Cybercrime – Kriminalitätsbekämpfung im Internet

Otto-von-Guericke Universität Magdeburg
Fakultät für Humanwissenschaften
Seminar: Digitale Gesellschaft (SoSe 2018)
Optionaler Bereich

vorgelegt von

Laura Zimmermann
Annastr. 29, 39108 Magdeburg
laura_255@hotmail.de
0177 – 4645191

Matrikelnummer: 206813
Kulturwissenschaften B.A.
HF: Europäische Geschichte, NF: Sozialwissenschaften
8. Fachsemester

Seminarleitung: Herr Dr.-Ing. Marcel Götze

„Die digitalisierte Welt ist eine der zentralen Herausforderungen der Kriminalitätsbekämpfung von heute. Durch die über das Internet zur Verfügung stehende digitale Infrastruktur eröffnen sich potenziellen Straftätern neuartige Tatmuster mit enormen Schadensausmaßen für Gesellschaft und Wirtschaft.“[1], definiert das Ministerium für Inneres, Digitalisierung und Migration des Landes Baden-Württemberg die Problematik der heutigen digitalen Kriminalitätsbekämpfung auf seiner Homepage.

Mit steigender Mediennutzung hat sich ein erheblicher Teil der Straftatbestände in den virtuellen Raum verlagert und erfordert daher eine ganz neue Herangehensweise und Auseinandersetzung der zuständigen Polizeibehörden. Aufgabe sei es nun die „neuen Dimensionen von Kriminalität“, die mit der Entwicklung des Internets einhergingen, „anzunehmen“ und „die Methoden der Strafverfolgung und Gefahrenabwehr den neuen Kriminalitätsformen anzupassen“.[2] Hierbei gehe es um in der Form vorher nicht dagewesene Delikte, wie beispielsweise Cyberstalking und -mobbing, Identitätsklau, Handel mit Kinderpornografie, Hackerangriffe und digitale Schutzgelderpressungen. Dabei haben nicht nur bisher bekannte Ordnungskriterien wie Zeit und Raum an Bedeutung verloren, sondern ebenso auch klassische Rechtsbegriffe wie Tatort, Tatzeit und örtliche Zuständigkeiten. „Cybercrime“ durchbreche funktionale und territoriale Grenzen und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Vor diesem Hintergrund erscheint es sinnvoll im Folgenden einige dieser neuartigen Tatbestände näher zu beleuchten und anschließend verschiedene Strategien und Handlungsempfehlungen zur Bekämpfung und Vermeidung ebendieser vorzustellen.

Definition „Cybercrime“:

Zu Beginn soll jedoch der Versuch einer Definition unternommen werden: Der Begriff „Cybercrime“ (lat. *crimen*: „Beschuldigung, Anklage, Schuld, Verbrechen“; engl. *cyber*: auf das Internet bezogen) bezeichnet Vergehen und Verbrechen, die im Zusammenhang mit dem Internet geschehen bzw. damit begangen werden. „Es umfasst alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren

1 vgl. Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg: Cybercrime, URL: https://im.baden-wuerttemberg.de/de/sicherheit/polizei/kriminalitaetsbekaempfung/cybercrime/, veröffentlicht: k.A., letzter Aufruf: 10.07.18.

2 vgl. ebd.

Daten richten oder die mittels dieser Informationstechnik begangen werden.[3]“ Unterschieden wird hierbei zwischen:

- *Computerkriminalität* im engeren Sinne, für diese Straftaten wird lediglich ein Computer mit oder ohne Internetnutzung als Tatwaffe eingesetzt
- *Internetkriminalität*, diese Straftaten basieren auf dem Internet oder geschehen mit den Techniken des Internets.[4]

Erscheinungsformen:

Nachfolgend werden einige aktuelle Erscheinungsformen von Cybercrime vorgestellt. An dieser Stelle soll darauf hingewiesen werden, dass die Bandbreite illegaler Tätigkeiten in und mittels der Internet sehr groß ist und es sich hierbei selbstredend nur um eine beispielshafte Auswahl handeln kann; eine Darstellung aller bisher bekannten Deliktsformen würde den Rahmen dieser Arbeit um ein Weites übersteigen.

