Thüringer Polizei Landeskriminalamt

www.thueringen.de/th3/polizei/lka

Cybercrime

Lagebild für Thüringen 2017

Impressum

Herausgeber:
Freistaat Thüringen,
Landeskriminalamt Thüringen,

Kontakt:
Landeskriminalamt Thüringen
Kranichfelder Straße 1
99097 Erfurt

Ansprechpartner:
Herr Nolte
Tel.: +49 361 341 - 1164
Fax: +49 361 341 - 1731
E-Mail: cybercrime.lka@polizei.thueringen.de
Internet: www.thueringen.de/de/lka/

Stand:
Mai 2018

Inhalt

1 Vorbemerkung

Cybercrime umfasst alle Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richtet. Cybercrime sind in diesem Zusammenhang auch Straftaten, die mittels Informationstechnik begangen werden[1].

Eine Eingrenzung erfolgt durch die sog. Cybercrime im engeren Sinne (Cybercrime i. e. S.). Hierbei handelt es sich um alle Delikte, bei denen Informations- und Kommunikationstechnik in den Tatbestandsmerkmalen einer Strafrechtsnorm enthalten sind. Zunehmend sind auch Straftaten, bei denen zu deren Begehung Informationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

Das Lagebild Cybercrime 2017 für den Freistaat Thüringen wurde in Anlehnung an das Bundeslagebild des Bundeskriminalamtes erstellt. Eine Betrachtung der Cybercrime für den Freistaat Thüringen ist zum Zwecke einer repräsentativen Darlegung der Phänomenologie unumgänglich. Hierbei gilt es die Entwicklungen im transnationalen Kontext der Phänomenologie in die Betrachtung mit einzubinden. Die Erscheinungsformen aus dem Bereich der Cybercrime treten weltweit ähnlich bzw. gleichgelagert auf. Zur rechtzeitigen Erkennung phänomenologischer Trends ist der Blick auf transnationale Entwicklungen auch für die Cybersicherheit im Freistaat Thüringen unumgänglich.
Das Lagebild Cybercrime 2017 für den Freistaat Thüringen wurde des Weiteren auf Grundlage der Polizeilichen Kriminalstatistik (PKS) und im Rahmen einer polizeiinternen Auswertung mittels des Recherche-Tools FINDUS erstellt. Es stellt eine Ergänzung zum Bundeslagebild Cybercrime des BKA dar. Folgende Schwerpunkte sind daher an dieser Stelle nicht allumfassend dargestellt, sondern können dem Bundeslagebild entnommen werden:

- Erfassungskriterien der PKS und die Auswirkungen auf die Darstellung des Lagebilds

[1] Definition nach Beschluss des Arbeitskreises II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 17./ 18.10.12

- Auswertung weiterer, außer der hier aufgeführten externen Quellen und weitere Dunkelfeldforschung
- Erläuterungen und Darstellung weiterer ausgewählter Phänomene
- weitere Ausführungen zum Gefahren- und Schadenspotential
- Gesamtbewertung der Kriminalitätslage und Ausblick auf die zukünftige Entwicklung

Das BKA hat im Lagebild 2016 festgestellt, dass der Großteil der Cybercrime-Delikte nicht zur Anzeige gebracht wird. Auf Grund dieses Umstandes ist eine allumfassende Einschätzung des Gefahrenpotentials des Phänomens zum gegenwärtigen Zeitpunkt nicht möglich. In einer repräsentativen Studie ermittelte das Deutsche Institut für Wirtschaftsforschung (DIW) für das Jahr 2015 insgesamt 14,7 Millionen Fälle von Cybercrime in Deutschland, während das Bundeskriminalamt für den gleichen Zeitraum 45.793 Cybercrime-Delikte i. e. S. im gesamten Bundesgebiet benannte. Das Bundeslagebild 2016 zeigte bereits ein Jahr später 82.649 Fälle der Cybercrime i. e. S. auf.

Es ist davon auszugehen, dass neben diesen Fallzahlen auch die Dunkelziffer des Phänomenbereichs innerhalb dieses Zeitraumes weiterhin stark angestiegen ist. Von einer Stagnation bzw. einem Rückgang der Fallzahlen ist auch für das Jahr 2017 nicht auszugehen. Eine Dunkelfeldforschung für den Freistaat Thüringen, die eine repräsentative Darstellung des Phänomens Cybercrime ermöglichen könnte, existiert zum gegenwärtigen Zeitpunkt nicht. Diesbezüglich können jedoch aus Forschungsergebnissen, die in Deutschland bereits vorliegen, Parallelen für die Lage in Thüringen gezogen werden. Eine durchgeführte Studie in Mecklenburg-Vorpommern offenbarte hierbei ein Dunkelfeld von 99,2 Prozent im Bereich der Cybercrime[2].

