 Umfasst die Delikte: Computerbetrug (PKS 517500), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900), Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (PKS 543000), Datenveränderung/ Computersabotage (PKS 674200) sowie Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen (PKS 67800).

Fallzahlen

Für das Jahr 2014 registriert die PKS insgesamt 49.925 Straftaten im Bereich Cybercrime im engeren Sinn.



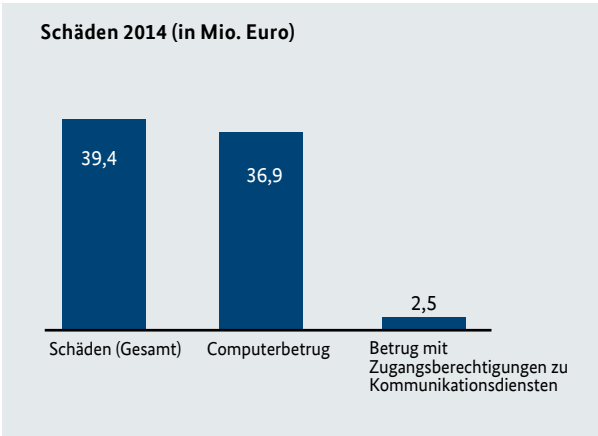
Bezogen auf die prozentuale Verteilung der einzelnen Phänomenbereiche ergibt sich folgendes Bild:



Einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking, Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch die vielfältigen anderen Erscheinungsformen der digitalen Erpressung (z. B. die sog. „Ransomware“) werden in der PKS nicht unter dem Begriff Cybercrime, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst. Insofern finden diese deliktischen Ausprägungen hier keine Berücksichtigung und sind in den Zahlen zum Tatmittel Internet enthalten.

Schäden

Bei Cybercrime im engeren Sinne werden Schäden nur bei den Delikten Computerbetrug (PKS 517500) und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900) registriert. Diese belaufen sich im Jahr 2014 auf rund 39,4 Mio. Euro. Davon entfallen rund 36,9 Mio. Euro auf den Bereich Computerbetrug und rund 2,5 Mio. Euro auf den Betrug mit Zugangsdaten zu Kommunikationsdiensten. Die Tatsache, dass zu lediglich zwei Deliktsbereichen eine statistische Schadenserfassung erfolgt, lässt keine belastbaren Aussagen zum tatsächlichen monetären (Gesamt-) Schaden durch Cybercrime zu.



02 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 2014).

03 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 („ransom“) gefordert.

Tatmittel Internet

Auch bezogen auf die PKS-Zahlen zum Tatmittel Internet gelten die gleichen Einschränkungen (siehe Seite 3) hinsichtlich der Vergleichbarkeit mit den Zahlen der Vorjahre.
Im Jahr 2014 wurden 246.925 Fälle erfasst, die unter Nutzung des Tatmittels Internet begangen wurden. Überwiegend handelte es sich hierbei um Betrugsdelikte (Anteil: 74,2 %; 180.826 Fälle), darunter vor allem der Warenbetrug (Anteil 40,8 %; 73.713 Fälle), also solche Fälle, bei denen der Täter über das Internet Waren zum Verkauf anbietet, sie jedoch entweder gar nicht oder in minderwertiger Qualität liefert. Dem Täter geht es dabei allein darum, den Käufer/das Opfer zu einer Zahlung ohne entsprechende Gegenleistung zu bringen.

2.2 DUNKELFELD

Bei Cybercrime ist von einem sehr großen Dunkelfeld auszugehen. Das heißt, dass vermutlich nur ein kleiner Teil der Straftaten in diesem Bereich zur Anzeige gebracht wird bzw. der Polizei und/oder den Strafverfolgungsbehörden bekannt ist.
Bereits 2013 hatte eine in Niedersachsen durchgeführte Dunkelfeldstudie ein Dunkelfeld von 91 % aller Cybercrimestraftaten errechnet[04].
Einer im Februar 2015 veröffentlichten repräsentativen Studie des Deutschen Instituts für Wirtschaftsforschung (DIW)[05] zufolge ist Deutschland mit jährlich 14,7 Millionen Fällen von Internetkriminalität[06] mit einem Gesamtschaden von 3,4 Milliarden Euro belastet, wobei alleine 84 % (rund 12,3 Millionen Fälle) auf die Bereiche „Phishing, Identitätsbetrug und Angriffe mittels Schadsoftware“ entfallen. Gemessen an der Zahl der in der PKS registrierten Straftaten im Bereich Cybercrime würde dies ein weitaus größeres Dunkelfeld bedeuten als ohnehin schon angenommen.
Ergänzend kommt hinzu, dass insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung

- eine große Anzahl der Straftaten aufgrund immer weiter verbreiteter technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinauskommt und von den Geschädigten nicht angezeigt wird, zumal meist kein finanzieller Schaden entsteht,
- Straftaten durch den Geschädigten nicht erkannt werden (die Infektion des Computers bleibt unentdeckt) oder
- der Geschädigte die erkannte Straftat in aller Regel nicht anzeigt, um beispielsweise im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner“ nicht zu verlieren.