Identitätsdiebstahl/ Phishing:

Unter dem Begriff „Phishing“ (Neologismus von engl. f*ishing*: angeln und *password*) , versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Die digitale Identität umfasst dabei alle Arten von Accounts und zahlungsrelevanten Informationen eines Internetnutzers, wie beispielsweise Zugangsdaten in den Bereichen Kommunikation (E-Mail- und Messengerdienste, Soziale Medien), E-Commerce (Onlinebanking und -brokerage, internetgestützte Vertriebsportale aller Art, wie beispielsweise Reiseportale), berufsspezifische Informationen (z. B. für den Online-Zugriff auf firmeninterne technische Ressourcen), Kreditkartendaten und Zahlungsadressen.[5]

Als seriöse Bank oder Firma getarnt, fordern Cyberkriminelle den Empfänger in einer E-Mail beispielsweise auf, seine Daten zu aktualisieren. Entweder, weil zum Beispiel

3 vgl. Bundeskriminalamt: Internetkriminalität/Cybercrime, URL: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html, veröffentlicht: k.A., letzter Aufruf: 08.07.18.

4 vgl. Siller, Helmut: Art. Cybercrime, in: Gabler Wirtschaftslexikon, URL: https://wirtschaftslexikon.gabler.de/definition/cybercrime-53423, veröffentlicht: 19.02.2018, letzter Aufruf: 08.07.18.

5 vgl. Bundesamt für Sicherheit in der Informationstechnik: Phishing, URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html, veröffentlicht: k.A., letzter Aufruf: 18.07.18.

die Kreditkarte ablaufe, das Passwort erneuert werden müsse, die Zugangsdaten verloren gegangen seien oder aus Sicherheitsgründen Kontoinformationen bestätigt werden müssten. Angreifer spekulieren dabei darauf, dass der Empfänger der massenweise verschickten Nachrichten auch tatsächlich Kunde der vorgegebenen Firmen ist. Der Inhalt der so genannten Phishing-Mails wirkt dabei täuschend echt. Der Empfänger wird für die Dateneingabe über einen Link auf eine Internetseite geführt, die zum Beispiel der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen darüber hinaus entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden oder aber sie fälschen die Adressleiste des Browsers mit einem JavaScript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht.

Datendiebstahl durch Social Engineering:

Schwächstes Glied in der Sicherheitskette ist meist der Internetnutzer selbst. Dessen sind sich auch Cyberkriminelle bewusst. Durch geschickte psychologische Manipulation verleiten sie ihre Opfer zu Handlungen, die die Sicherheit ihrer Daten kompromittieren. Sie nutzen menschliche Angewohnheiten wie Neugier oder Angst aus, um Zugriff auf Daten zu erhalten oder Rechner zu infizieren. Potenzielle Opfer werden beispielsweise anhand von selbst gemachten Angaben in Sozialen Netzwerken ausgewählt und gezielt kontaktiert. Ein gängiges Beispiel für einen Social-Engineering-Angriff ist die Anfertigung einer Kopie eines vorhandenen Nutzer-Accounts in Sozialen Netzwerken, von dem anschließend vertrauenserweckende Nachrichten an dessen Freunde, beispielsweise mit der Bitte um Kontaktaufnahme über eine separate E-Mail-Adresse oder Handynummer, versendet werden.

2016 haben laut einer Studie 98 Prozent der Unternehmen weltweit berichtet, dass Schadsoftware der größte Verursacher von internen Schäden war. Direkt dahinter folgte bereits Social Engineering, dem 70 Prozent der befragten Unternehmen zum Opfer gefallen sind (und die Infektion mit Schadsoftware kann ebenfalls eine Folge von Social Engineering sein).[6] Da die größte Schwäche bei dieser Art von Angriff der Internetnutzer selbst ist, kann Sicherheitssoftware allein keine Lösung sein. Auch die

6 vgl. Hülsbömer, Simon: Wie Sie Social Engineering erkennen, URL: https://www.computerwoche.de/a/wie-sie-social-engineering-erkennen,3094016, veröffentlicht: 22.02.16, letzter Aufruf: 18.07.18.