Der Blick auf den seitens des Cyber Security-Dienstleisters *Symantec Corporation* veröffentlichten *Norton Cyber Security Insight Report 2017* zeigt auf, welche Ausmaße der Phänomenbereich Cybercrime abseits der Definition der Cybercrime i. e. S. mittlerweile genommen hat. *Symantec* ist Mitglied des *German Competence Centers against Cyber Crime* (G4C), dessen Kooperationspartner das BKA ist. *Symantec* betrachtet in seinem

[2] Landeskriminalamt Mecklenburg-Vorpommern/ FH Güstrow/ Universität Greifswald (2017): Erste Untersuchung zum Dunkelfeld der Kriminalität in Mecklenburg-Vorpommern

Report auch Delikte, wie bspw. Cyber-Bullying[3], die zwar nicht der Cybercrime i. e. S. entsprechen, jedoch Tathandlungen sind, die ausschließlich unter Nutzung des Internets begangen werden können.

Dieser Report offenbart zudem das Ausmaß der Betroffenheit von Cybercrime in der Bevölkerung. So sind in Deutschland 38 Prozent aller Verbraucher laut der Auslegung von Cybercrime durch *Symantec* von der Phänomenologie betroffen.

Eine seitens des *Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom e. V.)* veröffentlichte Studie geht von einem noch größeren Ausmaß der Betroffenheit von Cybercrime in der deutschen Bevölkerung aus. Demnach waren 47 Prozent aller Privatpersonen im Jahr 2015 Opfer von Cybercrime. Die Umfragen der *Allianz für Cybersicherheit*[4] offenbaren ein stetig wachsendes Gefahren- und Schadenspotential durch Cybercrime. Waren 2015 noch 58,5 Prozent aller befragten Institutionen von Cyber-Attacken betroffen, waren es 2016 bereits 65,6 Prozent und 2017 gar 70 Prozent. Von einem derartigen Ausmaß der Betroffenheit ist in diesem Zusammenhang auch im Freistaat Thüringen auszugehen.

2 Polizeiliche Kriminalstatistik (PKS)

Die in der PKS erfassten Cybercrime-Delikte i. e. S. können auf Grund der Erfassungskriterien keine Grundlage für ein realistisches Lagebild sein. In der PKS werden Straftaten der Cybercrime nur erfasst, wenn konkrete Anhaltspunkte dafür bestehen, dass eine Tathandlung nachweislich innerhalb von Thüringen begangen wurde. Fand die ursprüngliche kriminelle Handlung dagegen im Ausland statt und ist lediglich die schädigende Folge in Thüringen eingetreten, werden solche Taten nicht in der PKS erfasst. Folglich besteht eine nicht unwesentliche Diskrepanz in den Deliktszahlen zwischen der PKS und den tatsächlich angezeigten und von der Polizei bearbeiteten Fällen der Cybercrime. Letztere liegt deutlich höher. Die PKS ist generell nicht in der Lage den hohen Anteil von Cybercrime-Delikten abzubilden, die aus dem Ausland begangen wurden. Durch

[3] Form der Verleumdung, Belästigung, Bedrängung und/oder Nötigung anderer Menschen, Unternehmen oder öffentlichen Organisationen mit Hilfe von Informations- und Kommunikationstechnologie über das Internet

[4] Initiative des BSI in Zusammenarbeit mit Bitkom e. V.: Zusammenschluss aller wichtigen Akteure im Bereich der Cybersicherheit; gegenwärtig 2.581 Institutionen aus privaten und öffentlichen Sektor

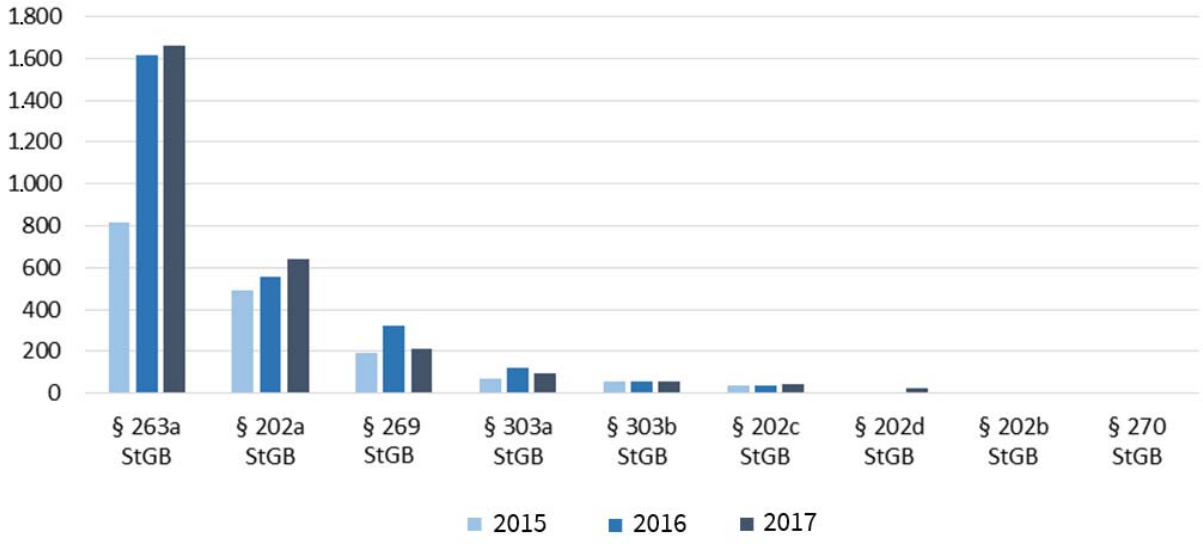
die Kommission Kriminalitätsbekämpfung (KKB) wurden entsprechende Möglichkeiten der Erfassung zuletzt geprüft, sind jedoch auf Bundes- und Landesebene noch nicht umgesetzt.