Eine Aufhellung des Dunkelfeldes ist für die Strafverfolgungsbehörden jedoch sehr wichtig, um die Bekämpfung der Cybercrime zu optimieren. Hierzu zählt u.a. die Analyse durchgeführter Angriffe. Durch eine solche Analyse lassen sich nicht nur Angriffsvektoren und mögliche Tatzusammenhänge erkennen und daraus eventuell neue Ermittlungsansätze gewinnen, sondern auch Präventionsmaßnahmen ableiten, wie das Patchen[07] von betroffenen Systemen oder auch die Sensibilisierung der Nutzer/der Öffentlichkeit zu bestimmten, neuen Modi Operandi.
Nur ein möglichst umfassendes Bild zur Dimension und den Erscheinungsformen dieses Deliktsbereiches gibt den Strafverfolgungsbehörden die Möglichkeit, auf neue Entwicklungen schnell und zielgerichtet zu reagieren bzw. mittel- und langfristige Bekämpfungs- und Präventionsstrategien zu entwickeln. Dadurch sollen auch die Nutzer von informationstechnischen Systemen besser geschützt werden.

04 Bundeslagebild Cybercrime 2013 (www.bka.de)

05 DIW-Studie „Tatort Internet: Kriminalität verursacht Schäden in Milliardenhöhe“, (Riekmann, J., Kraus, M.; DIW Wochenbericht, 12.2015).

06 Internetkriminalität im Sinne der Studie umfasst die Bereiche Phishing, Identitätsbetrug, Waren- und Dienstleistungsbetrug und Angriffe mit Schadsoftware.

07 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 2014)

2.3 AKTUELLE PHÄNOMENE

Cybercrime-as-a-Service

Das Geschäftsmodell „Cybercrime-as-a-Service“ gewinnt mehr und mehr an Bedeutung. Die digitale Underground Economy[08] 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.:

- Bereitstellung von Botnetzen für verschiedenste 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 Underground Economy Foren,
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität,
- sog. Dropzones[09] zum Ablegen illegal erlangter Informationen und/oder Waren.

Diese Beispiele zeigen, dass Kriminelle auch ohne eigene technische Kenntnisse und mit vergleichsweise geringem Aufwand Zugang zu hochentwickelten Werkzeugen erhalten, 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 von Schadsoftware,
- Beratungsdienste,
- Anti-Erkennungsmechanismen,
- 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 die Schadsoftware bezüglich ihrer Erkennungsraten von aktuellen Cyber-Sicherheitsprodukten testen können. Hierdurch besteht die Möglichkeit, durch Änderungen an der Schadsoftware deren Erfolgsaussichten für eine „Verteileroffensive“ zu verbessern.

Diebstahl digitaler Identitäten

Unter digitaler Identität wird hier die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner personenbezogenen Daten und Aktivitäten innerhalb der Gesamtstruktur des Internets verstanden. Konkret beinhaltet dies auch alle Arten von Nutzer-Accounts, also zum Beispiel Zugangsdaten in den Bereichen:

- Kommunikation (E-Mail- und Messengerdienste),
- E-Commerce (Onlinebanking, Onlinebrokerage, 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.

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) Bestandteil der digitalen Identität.
Die digitale Identität als Ganzes ist oder zumindest Teile davon 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.
Um in den Besitz dieser Informationen zu gelangen, werden täterseitig häufig neben sog.„Trojanischen

08 Schattenwirtschaft: Globale virtuelle Schwarzmärkte im DarkDarknet (Definition siehe Kapitel Underground Economy (Seite 10)), über die Anbieter und Käufer ihre kriminellen Geschäfte rund um die digitale Welt anbahnen und abwickeln können

09 Definition siehe Kapitel Diebstahl digitaler Identitäten (Seite 6)

10 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 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 (Hintertür) zum Computer öffnen. (Quelle: BSI-Gefährdungskataloge)

Pferden“[10] auch andere Methoden unter Nutzung des Internets eingesetzt, wie z. B.:

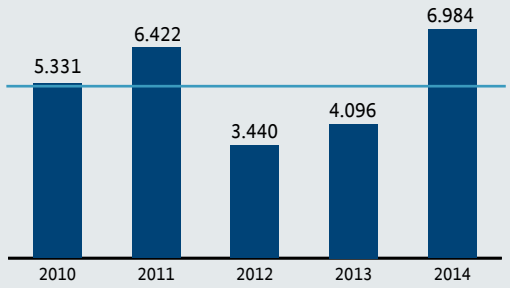
- Installation von Schadprogrammen über Drive-By-Exploits[11],
- Phishing,
- Einbruch auf Servern und Kopieren der Anmeldeinformationen,
- Einsatz von Keyloggern[12] oder Spyware[13].