beste Software wehrt keinen Angreifer ab, der sich korrekt über die üblichen Wege mit einem gültigen Login und Passwort anmeldet. Es gilt daher, Mitarbeiter in Unternehmen für die Gefahren von Social Engineering zu sensibilisieren. Interne Seminare und Kurse können dabei helfen, Personen mit Zugang zu wichtigen Daten aufzuklären.[7]

Einsatz von Schadsoftware („Malware"):

Der Begriff „Schadsoftware" (auch engl.: „Malware") beschreibt eine große Bandbreite von Software, die einen vorwiegend oder ausschließlich schadhaften Einfluss auf Computersysteme und -netzwerke nimmt und zu teilweise erheblichen Schäden führen kann. Obwohl Schadsoftware schon zu Beginn des Computerzeitalters von Bedeutung war, führt die größere Verbreitung und Bedeutung der sogenannten neuen Medien und deren vermehrt sorgloserer Umgang (gerade unter den immer jünger werdenden Nutzern) zu einem vergrößerten Bedrohungspotential. Die möglichen Schäden sind vielseitig und reichen von Angriffen auf die Privatsphäre, über üble Scherze, Betrug und Erpressung, bis hin zur Zerstörung wichtiger PC-Bauteile.

Im Folgenden sollen nun unterschiedliche Arten von Schadsoftware vorgestellt, ihre Wirkweise erklärt und kurz auf ihre mögliche Verbreitung eingegangen werden.

1. Computerviren: Der Begriff „Virus" unterliegt einer gewissen Generalisierung, weshalb heute verschiedene, teilweise höchst unterschiedliche Typen gemeinhin mit ihm bezeichnet werden. Der klassische Computervirus ist meist jedoch weniger gefährlich, als oftmals vermutet wird. Viren verhalten sich im Grunde wie ihre biologischen Pendants, was bedeutet, dass sie bereits vorhandene Dateien in Computersystemen „infizieren" und teilweise umschreiben. Die Schäden sind meist eher gering, primär wird eine möglichst weite Verbreitung angestrebt. Die Motive sind meist persönlicher Natur und reichen von üblen Scherzen, bis hin zur Verbreitung politischer Botschaften.[8]

2. Computerwürmer: Würmer gehören zu den schädlichsten Vertretern unter den Schadsoftwares, da sie bis zu einem gewissen Punkt autonom agieren können und die vorhandene Infrastruktur des Computers (wie beispielsweise den Email-Verteiler)

7 vgl. Förster, Moritz: Ganz ohne Social Engineering. Angriff aufs Unternehmensnetz, URL: https://www.heise.de/ix/meldung/Ganz-ohne-Social-Engineering-Angriff-aufs-Unternehmensnetz-4059973.html, veröffentlicht: 29.05.18, letzter Aufruf: 17.08.18.

8 vgl. Computerbild Redaktion: Viren, Würmer, Trojaner und Co. genau erklärt, URL: http://www.computerbild.de/artikel/cbs-Ratgeber-PC-Viren-Wuermer-Trojaner-und-Co.-genau-erklaert-1552156.html, veröffentlicht: 22.08.07, letzter Aufruf: 01.07.18.

nutzen können. Bei Schadsoftware, die via Emailanhang versendet wird, handelt es sich häufig um Computerwürmer. Finanzelle Schäden entstehen zumeist dadurch, dass Netzwerkressourcen verschwendet werden, sowie ganze Systeme durch die Mehrbelastung zusammenbrechen können.[9]

3. Trojaner: Bei Trojanern handelt es sich um Schadsoftware, die getarnt im System operiert und oftmals vom Nutzer selbst unwissentlich eingeschleust wird. Wie das namensgebende „Trojanische Pferd“ in der griechischen Mythologie, basieren Trojaner auf Täuschung. So geben sie sich meist als nützliche Software aus und erfüllen teilweise sogar die eigentlich erwünschte Funktion, während sie gleichzeitig Schaden am System anrichten. Die schädliche Wirkweise unterscheidet sich von Fall zu Fall, häufig ist jedoch Spionage eine mögliche Motivationsgrundlage.[10]