Zur Planung, Vorbereitung oder auch Ausführung werden in mittlerweile nahezu allen Deliktsbereichen Mittel der digitalen Datenverarbeitung eingesetzt. Hierzu können als Beispiele der Vertrieb von Waffen, Betäubungsmitteln oder strafbaren Dienstleistungen auf illegalen Marktplätzen, der Tausch kinderpornografischer Schriften, Erpressungshandlungen oder Urheber- und Markenrechtsverletzungen benannt werden. Derartige strafbare Handlungen werden in der PKS unter der Sonderkennung „Tatmittel Internet“ zusammengefasst.

2.1 Cybercrime im engeren Sinne

Auch im Jahr 2017 ist ein weiterer Anstieg der Cybercrime i. e. S. festzustellen. In den meisten Delikten der Cybercrime i. e. S. haben die Fallzahlen im Vergleichszeitraum von 2015 bis 2017 kontinuierlich zugenommen. Die folgende Darstellung zeigt die Entwicklung der Fallzahlen der einzelnen Delikte der Cybercrime i. e. S. in Thüringen seit dem Jahr 2015 im Vergleich lt. PKS[5].

Fallzahlen der Cybercrime i. e. S. in Thüringen im Vergleich 2015 - 2017 lt. PKS



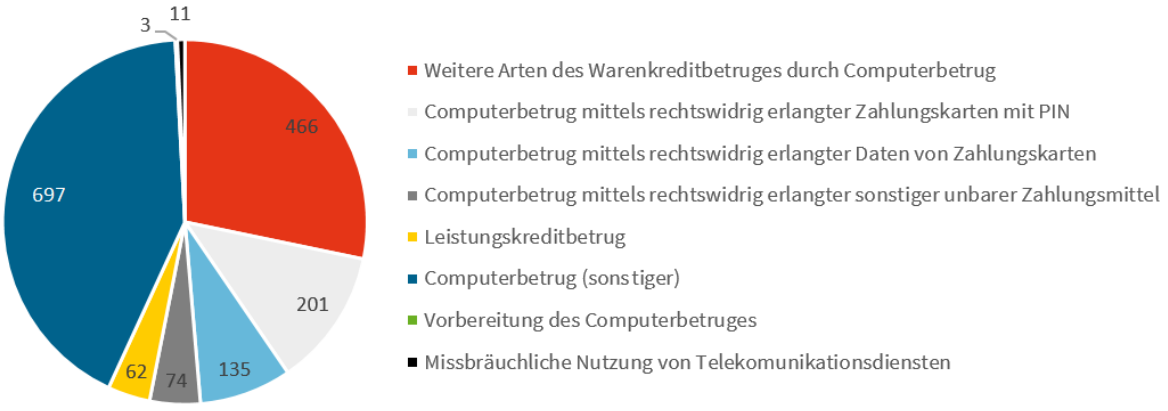
[5] Der Wortlaut der jeweiligen strafrechtlichen Norm kann in der Anlage 1 dieses Lagebildes eingesehen werden.

Computerbetrug machte im Jahr 2017 60 Prozent aller erfassten Delikte der Cybercrime i. e. S. aus. Eine etwa gleiche prozentuale Verteilung lag auch in den Jahren 2015 und 2016 im Deliktsfeld vor. Neben dem Computerbetrug weist auch das Ausspähen von Daten einen deutlichen Anstieg von 490 erfassten Fällen 2015 auf 638 registrierte Delikte 2017 auf. Allein die Entwicklung der Fallzahlen dieser beiden am häufigsten aufgetretenen Delikte offenbart einen weiteren starken Anstieg des Gefährdungspotentials durch Cybercrime i. e. S. in Thüringen. Eine genaue Aufschlüsselung der konkreten Fallzahlen zu den Delikten befindet sich in der Anlage zum Lagebild.

2.2 Computerbetrug

Das Delikt des Computerbetruges ist vor dem Hintergrund seiner Vielzahl an tatbestandlichen Verwirklichungsmöglichkeiten an dieser Stelle nochmalig detailliert abgebildet. Der Großteil wurde in der PKS als sonstiger Computerbetrug erfasst (697 Delikte). 466 registrierte Fälle des Warenkreditbetruges durch Computerbetrug gemäß § 263a StGB zeigen deutlich die Entwicklung des Phänomens des Identitätsdiebstahls und Identitätsmissbrauchs auf. Mittels entwendeter personenbezogener Daten zu Accounts jeglicher Art (E-Mail-Konten, Onlinebanking, Online-Shops, Zahlungsdaten), die im Darknet im großen Ausmaß gehandelt werden, bestellen zunehmend unbekannte Täter Waren oder Dienstleistungen im Internet auf Kosten der Geschädigten. In der folgenden Darstellung sind die Fallzahlen der tatbestandlichen Verwirklichungsmöglichkeiten des Computerbetruges lt. PKS in Thüringen 2017 dargestellt.