Die gestohlenen Identitäten werden dann mittels der eingesetzten Schadsoftware meist automatisch in speziellen Speicherorten im Internet (sog. Dropzones) gesammelt, auf welche der/die Täter bzw. deren Auftraggeber zugreifen kann/können.
Dass digitale Identitäten bei Kriminellen begehrt sind, zeigen auch folgende Vorfälle:
Nachdem im Januar 2014 der Diebstahl von 16 Millionen E-Mail-Adressen bekannt geworden war, konnte die Staatsanwaltschaft Verden im März 2014 in einem von ihr geführten Ermittlungskomplex weitere 18 Millionen gestohlene E-Mail-Adressen nebst zugeordneten Passwörtern sicherstellen.
Anfang 2014 verschafften sich bislang unbekannte Täter Zugang zu einer Datenbank des Online-Händlers Ebay und erlangten dadurch Zugriff auf 145 Millionen Datensätze. Dazu gehörten persönliche Kundendaten wie Namen, verschlüsselte Passwörter, E-Mail-Adressen, Geburtstage, Adressen und Telefonnummern.

Phishing im Onlinebanking – erneuter Anstieg

Die bekannteste Variante des digitalen Identitätsdiebstahls ist das sog. „Phishing im Zusammenhang mit Onlinebanking“. Für das Jahr 2014 wurden dem Bundeskriminalamt 6.984 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2013 (4.096) bedeutet dies eine Zunahme der Fallzahlen um 70,5 %. Die Anzahl der Fallzahlen liegt deutlich über dem Durchschnitt der Fallzahlen der letzten fünf Jahre (5.255).

Fälle – Phishing im Onlinebanking 2010-2014



Nachdem u. a. durch (verschiedene Schutzmaßnahmen wie die verstärkte Nutzung) des mTAN-Verfahrens (auch bezeichnet als smsTAN)[14] als Sicherungsmethode im Onlinebanking sowie eine noch intensivere Sensibilisierung der Anwender eine annähernde Halbierung der Fallzahlen im Jahr 2012 erreicht werden konnte, haben sich die Fallzahlen seither mehr als verdoppelt.
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 Trojaner, die speziell auf den deutschen Bankensektor ausgerichtet sind und über das technische Potenzial verfügen, sowohl das iTAN- als auch das mTAN-Verfahren mittels sog. Echtzeitmanipu-

11 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).

12 Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen 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).

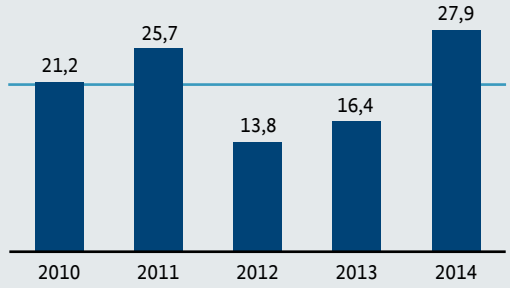
13 Wortschöpfung aus Spy (spionieren) und Software. Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können. (Quelle: www.bsi.bund.de, Glossar)

14 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.

15 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.