4. Spyware: Spyware hat, wie der Name schon andeutet, hauptsächlich die Funktion, den Geschädigten auszuspionieren. Dies hat meist einen finanziellen Hintergrund, da diese Art von Schadsoftware vornehmlich das Surfverhalten und die Interessen des beobachteten Nutzers ausliest. Diese Informationen werden wiederum an Dritte verkauft, häufig Firmen und Werbekunden, welche künftig gezielt auf den spionierten Nutzer ausgerichtete Werbung schalten können. Doch auch größere Schäden, wie das Auslesen von Passwörtern, Bankdaten usw. sind möglich. Spyware befindet sich häufig getarnt im Gefolge nützlicher, erwünschter Software. (s.Trojaner)[11]

5. Ransomware: Dieser Typus Schadsoftware basiert im Wesentlichen auf Erpressung. Das Programm verschlüsselt eine wichtige Datei des Geschädigten so, dass dieser nicht mehr auf diese zugreifen kann. Gleichzeit erhält er eine Nachricht, die ihn zur Zahlung einer bestimmten Summe auffordert, um die Sperrung aufzuheben. Oftmals sind hiervon wichtige Systemdateien betroffen, sowie Ordner, denen ein bestimmter emotionaler Wert beigemessen wird (Eigene Dateien, Bildordner usw.).[12]

6. Schadsoftware für mobile Endgeräte:

Aufgrund der rasant zunehmenden weltweiten Nutzung mobiler Endgeräte bringen

9 vgl. ebd.
10 vgl. ebd.
11 vgl. Rouse, Margaret: Spyware, URL: https://www.searchsecurity.de/definition/Spyware, veröffentlicht: 01.05.15, letzter Aufruf: 02.07.18.
12 vgl. Eckermann, Ines Maria: Was ist eigentlich Ransomware?, URL: https://www.gdata.de/ratgeber/was-ist-eigentlich-ransomware, veröffentlicht: 15.01.17, letzter Aufruf: 01.07.18.

Cyberkriminelle zunehmend auch speziell für Smartphones entwickelte Schadsoftware in Umlauf, beispielsweise zur Umgehung des Mobile-TAN-Verfahrens im Online-Banking. Die Infektion mobiler Endgeräte erfolgt – ebenso wie beim PC – über das Herunterladen infizierter Anhänge und das Aufrufen infizierter Links und Webseiten oder aber über die Installation spezieller infizierter Apps.[13]

Illegaler Handel mit Waffen, Betäubungsmitteln und Ausweisdokumenten im sogenannten „Darknet“:

Der Begriff "Darknet" ist recht schwammig und hat je nach Verwendung unterschiedliche Bedeutungen. Oft sind Anonymisierungs-Netzwerke wie Tor (Abkürzung engl. *The Onion Router*: Der Zwiebel-Router) damit gemeint, manchmal auch Teile des öffentlichen Internets, zu denen nicht jeder Zugang hat. Also Server und Foren, auf die es keine öffentlichen Links gibt und die man nur auf Einladung und mit speziellen Zugangsdaten findet. Nicht selten werden damit jene Teile des öffentlichen und nicht öffentlichen Netzes bezeichnet, wo man verbotenen Substanzen, Falschgeld, Waffen, Malware, Adressen aus Datenbanken und Debit-Karten mit und ohne Passwort kaufen kann.

Das Wort "Zwiebel" weist auf die Schichten hin, die die Daten durchdringen müssen: Anders als beim gewöhnlichen Surfen verbindet sich der Computer nicht direkt mit dem Server, auf dem die Website liegt. Stattdessen sind eine ganze Reihe von Servern in die Verbindung involviert, um größtmögliche Anonymität herzustellen.[14] Anonymität ist vor allem für zwei Gruppen interessant: Auf der einen Seite stehen Menschen, die den Schutz des Darknets für Ihre Kommunikation benötigen. Sie teilen sensible Daten und Informationen. Zu dieser Gruppe gehören politisch Unterdrückte oder Dissidenten, Oppositionelle aus diktaturgeführten Länder oder Journalisten und Whistleblower. Über das Darknet können sie auch auf Inhalte zugreifen, die ihnen im sichtbaren Netz durch politische Restriktionen nicht zur Verfügung stehen, die zensiert sind oder den Informanden in Lebensgefahr bringen würden. Auf der anderen Seite stehen Personen, die sich die Anonymität des Darknets zu Nutze machen, um negativen Konsequenzen zu

13 vgl. Mayrhans, Thomas/ Grimm Markus: HummingBad: Gegen den Android-Virus hilft nur dieses Mittel, URL: https://www.chip.de/news/Vorsicht-Android-Nutzer-85-Millionen-Nutzer-von-Malware-HummingBad-betroffen_96355370.html, veröffentlicht: 06.07.16, letzter Aufruf: 02.07.18.