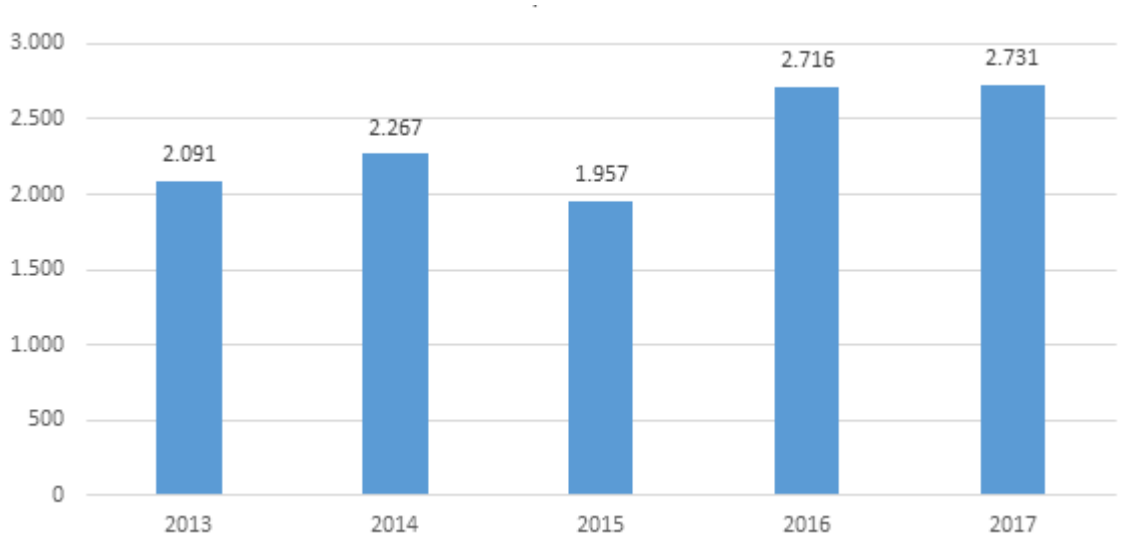
Fallzahlen des Computerbetruges in Thüringen 2017 lt. PKS



2.3 Computerkriminalität

Die PKS fasst unter dem Begriff Computerkriminalität alle Straftaten der Cybercrime i. e. S. mit den Delikten der Softwarepiraterie durch Verstöße gegen das Marken- oder Urheberrecht zusammen. In den letzten Jahren ist eine kontinuierliche Zunahme in diesem Bereich festzustellen. Auch diese Entwicklung verdeutlicht das Gefahrenpotential der Cybercrime. Vor dem Hintergrund der wachsenden Digitalisierung ist auch mit einer zukünftigen Zunahme der Fallzahlen in diesem Bereich zu rechnen.

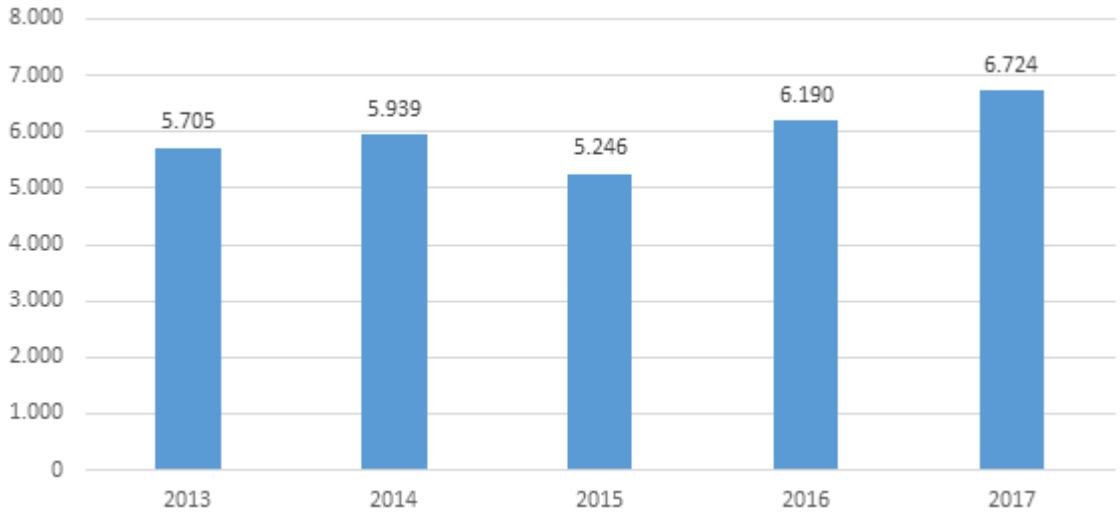
Entwicklung der Fallzahlen der Computerkriminalität in Thüringen lt. PKS



2.4 Tatmittel Internet

Die PKS verwendet die Sonderkennung „Tatmittel Internet“, sobald das Internet mit Blick auf die Verwirklichung einer erfassten Straftat eine wesentliche Rolle spielt. Auch in diesem Bereich ist in Thüringen ein deutlicher Anstieg der Fallzahlen seit 2015 auszumachen. Den Großteil der 6.724 im Jahr 2017 begangenen Delikte machen in diesem Zusammenhang mit 5.005 Fällen Betrugsdelikte aus, wobei hiervon wiederum 2.701 erfasste Delikte des Waren- und Warenkreditbetruges auszumachen sind. Auch diese Taten lassen einen Rückschluss auf die Entwicklung der Phänomenologie der „Fake Shops“ und des Identitätsdiebstahls und -missbrauchs zu.