lation (Man-In-The-Middle-/Man-In-The-Browser-Attacken[15]) erfolgreich anzugreifen.
Entsprechende Schadsoftware zur Infizierung des vom jeweiligen Bankkunden genutzten Mobiltelefons wurde bereits am Schwarzmarkt platziert und ist für die meisten Smartphone-Betriebssysteme erhältlich. Hier zeigen sich keine grundlegenden Änderungen hinsichtlich der eingesetzten Schadsoftware gegenüber dem Vorjahr.
Diese Entwicklung zeigt, dass die Täterseite jederzeit in der Lage ist, mit verbesserten Sicherheitsmechanismen im Onlinebanking, wenn auch mit zeitlicher Verzögerung, Schritt zu halten.
Hierzu setzen die Täter jedoch nicht nur auf technische Lösungen, sondern versuchen mittels sogenannten Social Engineerings[16] an die notwendigen Kundeninformationen zu kommen, um die mittlerweile weitgehend in Deutschland verwendeten Autorisierungsmechanismen im Onlinebanking, die ein aktives Handeln/Zutun des Kontoberechtigten erfordern (unter Nutzung eines zweiten Kommunikationskanals, „Two-factor authentication"), auszuhebeln und für die eigenen Zwecke zu nutzen. Bekanntestes Beispiel ist der Versand von E-Mails in vertrauenserweckender Aufmachung mit der Aufforderung, aus bestimmten Gründen vertrauliche Informationen preiszugeben.
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 2014 rund 4.000 Euro pro Fall. Auf dieser Berechnungsgrundlage wurden im Jahr 2014 Schäden in Höhe von 27,9 Mio. Euro versursacht, deutlich mehr als der durchschnittliche Schaden in den letzten fünf Jahren (21,0 Mio. Euro). Demzufolge ergeben sich unter Berücksichtigung der dem Bundeskriminalamt in den letzten fünf Jahren gemeldeten Fallzahlen folgende ungefähre Schäden:

Schäden – Phishing im Onlinebanking 2010-2014 (in Mio. Euro)



Botnetze

Sogenannte Botnetze spielten auch im Jahr 2014 im Bereich Cybercrime 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 dabei für den Besitzer unbemerkt auf verschiedene Art und Weise, sei es durch Öffnung eines infizierten E-Mail-Anhanges oder auch mittels „Drive-by-Infection"[17].
Eine weitere Variante ist die Verteilung der Schadsoftware über Soziale Netzwerke (z. B. Facebook). Den Teilnehmern der Netzwerke werden von vermeintlichen Bekannten Nachrichten mit infizierten Anhängen zugesandt. Wenn diese aufgrund des mutmaßlich bestehenden Freundschaftsverhältnisses gutgläubig geöffnet werden oder entsprechende Links aktiviert werden, führt dieses zur Infektion des Computers. In der Folge hat der Täter durch die Installierung von Schadsoftware einen nahezu vollständigen Zugriff auf den infizierten Computer des Opfers.
Weitere Verbreitungskanäle sind das Usenet[18] und Tauschbörsen / P2P (Peer to Peer)-Netze[19], in denen die Schadsoftware meist als Video- oder Sounddatei getarnt und zum Download angeboten wird.

16 Soziale Manipulation – Beeinflussung einer Person zur Preisgabe vertraulicher Informationen. Bei Cyber-Angriffen 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 2014)

17 Infektionen, die durch Drive-by-Exploits verursacht werden (siehe Fussnote 11, Seite 7).

18 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, die Newsgroups, an denen grundsätzlich jeder teilnehmen kann.

19 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).

Botnetze und ihre Kapazitäten stellen nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy dar. Die „Bot-Herder“[20] vermieten Bots, durch die mittels DDoS-Attacken gezielte Angriffe z. B. auf die Server eines Unternehmens durchgeführt werden, massenweise Spam-Mails versendet werden oder auch gezielte Datendiebstähle erfolgen können.
Seriöse Angaben zur Gesamtzahl der in Deutschland bzw. weltweit in Botnetzen zusammengeschlossenen Rechner sind nur sehr schwer möglich:

- Im seinem Jahresbericht 2014 spricht das BSI von mehr als einer Million Internetrechnern in Deutschland, die Teil eines Botnetzes sind.
- Der Verband der deutschen Internetwirtschaft e.V. (ECO)[21] berichtet in seiner Jahresstatistik, dass im Jahr 2014 der Anteil der mit Botnetz-Schadsoftware infizierten Systeme bei 40 % lag und damit um sieben Prozent höher als im Jahr 2013 (33 %).

Im November 2014 gelang dem BKA die Identifizierung und Zerschlagung eines Botnetzes mit bis zu 11.000 Computersystemen in über 90 Staaten, wobei sich mehr als die Hälfte der infizierten Systeme in Deutschland befand. Parallel zu den weiteren Ermittlungen wurden in Zusammenarbeit mit dem BSI, dem Fraunhofer-Institut (FKIE) sowie zwei deutschen Antivirenherstellern die Benachrichtigung der vom Botnetz betroffenen Computerinhaber über ihre Provider veranlasst. Die Geschädigten erhielten auf den Internetseiten des BKA und des BSI weitere Informationen zur Infektion, eine Hilfestellung bei der Bereinigung der infizierten Rechner sowie Hinweise zur Anzeigenerstattung.