14 vgl. Eckermann, Ines Maria: Was ist eigentlich das Darknet?, URL: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet, veröffentlicht: 11.06.17, letzter Aufruf: 18.07.18.

gehen und sich einer eventuellen Strafverfolgung zu entziehen. Diese Gruppe setzt sich aus Menschen zusammen, deren Aktivitäten im sichtbaren Internet sehr schnell zu einer Anzeige sowie Geld- und Haftstrafen führen würden. Im Darknet finden sich Foren, Webshops und Handelsplattformen für Dienstleistungen und Waren, die entweder illegal oder strengen gesetzlichen Regelungen unterworfen sind.[15] Beispiele hierfür sind: Organhandel, Handel mit Betäubungsmitteln, Kreditkartennummern, Waffen, gefälschte Ausweisdokumente und Urkunden.

Bekämpfung von Kinderpornografie:

Unter Kinderpornografie versteht man pornografische Darstellungen, die den sexuellen Missbrauch von unter 14-Jährigen zeigen. Kinderpornografie ist die dokumentierte sexuelle Ausbeutung von Kindern (Jungen und Mädchen). In Ton, Bild und/oder Schrift wird festgehalten, wie Kindern Leid zugefügt wird, das sie lebenslang nachhaltig schädigt. Sie ist in vielfältiger Form in Umlauf: Filme, Videos, Datenträger, Zeichnungen, Fotos, Tonbänder und Druckschriften werden konventionell, also per Versand, oder von Hand zu Hand, vor allem aber weltweit über das Internet verbreitet. Einmal auf „den Markt“ gekommen und in Umlauf gebracht, verschwindet kinderpornografisches Material nicht mehr, vielmehr wird es wieder und wieder kopiert und neu zusammengeschnitten. In § 184 b Strafgesetzbuch ist das Strafmaß geregelt. Wer demnach „Kinderpornografie besitzt, verbreitet, zugänglich macht, sich beschafft oder herstellt macht sich strafbar.“ Bei Verstoß ist mit einem Freiheitsentzug von bis zu zehn Jahren zu rechnen.[16]

Laut Aussage des Bundeskriminalamtes seien alleine im Jahr 2017 6.512 Fälle von Kinderpornografie registriert worden. Die Aufklärungsquote soll dabei rund 90 Prozent betragen haben. Diese Daten seien jedoch noch um etwa 8.400 weitere Fälle zu ergänzen, die von einer US-amerikanischen Organisation übermittelt wurden. Eine Aufklärung dieser Sachverhalte sei mangels Umsetzung der Vorratsdatenspeicherung nicht möglich. Das Bundeskriminalamt weist bereits seit geraumer Zeit auf die enorme Bedeutung der Vorratsdatenspeicherung für die Bekämpfung von Kinderpornografie hin - ohne eine Umsetzung der Vorratsdatenspeicherung blieben tausende Fälle von

15 vgl. Neller, Marc: So funktioniert der illegale Waffenhandel im Netz, URL: https://www.welt.de/wirtschaft/article156844225/So-funktioniert-der-illegale-Waffenhandel-im-Netz.html, veröffentlicht: 06.07.16, letzter Aufruf: 17.07.18.

16 vgl. Landeskriminalamt Berlin: Bekämpfung der Kinderpornografie, URL: https://www.berlin.de/polizei/dienststellen/landeskriminalamt/lka-1/artikel.148846.php, veröffentlicht: k.A., letzter Aufruf: 18.07.18.