Entwicklung der Fallzahlen mit der Sonderkennung „Tatmittel Internet“ in Thüringen lt. PKS



2.5 Schäden

Die Bestimmung des tatsächlich durch Cybercrime verursachten Schadens gestaltet sich schwierig. *Symantecs Norton Cyber Security Insight Report 2017* offenbart das Schadenspotential durch Cybercrime. Für Deutschland wurde hierbei im Rahmen der Studie eine Schadenssumme von ca. 2,2 Milliarden Euro für das Jahr 2017 errechnet.

Die mittels der PKS 2016 auf Bundesebene errechnete Gesamtschadenssumme durch Cybercrime i. e. S. beläuft sich auf 51,63 Millionen Euro, wobei auf Computerbetrug 50,9 Millionen Euro fallen. Diese Zahlen stellen kein repräsentatives Lagebild dar.

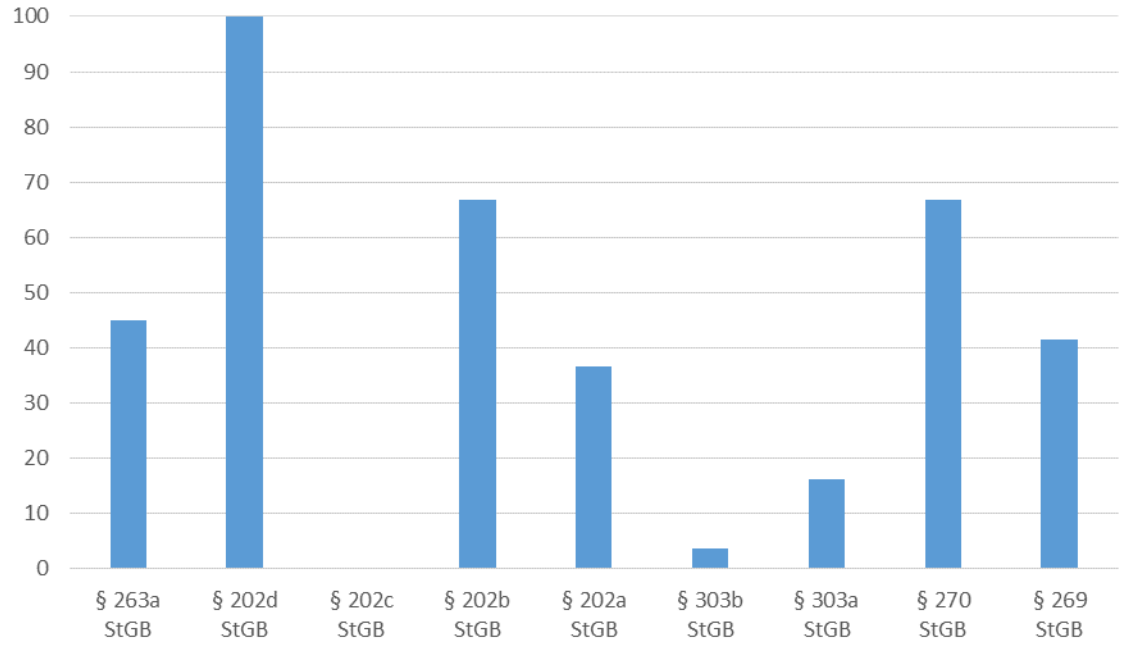
Eine seitens *Bitkom e. V.* durchgeführte Studie durch die Befragung von über 1.000 Unternehmen mit mehr als 10 Mitarbeitern zeigt einen Schaden von 55 Milliarden Euro für die deutsche Wirtschaft im Jahr 2016. Die enorme Differenz der seitens der PKS ermittelten Schadenssumme zu derer von *Bitkom e. V.* offenbart, wie hoch das Schadenspotential der Cybercrime in diesem Zusammenhang auch für den Freistaat Thüringen ist.

Durch Cyber-Angriffe erleiden Unternehmen Schädigungen enormen Ausmaßes. Der Aufbau von kostspieligen Ersatzmaßnahmen, Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen, Patentrechtverletzungen und Imageschäden bei Kunden und Lieferanten sind hierbei einige der zentralen negativen Folgen für die deutsche Wirtschaft. Auch Thüringer Unternehmen sind von derartigen Entwicklungen nicht ausgenommen. Hinsichtlich der Höhe der Schäden für Thüringen können lediglich Mutmaßungen aufgestellt werden, genaue Zahlen liegen hier derzeit keine vor.

2.6 Aufklärungsquote

In der Cybercrime i. e. S. ist in Thüringen eine sehr differenzierte Aufklärungsquote zwischen den einzelnen Delikten auszumachen. Insbesondere bei Tatbeständen (bspw. Datenveränderung, Computersabotage etc.), die intensiver technischer Ermittlungen bedürfen, sind die Aufklärungsquoten deutlich geringer.