DDoS

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. Eine im Herbst 2014 von der Allianz für Cyber-Sicherheit veröffentlichte Umfrage ergab, dass mehr als ein Drittel der befragten Unternehmen in den letzten drei Jahren Ziel eines DDoS-Angriffs auf ihre Webseiten geworden ist.
Polizeiliche Daten zur Dimension (Anzahl, Dauer usw.) liegen nicht vor. Das BSI berichtet in seinem schon zuvor erwähnten Jahresbericht von 32.000 DDoS-Angriffen in Deutschland im Jahr 2014.
Gerade im wettbewerbsintensiven Marktsegment Internet können Nichterreichbarkeiten von Vertriebsportalen zu schwerwiegenden wirtschaftlichen Nachteilen bzw. Schäden führen. Die Motivlage der Täterseite reicht von politisch/ideologischen Gründen über Rache und Erlangung von Wettbewerbsvorteilen bis hin zu reinen monetären Gründen (Erpressung).
Die durch DDoS-Angriffe verursachten Schäden bzw. Kosten für den Geschädigten lassen sich nur schwer in monetären Dimensionen ausdrücken, 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 bezifferbar sind.

Schadprogramme (allgemein)

Schadprogramme, d. h. Software, über die ein Angreifer zumindest teilweise die Kontrolle über ein Endsystem erreichen will, sei es zum Ausspähen digitaler Identitäten oder auch zur Durchführung sogenannter „digitaler Erpressungen“, spielen nach wie vor eine zentrale Rolle bei der Begehung von Straftaten im Bereich Cybercrime.
Die häufigsten Verbreitungswege von Schadprogrammen sind Anhänge in Spam-Mails, Drive-by-Exploits und Botnetze.
Valide Daten zur Verbreitung von Schadprogrammen liegen nur sehr begrenzt vor. Schätzungen zu Folge hat die Gesamtzahl der PC-basierten Schadprogrammvarianten mittlerweile die 250-Millionen-Marke überschritten, wobei deren Anzahl täglich um rund 300.000 Varianten steigt. In Deutschland ereignen sich jeden Monat mindestens eine Million Infektionen durch Schadprogramme. Bezogen auf mobile Endgeräte wie Smartphones und Tablets gehen die Schätzungen von mindestens drei Millionen Schadprogrammen aus[24].

20 Herder (englisch) – Hirte

21 www.eco.de

22 Distributed Denial of Service (vgl. Fußnote 2 Seite 4)

23 www.allianz-fuer-cybersicherheit.de

24 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2014“

Ransomware

Digitale Erpressung mittels sogenannter „Ransomware“ ist auch in Deutschland weit verbreitet. Entsprechende Schadsoftware oder auch die gesamte „Dienstleistung“ kann in einschlägigen Foren der Underground Economy erworben werden, sodass kein besonderer IT-Sachverstand für eine digitale Erpressung mehr erforderlich ist.

Grundsätzlich muss hier zwischen zwei Varianten unterschieden werden:

a) Ransomware, die keine Verschlüsselung der Festplatte, sondern lediglich eine Manipulation des Betriebssystems verursacht und deren Bereinigung unter Nutzung der im Internet verbreiteten Anleitungen vergleichsweise einfach ist. Die wohl bekanntesten Ausprägungen sind der sogenannte „BKA-Trojaner“ und der „GVU-Trojaner“, bei denen Namen und Logos missbraucht wurden, um der kriminellen Zahlungsaufforderung einen offiziellen Charakter zu verleihen.[25]

b) Ransomware, die die Daten auf Endsystemen oder Servern tatsächlich verschlüsselt, und der Zugriff auf die Daten, wenn überhaupt, nur durch Zahlung des geforderten „Lösegeldes“ zurückerlangt werden kann. Diese Variante ist weitaus gefährlicher, da es in den meisten Fällen keinen anderen Weg gibt, die verschlüsselten Daten wiederzuerlangen bzw. die verschlüsselten Daten trotz Zahlung des geforderten „Lösegeldes“ nicht wiedererlangt werden können.