Kinderpornografie unaufgeklärt. Die Daten fänden bisher keinen Eingang in die Polizeiliche Kriminalstatistik (kurz: PKS), weil sie zwar deutschen IP-Adressen, nicht aber einer konkreten Person in einem Bundesland zuzuordnen sind. Gleichwohl müssten für eine Einschätzung der Lage beide Zahlen zusammengefasst werden. Im Ergebnis erlangte die deutsche Polizei im Jahr 2017 Kenntnis von rund 14.900 Fällen. Die Aufklärungsquote reduziere sich somit von knapp 90 auf rund 40 Prozent.[17]

Die meisten Hinweise zu Dateien mit kinderpornografischen Inhalten erhalte das BKA aktuell von der US-amerikanischen Nichtregierungsorganisation „National Centre for Missing and Exploited Children“ (kurz: NCMEC). Diese arbeite wiederum mit amerikanischen Internetanbietern und Serviceprovidern wie Facebook, Microsoft, Yahoo oder Google zusammen, die ihre Datenbestände und die über ihre Dienste verbreiteten Daten mittels modernster Filtertechnologien permanent nach Missbrauchsabbildungen scannen. Die festgestellten Dateien würden gelöscht und die verfügbaren Informationen dem NCMEC übermittelt. Das NCMEC leite diese Verdachtsanzeigen dann auf Basis der IP-Adresse, von der aus der Upload des strafrechtlich relevanten Materials stattgefunden hat, an die jeweils zuständige polizeiliche Zentralstelle des Landes weiter, in dem die Straftat stattgefunden hat. Über 35.000 Hinweise auf mögliche strafbare Handlungen in Deutschland seien auf diese Weise im vergangenen Jahr im Bundeskriminalamt eingegangen. Als Zentralstelle ist das BKA für die Auswertung und die Weiterleitung der Erkenntnisse an die zuständigen Strafverfolgungsbehörden der Bundesländer zuständig. Eigens dafür wurde die „Zentralstelle Sexualdelikte zum Nachteil von Kindern und Jugendlichen“ eingerichtet, die als Bindeglied Aufgaben zwischen in- und ausländischen Strafverfolgungsbehörden sowie einer nationalen zentralen Auswerte- und Koordinierungsstelle für diese Behörden wahrnimmt. In den vergangenen Jahren sei die Zahl der Hinweise auf Missbrauchsabbildungen im Internet kontinuierlich gestiegen. Die Zahl der Fälle, die Eingang in die Polizeiliche Kriminalstatistik (PKS) fanden, bliebe jedoch annähernd gleich, im Vorjahr lag sie, wie bereits erwähnt, bei 6.512 Fällen und einer Aufklärungsquote von knapp 90 Prozent - ein „auf den ersten Blick sehr guter Erfolg.“[18] Eine Vielzahl der aufgeklärten Fälle seien möglich gewesen, da oftmals die Inhaber der

17 vgl. Bundeskriminalamt: Polizeiliche Kriminalstatistik (PKS) 2017, URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html, veröffentlicht: 08.05.18, letzter Aufruf: 18.07.18.

18 vgl. Landeskriminalamt Berlin: Bekämpfung der Kinderpornografie, URL: https://www.berlin.de/polizei/dienststellen/landeskriminalamt/lka-1/artikel.148846.php, veröffentlicht: k.A., letzter Aufruf: 18.07.18.

ermittelten IP-Adresse noch festgestellt werden konnten. Dennoch bilde die PKS nur einen sehr kleinen Teil der tatsächlichen Straftaten ab. Dies erkenne man daran, dass die Zahl der erfassten Fälle sehr viel geringer ist, als die Zahl der Hinweise (rund 35.000). Die im Vergleich zu den eingehenden Hinweisen geringe Anzahl an registrierten Fällen sei einerseits darin begründet, dass nicht jedes gemeldete Foto oder Video tatsächlich strafbare Handlungen enthielt. Andererseits könne in vielen Fällen die vom Provider mitgelieferte IP-Adresse mangels Vorratsdatenspeicherung keinem konkreten Anschluss in Deutschland mehr zugeordnet werden, da der Provider die zur Identifizierung notwendigen Daten bereits gelöscht habe. Diese Fälle fänden keinen Eingang in die PKS, weil sie eine Zuordnung zu einem bestimmten Bundesland voraussetzt. 2016 und 2017 betraf dies nach eigener Angabe jeweils rund 8.400 Fälle.[19]