Aufklärungsquote Cybercrime i. e. S. in Prozent in Thüringen



Die zum Teil hohen Aufklärungsquoten im Bereich der Cybercrime i. e. S. lassen sich durch die sehr geringen Fallzahlen der Delikte der §§ 202d, 202b und 270 StGB, die schlussendlich tatsächlich in die PKS eingeflossen sind, erklären. Hierbei wurden beim § 202d StGB 21 von 97 und in den Fällen der §§ 202b StGB und 270 StGB jeweils drei von drei angezeigten Straftaten in die PKS übernommen. Die Aufklärungsquote von 100 Prozent bezieht sich also im Falle des § 202d StGB nicht auf die 97 tatsächlich angezeigten und bearbeiteten Delikte, sondern auf die 21 in die PKS eingeflossenen Straftaten. Dieses Beispiel veranschaulicht, dass die Aufklärungsquoten, die aus der PKS generiert werden, die tatsächlichen Aufklärungsquoten insbesondere im Phänomenbereich Cybercrime nicht realistisch wiedergeben können.

Betrachtet man die Aufklärungsquoten des Computerbetruges gem. § 263a StGB, so scheint diese mit 44,9 Prozent recht hoch zu sein. Diese Zahl ist jedoch nicht repräsentativ.

In den Computerbetrug fließen auch die Delikte der weiteren Arten des Warenkreditbetruges durch Computerbetrug gem. § 263a StGB mit ein. Allein diese Tatbestände machten im Jahr 2017 fast 28,1 Prozent aller Delikte des Computerbetruges aus. Konkret handelt es sich bei derartigen Delikten in aller Regel um Tathandlungen in Bezug auf die Abwicklung von Geldtransfers nach dem Kauf oder Verkauf einer Ware auf Online-Marktplätzen, wie Amazon oder Ebay. In derartigen Fällen ist in Folge konventioneller Ermittlungen, wie Abfragen personenbezogener Daten zu Accounts bei den entsprechenden Online-Marktplätzen, die Aufklärungsquote höher.

Betrachtet man hingegen Delikte, die ein hohes Maß an Spezialisierung zum Zwecke technischer Ermittlungen benötigen, so ist die Aufklärungsquote dort sehr niedrig. Sie liegt z. B. in Fällen der Datenveränderung gem. § 303a StGB bei gerade einmal 16,3 Prozent, bei 98 in die PKS aufgenommenen Delikten. Die Computersabotage gem. § 303b StGB hat bei 56 in der PKS registrierten Fällen sogar eine Aufklärungsquote von nur 3,6 Prozent.

Eine Vielzahl der Cybercrime-Delikte, bei denen die Schädigung innerhalb Thüringens eintritt, verweist auf einen Tatort außerhalb Deutschlands. Hierbei sind die Ermittlungsmöglichkeiten insbesondere in Staaten außerhalb institutioneller Zusammenschlüsse, wie derer der EU oder Europol und dort wo keine etablierten Rechtshilfeabkommen bestehen, oftmals von Anbeginn nicht sonderlich erfolgsversprechend. Die Aufklärungsquoten in diesen Bereichen sind entsprechend niedrig.

3 Phänomene

Cybercrime kann ebenso wie andere Kriminalitätsfelder durch klar differenzierbare Delikte dargestellt werden, jedoch wird nur durch eine Betrachtung der phänomenologischen Erscheinungsformen das sich dynamisch verändernde Lagebild repräsentativ abgebildet. Der Freistaat Thüringen prüft gegenwärtig Möglichkeiten, die im Bundeslagebild des BKA dargestellten Phänomene quantifizierbar zu machen. Im Jahr 2016 waren dort

insbesondere die Verbreitung von Ransomware[6], der Diebstahl und Missbrauch digitaler Identitäten, sog. DDos-Angriffe[7], Data-Breaches[8] und im Internet betriebene Fake-Shops von besonderer Bedeutung. Diese Phänomene waren auch im Jahr 2017 weltweit weiterhin von großer Relevanz.

Das Institut der Wirtschaft Thüringens GmbH konnte auf Grundlage einer Umfrage der Arbeitgeber- und Wirtschaftsverbände Thüringens 2017 dahingehend die Betroffenheit der Thüringer Unternehmen durch entsprechende Phänomene der Cybercrime darlegen. So äußerten z. B. 50,6 Prozent der Befragten, dass sie 2016 mehrfach Angriffsversuchen durch Schadsoftware oder gezielten Hackerangriffen ausgesetzt waren. Von einem Rückgang ist auch im Jahr 2017 nicht auszugehen. Laut *Bitkom e. V.* zeigt ein Großteil der von Cybercrime betroffenen deutschen Unternehmen derartige Vorfälle nicht bei der Polizei an. Im Rahmen einer Studie im Jahr 2017 gaben 41 Prozent der Unternehmen an, dass sie Angst haben Imageschäden in Folge einer möglichen Veröffentlichung zu erleiden. 34 Prozent sprechen davon, dass die Polizei nicht in der Lage ist Täter zu ermitteln und hierdurch eine Anzeige keinen Sinn mache. In diesem Zusammenhang ist davon auszugehen, dass die verschiedenen Phänomenologien auch in Thüringen im öffentlichen und privatwirtschaftlichen Sektor von großer Bedeutung sind.