Für das Jahr 2014 wurden dem BKA lediglich 545 Fälle von digitaler Erpressung gemeldet, was gegenüber dem Vorjahr (6.048 Fälle) einen Rückgang um 91,0 % bedeutet.
Die Entwicklung deckt sich im Wesentlichen mit den Feststellungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Bezug auf Anfragen von Bürgerinnen und Bürgern, die Opfer von Ransomware-Angriffen geworden sind. Während das BSI-Service-Center für das Jahr 2013 mehr als 8.500 Anfragen registrierte, waren es im Jahr 2014 nur noch knapp 1.200 Anfragen.[26]
Möglicher Erklärungsansatz für diese Entwicklung ist, dass die unter Variante a) beschriebene Ransomware kaum noch eingesetzt wird bzw. durch die umfangreiche Öffentlichkeitsarbeit und mediale Berichterstattung die betroffenen Nutzer entsprechend sensibilisiert sind. Diese leisten keine Zahlungen mehr und nutzen die vielfältig im Internet verbreiteten Anleitungen zur Bereinigung der befallenen Systeme. Somit dürfte diese Variante von Ransomware nicht mehr die erwünschte Wirkung (finanzielle Gewinne) erzielen und den Einsatz bzw. die Nutzung aus Sicht der Täterseite unattraktiv machen.
Darüber hinaus dürfte diese Selbsthilfe sich auf das Anzeigeverhalten der Betroffenen auswirken, da ihnen weder ein materieller noch erheblicher immaterieller Schaden entstanden ist und keine Veranlassung zur Erstattung einer Strafanzeige besteht.
Denkbar ist auch, dass viele Erpressungsversuche mittels Ransomware bereits im Versuchsstadium scheitern, da sich die Schadsoftware aufgrund technischer Maßnahmen des Nutzers, wie z. B. regelmäßige System- und Programmupdates, nicht auf dessen System installieren kann.

Underground Economy

Die Foren oder illegalen Marktplätze der sog. digitalen Underground Economy spielen zunehmend eine zentrale Rolle bei der Begehung von Straftaten im Bereich Cybercrime. Die Foren dienen hauptsächlich der Kommunikation der 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 sog. Darknet[27] kriminelle Marktplätze betrieben, in denen man im Schwerpunkt illegale Waren erwerben kann. Die Angebote umfassen dabei u.a. Drogen, Waffen, Falschgeld, gefälschte Ausweise, gestohlene Kreditkartendaten oder gefälschte Markenartikel.
Zur Bezahlung dieser Waren werden ausschließlich digitale Kryptowährungen, wie z.B. Bitcoin, 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 des Treuhandsystems ermöglicht dieses den als „Treuhändern“ agierenden Kriminellen, das ihnen anvertraute Geld aus allen laufenden Transaktionen des Marktplatzes zu unterschlagen und danach „unterzutauchen“ („exit scam“).
Insbesondere im Bereich der Underground Economy lässt sich eine zunehmende Verlagerung von Delikten aus der analogen in die digitale Welt beobachten. Ausschlaggebend für diese Entwicklung dürfte nicht nur die erhöhte Anonymität sein, sondern auch der Umstand, dass über diese illegalen Online-Markplätze weltweit eine Vielzahl von potentiellen Kunden erreicht werden kann und diese Foren und Marktplätze im Darknet einfach und ohne tiefergehende Computerkenntnisse erreichbar sind.

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

26 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2014“

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

2.4 TÄTERSTRUKTUREN

Der überwiegende Teil der Cyberkriminellen handelt aus finanzieller Motivation. Dabei reicht die Palette vom klassischen Einzeltäter bis hin zu international organisierten Tätergruppierungen.
Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Angeboten wird dabei in der Underground Economy die zur Begehung von Straftaten erforderliche Schadsoftware bis hin zu kompletten technischen Infrastrukturen.
Ermittlungsverfahren belegen diese „Dienstleistungsorientierung“ und Spezialisierung und zeigen die Dimension der zu erzielenden kriminellen Erträge auf.
Im Jahr 2014 wurden Ermittlungen gegen die Betreiber und Mitglieder eines Forums innerhalb der Underground Economy geführt. Das Forum, eine Kommunikations- und Handelsplattform, beinhaltete Informationen über Techniken zum Ausspähen von Daten, Schadcode-Programmierung und das Vorgehen bei Warenkreditbetrugsdelikten. Auf der Handelsplattform wurde u.a. mit illegal erlangten Daten, Betäubungsmitteln und gefälschten Kreditkarten gehandelt. Die Mitarbeiter des Forums hatten sich, neben der Bereitstellung der IT-Plattform, aktiv an der Verwirklichung der Straftaten einzelner Mitglieder beteiligt, indem sie ein Treuhandsystem aufbauten, welches die ordnungsgemäße Durchführung der illegalen Dienstleistungen förderte und unterstützte.
Im Rahmen der Ermittlungen wurde darüber hinaus festgestellt, dass einige Beschuldigte Schadsoftware einsetzten, um fremde Rechner zu kompromittieren. Ca. 500 Geschädigte konnten namentlich identifiziert und über die zuständigen Polizeidienststellen entsprechend informiert werden.
Insgesamt wurden fünf Täter ermittelt; die erzielten kriminellen Erträge dürften über einer Million Euro liegen.

Im Bereich der Organisierten Kriminalität (OK) ist hinsichtlich der Betätigung von Tätergruppierungen im Deliktsfeld Cybercrime im Vergleich zum Vorjahr eine Steigerung feststellbar. Waren 2013 noch sechs OK-Gruppierungen mit Hauptaktivitätsfeld Cybercrime registriert worden, so wurden 2014 insgesamt 12 OK-Gruppierungen mit Hauptaktivitätsfeld Cybercrime festgestellt. Gemessen an der Gesamtzahl der im Jahr 2014 registrierten OK-Gruppierungen (571) bewegt sich der Anteil der im Bereich Cybercrime tätigen OK-Gruppierungen zwar auf einem relativ niedrigen Niveau, jedoch ergeben sich zumindest Hinweise darauf, dass Täterstrukturen, die der Organisierten Kriminalität zuzurechnen sind, zunehmend auch im Bereich Cybercrime aktiv sind.

3 BEDROHUNGS- UND GEFÄHRDUNGSPOTENZIAL

Die Intensität der kriminellen Aktivitäten im Bereich Cybercrime hat zugenommen, was zwangsläufig zu einer Steigerung der Bedrohungslage und damit einhergehend auch zu einer weiter zunehmenden Gefährdung von Privaten, Unternehmen und staatlichen Einrichtungen führt.
Wesentlichen Einfluss auf die weitere Entwicklung der Bedrohungs- und Gefährdungslage haben dabei die sich den Cyberkriminellen bietenden Tatgelegenheiten.

79 Prozent der Deutschen online

Die ARD-ZDF-Onlinestudie 2014 [28] hat ergeben, dass 79,1 % der Erwachsenen in Deutschland (2013: 77,2 %) online sind. Dies entspricht 55,6 Millionen Personen ab 14 Jahren (2013: 54,2 Millionen). Die höchsten Zuwachsraten gibt es weiterhin bei den über 60-Jährigen, von denen inzwischen fast jeder Zweite das Internet nutzt (45 %). Bei den 60- bis 69-Jährigen stieg der Anteil der Internetnutzer binnen Jahresfrist von 59 % auf 65 %.
Durchschnittlich ist ein Internetnutzer in Deutschland an 5,9 Tagen wöchentlich online und verbringt täglich 166 Minuten im Netz. Zur Einwahl ins Netz stehen jedem Onliner im Schnitt 2,8 Endgeräte zur Verfügung.
Beliebtester Zugang war 2014 erstmals der Laptop (69 %) vor Smartphone und Handy (60 %) und dem stationären PC (59 %). Wachstumstreiber für die mobile Nutzung sind vor allem die Tablet-PCs: Der Anteil der Onliner, die über Tablets Internetinhalte abrufen, stieg von 16 % auf 28 %.
Diese Entwicklungen bedeuten, dass die Anzahl der potentiellen Opfer von Cybercrime immer weiter zunimmt.

Mobile Endgeräte – 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 Millionen Bundesbürger (ab 14 Jahre) ein Smartphone, was einer Zunahme von rund zwei Millionen innerhalb der letzten sechs Monate entspricht [29]. 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 %).

Die steigende Verbreitung sowie die teilweise immer noch mangelnde Sensibilität der Nutzer hinsichtlich der digitalen Gefahren im Umgang mit diesen mobilen Endgeräten sorgen für eine weiterhin hohe Attraktivität für die Täterseite. Dies zeigt sich u. a. auch in der Zunahme der für Smartphones programmierten Schadprogramme.
Ein wesentlicher Aspekt dabei 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 Transaktionen im Onlinebanking, Zugriff auf E-Mail-Konten und soziale Netzwerke oder auch Aktivitäten im Bereich 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.

28 www.ard-zdf-onlinestudie.de

29 www.bitkom.org; Umfrage vom Februar 2015

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. Solche intelligenten Endgeräte sind beispielsweise Kühlschränke, Fernseher oder Router aber auch Sensoren, über die andere Geräte via Internet per Smartphone oder Tablet gesteuert werden können (Waschmaschinen, Glühbirnen, Kaffeemaschinen, etc.). Diese Geräte verfügen in der Regel über eine nicht zu unterschätzende Rechenleistung und sind mit entsprechenden Betriebssystemen ausgestattet, welche oftmals eigens für die Geräte durch den Hersteller auf Open Source Code Basis[30] entwickelt werden.
In der Regel verfügen diese sogenannten „intelligenten Endgeräte“ über keine oder nur unzureichende Schutzmechanismen und nutzen häufig veraltete Software mit Sicherheitslücken. Für Cyberkriminelle sind solche Geräte also relativ leichte Beute, wobei Infektionen für die Benutzer kaum feststellbar sind.
Das sogenannte „Smart Home“, d.h. die Vernetzung von Haustechnik und Haushaltsgeräten (z.B. Lampen, Jalousien, Heizung, Garagentor, etc.) und die gezielte Fernsteuerung der Funktionen verbreiten sich ebenfalls fortwährend.
Auch die fortschreitende Vernetzung in und von Kraftfahrzeugen nimmt stetig zu, wodurch sich auch die Angriffsflächen für Cyberkriminelle auf interne Steuerbefehle von Kraftfahrzeugen vergrößern. Immer mehr Kraftfahrzeuge sind mittlerweile auch internetfähig und verfügen über handelsübliche Internetbrowser.