Das Thüringer Landesrechenzentrum (TLRZ) registrierte für das Jahr 2017 im Vergleich zum Jahr 2016 eine starke Zunahme von Anomalien, die von dessen Angriffserkennungssystem als Cyberattacken auf die Netzwerke der Thüringer Landesverwaltung interpretiert wurden. In nahezu allen Phänomenbereichen konnte ein starker Anstieg ausgemacht werden[9]. Beispielsweise wurden im Jahr 2016 noch 125.000

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

[7] Distributed-Denial-of-Service (DDoS) ist ein „verteilter“ Denial-of-Service (DoS). Bei diesem handelt es sich um die Blockade eines Internetdienstes, der vorliegt wenn dieser auf Anfrage nicht mehr erreichbar ist. Diese Nichtverfügbarkeit wird gezielt durch die Überlastung des angefragten Dienstes erreicht. Durch Überlastung werden die Websites des Dienstes extrem langsam oder ist gar nicht mehr erreichbar.

[8] Verlust sensibler Daten in eine nicht vertrauenswürdige Umgebung

[9] Auswertung des Intrusion Prevention System (IPS) des Thüringer Landesrechenzentrums (2017)

als SQL-Injection[10] und 67.000 DDos- oder Dos-Angriff[11] klassifizierte Vorfälle registriert bzw. abgewehrt. 2017 waren dies bereits 325.000 als SQL-Injection und als 488.000 DDos- oder Dos-Angriff eingestufte Ereignisse. Ob es sich hierbei um gezielte Cyberattacken gegen die IT-Infrastrukturen der Thüringer Landesverwaltung handelt kann aus polizeilicher Sicht mit den gegenwärtigen technischen Ermittlungsmöglichkeiten nicht abgeschätzt werden. Eine strafrechtliche Würdigung kann daher in den vorliegenden Cyberangriffen auf die Landesverwaltung auch für den Einzelfall nicht durchgeführt werden.

Ebenso sind digitale Schwarzmärkte der Underground Economy, über die bspw. Waffen, Betäubungsmittel, Falschgeld, Kreditkartendaten und Kinderpornografie - insbesondere über das sog. Darknet - vertrieben werden, weiterhin eine Problematik, die eine ernstzunehmende Gefahr für die öffentliche Sicherheit und Ordnung darstellen.

4 Organisatorische Rahmenbedingungen der Thüringer Polizei zur Bekämpfung der Cybercrime

Um dem Anstieg der Cybercrime, den damit einhergehenden neuartigen phänomenologischen Entwicklungen und der Notwendigkeit einer handlungsfähigen Strafverfolgung durch ein Höchstmaß an fachlicher Expertise in diesem Bereich gerecht zu werden, sind die gegenwärtigen organisatorischen und strukturellen Rahmenbedingungen innerhalb der Thüringer Polizei auch weiterhin entsprechend anzupassen.

Straftaten der Cybercrime werden in Dienststellen der Schutz- und Kriminalpolizei, sowie im Dezernat 64 des Landeskriminalamtes Thüringen bearbeitet. Im Zuge der weiter voranschreitenden Digitalisierung besteht Bedarf für die Ermittlungsarbeit in einer Vielzahl von Deliktsbereichen die Notwendigkeit ausreichendes technisches Verständnis zur

[10] SQL-Injection: Ausnutzen einer Sicherheitslücke im Zusammenhang mit SQL-Datenbanken. Hierbei versucht der Angreifer eigene Datenbankbefehle einzuschleusen, um hierdurch Daten auszuspähen oder zu verändern, die Kontrolle über den Server zu übernehmen oder einen größtmöglichen Schaden anzurichten.
[11] Mutwillig herbeigeführte Überlastung eines Internetdienstes, mit der Absicht bereitgestellte Dienste funktionsunfähig zu machen.

Gewährleistung geeigneter Ermittlungsmöglichkeiten weiter zu entwickeln. Die organisatorischen Rahmenbedingungen sind nach näherer Betrachtung zu verbessern.

Im Rahmen einer Befragung der Innenministerien der Länder durch das Magazin *Der Spiegel* wurde die Anzahl der Cyber-Ermittler in Deutschland erhoben[12]. Hierbei nahm Thüringen den drittletzten Platz unter den sechzehn Ländern des Bundes ein. Lediglich 0,2 speziell geschulte Polizeibeamte pro 100.000 Einwohner stehen demnach für die Bekämpfung der Cybercrime in Thüringen zur Verfügung. Die Vielzahl der Länder ist hier mit mindestens 2 oder gar mehr als 3 Beamten deutlich besser aufgestellt. Diese Zahlen verdeutlichen den Handlungsbedarf der in Thüringen in diesem Zusammenhang besteht.

Die gegenwärtige Aus- und Fortbildung von Polizeibeamten in Thüringen reicht nicht aus, um den Bedarf an Personal mit entsprechender technischer Expertise zur polizeilichen Aufgabenerledigung sicherzustellen. In anderen Ländern (Bayern, Baden-Württemberg, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen) wurden Sonderlaufbahnen geschaffen, um Personal aus dem Bereich der Informatik für die Beamtenlaufbahn mit und ohne Vollzugsaufgaben zu gewinnen[13]. Derartige Anreize wurden für die Landespolizei Thüringen bisher nicht gesetzt.