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“)[31] und Sozialer Netzwerke im Arbeitskontext nimmt stetig zu.
Der Trend des „Bring your own device“ birgt 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. Wirtschaftsspionage oder Diebstahl geistigen Eigentums geöffnet.

Ebenso gewinnt die elektronische und webbasierte Steuerung von Prozessen in Unternehmen immer mehr an Bedeutung. Die zunehmende Vernetzung, die Abhängigkeit vernetzter, sich selbst steuernder Produktionsprozesse und Logistikketten von der Verfügbarkeit der Netze und die Problematik der Trennung/Abschottung dieser Netze zum Internet, stellen dabei eine große Herausforderung dar.
Die Folge dieser Entwicklung ist eine steigende Abhängigkeit der Unternehmen von der Informationstechnik. Daraus resultiert ein sehr hohes Bedrohungspotenzial für die Wirtschaft. Eine Schädigung der IT-Infrastruktur von Unternehmen kann mittlerweile nicht mehr nur zur Störung der Kommunikation führen, sondern vielmehr auch zum kompletten Produktionsstillstand, was enorme Verluste für Unternehmen nach sich ziehen würde.
Insbesondere die Gefahr der digitalen Erpressung von Unternehmen steigt dadurch.

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

31 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 transnationale Kriminalität. Das vom Phänomenbereich Cybercrime ausgehende Gefährdungs- und Schadenspotenzial ist weiter gestiegen. Mit der weiter steigenden Bedeutung der IT im privaten wie professionellen Einsatz erhöhen sich auch die Manipulations- und Angriffsmöglichkeiten für Cyberkriminelle.

Das sehr große Dunkelfeld zeigt, dass polizeiliche Statistiken lediglich einen kleinen Ausschnitt der tatsächlichen Dimension von Cybercrime abbilden und daher nicht ausreichen, um das Gesamtphänomen und das daraus resultierende Gefährdungs- und Bedrohungspotenzials vollständig zu beschreiben.

Die bereits in den Vorjahren festgestellte Veränderung der Täterstrukturen hat sich im Berichtsjahr fortgesetzt. Die Täter begehen heute nicht mehr nur die Straftaten im eigentlichen Sinne, sondern bieten vielmehr die zur Begehung von Straftaten erforderliche Schadsoftware oder gar komplette technische Infrastrukturen in der Underground Economy an. Diese Werkzeuge sind aufgrund ihrer einfachen Handhabung auch für Täter ohne fundierte IT-Spezialkenntnisse nutzbar. Es agieren daher nicht mehr nur hoch spezialisierte Einzeltäter mit umfassenden IT-Kenntnissen, sondern vermehrt auch Kriminelle ohne spezifische Fachkenntnisse, die für die Begehung der Straftaten arbeitsteilig zusammenwirken. Dabei gewinnen organisierte Täterstrukturen zunehmend an Bedeutung, also solche Strukturen im Sinne der „klassischen OK“, welche sich zur Begehung von Straftaten dauerhaft zusammengeschlossen haben. Diese Entwicklung dürfte weiter fortschreiten.

Eine wirkungsorientierte, nachhaltige Bekämpfung von Cybercrime muss im Sinne eines ganzheitlichen Ansatzes, d. h. im Verbund der zuständigen Sicherheitsbehörden und in Kooperation mit der Privatwirtschaft erfolgen. Hierbei kommt der internationalen Zusammenarbeit eine wesentliche Rolle zu.

Zusammenfassend ist davon auszugehen, dass die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren in ihrem Ausmaß und in ihren Ausprägungen weiter zunehmen werden, wobei aktuelle Entwicklungen wie z.B. das „Internet der Dinge“, „Industrie 4.0“ oder auch die weiterhin ansteigende Nutzung des Internets durch den Privatanwender einen wesentlichen Einfluss haben dürften. Hieraus ergeben sich mehr Tatgelegenheiten und neue Tatgelegenheitsstrukturen, was zu einer weiteren Steigerung des Bedrohungs- und Gefährdungspotenzials führt.

IMPRESSUM

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2014

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de