Auf Bitten des Arbeitskreises Innere Sicherheit (AK II) richtete die Kommission Kriminalitätsbekämpfung (KKB) am 01.01.2014 eine Bund-Länder-Projektgruppe zur Erarbeitung einer weiterentwickelten polizeilichen Strategie zur Bekämpfung von Cybercrime (BLPG Bekämpfungsstrategie) ein. Mit Stand vom 10.09.2015 wurde durch die BLPG Bekämpfungsstrategie die letzte Fassung der aktuell gültigen *Strategie zur Bekämpfung der Cybercrime* als Grundlage für die Bekämpfung der Cybercrime in den Polizeien des Bundes und der Länder aufgestellt. Diese Bekämpfungsstrategie bildet das Fundament zur Bekämpfung der Phänomenologie für Entscheidungsträger innerhalb der Polizei auf strategischer und operativer Ebene.

[12] Anfrage des Magazins *Der Spiegel* vom 31.08.2017 an das Thüringer Ministerium für Inneres und Kommunales

[13] Vgl. Beschluss 203. IMK TOP 15, Bericht S. 40: Feststellung der Innenministerkonferenz, dass nur durch Einstellung externen Personals mit entsprechender IT-Fachausbildung polizeiliche Aufgabenerledigung sichergestellt werden kann.

Als Grundlage für eine effektive Bekämpfung der Cybercrime in Thüringen wurde durch das Landeskriminalamt Thüringen die *Konzeption zur Bekämpfung der Cybercrime* entwickelt. Diese Konzeption dient

- der Ausrichtung an der Strategie zur Bekämpfung der Cybercrime der deutschen Polizei
- dem frühzeitigen Erkennen von neuen Entwicklungen und Bearbeitungsschwerpunkten dieses Phänomenbereiches
- dem Erkennen und Bündeln polizeilicher Ressourcen zur Bekämpfung der Cybercrime im Zuständigkeitsbereich der Thüringer Polizei
- der Koordinierung der Zusammenarbeit zwischen den Behörden und dem TLKA sowie innerhalb des TLKA
- der präzisierenden Festlegung von Bearbeitungszuständigkeiten innerhalb der Thüringer Polizei auf dem Gebiet der Cybercrime
- der Koordination und anlassbezogenen Zusammenarbeit mit Bund und Ländern

Gleichwohl gibt es weiteren Regelungsbedarf etwa in punkto Bearbeitungszuständigkeiten. Dem TLKA obliegt es u. a. als zentraler Dienststelle für kriminalpolizeiliche Aufgaben gem. § 3 IV ThürPOG die Kriminalitätsbekämpfung zu koordinieren und entsprechende Verwaltungsvorschriften nach Zustimmung des zuständigen Ministeriums zu erlassen. In diesem Zusammenhang sind die dazu erforderlichen Regelungen zur Bekämpfung der Cybercrime in enger Abstimmung mit der Landespolizeidirektion im Laufe der kommenden Jahre zu entwerfen.

Wünschenswert und vorstellbar ist in diesem Zusammenhang auch eine Gesetzesnovelle des Thüringer Polizeiorganisationsgesetzes bzw. einer entsprechenden Durchführungsverordnung, die eine klare Regelung zu Bearbeitungszuständigkeiten enthalten. Ebenso ist Regelungsbedarf hinsichtlich der Zuständigkeiten über die Fachaufsicht bei der kriminalpolizeilichen Bekämpfung der Cybercrime gegeben. In der *Thüringer Verordnung zur Bestimmung der sachlichen Zuständigkeiten der Polizeibehörden* finden sich hierzu keinerlei Regelungen.

Um sich den dynamischen Entwicklungen des Phänomens Cybercrime zu stellen, gilt es die notwendigen organisatorischen Rahmenbedingungen weiter zu verbessern. Die immer

komplexer werdenden Gefahren- und Schadenslagen in der digitalen Welt stellen auch die Thüringer Polizei in den kommenden Jahren vor große Herausforderungen.

5 Anlagen

Fallzahlen Cybercrime i. e. S. in Thüringen lt. PKS	2017	2016	2015
§ 269 StGB - Fälschung beweiserheblicher Daten	210	322	195
§ 270 StGB - Täuschung im Rechtsverkehr bei Datenverarbeitung	3	6	1
§ 303a StGB - Datenveränderung	98	124	72
§ 303b StGB - Computersabotage	56	55	55
§ 202a StGB - Ausspähen von Daten	638	553	490
§ 202b StGB - Abfangen von Daten	3	4	4
§ 202c StGB - Vorbereiten des Ausspähens und Abfangens von Daten	43	36	38
§ 263a StGB - Computerbetrug	21	-	-
§ 263a StGB - Computerbetrug	1.659	1.616	817

Fallzahlen der verschiedenen Erscheinungsformen des Computerbetruges gem. § 263a StGB in Thüringen 2017 lt. PKS	
§ 263a StGB - Computerbetrug	1.659
- Weitere Arten des Warenkreditbetruges durch Computerbetrug	466
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	201
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	135
- Computerbetrug mittels rechtswidriger erlangter sonstiger unbarer Zahlungsmittel	74
- Leistungskreditbetrug	62
- Computerbetrug (sonstiger)	697
- Vorbereitung des Computerbetruges	3
- Missbräuchliche Nutzung von Telekommunikationsdiensten	11