Der Nachweis von Straftaten im Bereich Kinderpornografie ist für die zuständigen Polizeibehörden schwierig. Nicht nur aufgrund der bereits beschriebenen Anonymität des Darknets, sondern auch aufgrund des eingeschränkten Handelsspielraums der Ermittler. Oftmals werden sogenannte „Keuschheitsproben“ in den entsprechenden Foren gefordert, um Zugang zu ebendiesen zu bekommen. Damit werden sie aufgefordert selbst kinderpornografisches Material hochzuladen. "Da ihnen dies nach geltendem Recht nicht möglich ist, können die Täter verdeckte Ermittler schnell enttarnen.", erklärt Bayerns Justizminister Winfried Bausback in einem Interview. Immer wieder entfachen Diskussionen darüber, den Ermittlern eine entsprechende Rechtsgrundlage zu schaffen, die ihnen so ein Vorhaben erlaube. Durch den Einsatz von eigens zu Zwecken der verdeckten Ermittlung hergestellten Fake-Bildern und -Videos mit kinderpornografischen Inhalten könne die „Tarnung der Beamten aufrecht erhalten und zugleich Tätern besser das Handwerk gelegt werden“. Die Ermittler müssten zweifelsohne "sehr behutsam vorgehen", zudem brauche die Neuregelung enge Grenzen: "So dürfen die verdeckten Ermittler selbstverständlich kein echtes kinderpornografisches Material hochladen, sondern nur echt aussehendes", sagt Bausback weiter. Die Ermittlungsbehörden dürften keinesfalls dazu beitragen, dass Kinder tatsächlich zu Schaden kommen. Ziel aller Anstrengungen müsse es sein, sexuellen Missbrauch zu verhindern und weitere Taten zu unterbinden.[20] Ob eine solche

19 vgl. Bundeskriminalamt: Zahlen und Fakten zur Bekämpfung der Kinderpornografie - Klarstellung durch das Bundeskriminalamt, URL: https://www.presseportal.de/blaulicht/pm/7/3963573, veröffentlicht: 06.06.18, letzter Aufruf: 18.07.18.

20 vgl. BR Redaktion: Mit Fake-Kinderpornos gegen Sexualverbrecher, URL: https://www.br.de/nachrichten/justizminister-will-sexualverbrecher-mit-fake-kinderpornos-koedern-100.html, veröffentlicht: 13.03.18, letzter Aufruf: 18.07.18.

Vorgehensweise nun moralisch vertretbar ist oder nicht; eine Aktion der Menschenrechtsorganisation „Terre des Hommes“ zeigt wie erfolgreich ein solches Verfahren zur Bekämpfung von Kinderpornografie eingesetzt werden kann: Mit einer am Computer animierten Figur namens "Sweetie", einem zehnjährigen philippinischen Mädchen, nahmen die Aktivisten Kontakt zu Usern verschiedener Internetforen auf. Über einen Zeitraum von zehn Wochen suchten mehr als 20.000 Männer Kontakt zu Sweetie, um sie für sexuelle Handlungen vor der Webcam zu bezahlen. Mit der Lockvogel-Aktion wollte die niederländische Abteilung von Terre des Hommes auf ein weitgehend unbekanntes, sich aber offenbar rasant ausbreitendes Phänomen aufmerksam machen: die sogenannte Webcam-Kinderprostitution.[21] Von rund 1.000 Männern aus 71 Ländern sollen Kontaktdaten gesammelt und den Behörden weitergegeben worden sein. Erst einer soll deshalb verurteilt worden sein. Die gesammelten Daten übergaben die Mitarbeiter schließlich an die niederländischen Behörden, die diese gemeinsam mit Europol auswerteten. Anschließend wurden die Informationen an nationale Polizeibehörden weitergegeben. Doch eine Verurteilung ist in den meisten Ländern nicht möglich, da die Rechtslage die Fälle nicht vor Gericht kommen lässt. Um eine Straftat begangen zu haben, hätten die Männer ein reales Kind anschreiben müssen. Außerdem ist der Einsatz eines "Agent provocateur" streng verboten.[22] Das Sicherheits- und Justizministerium der Niederlande, wo die Informationen gelandet waren, hat ebenfalls keine Ermittlungen eingeleitet. Die "Sweetie"-Kontakte seien in den Niederlanden nicht strafbar. Terre des Hommes fordere deshalb, dass die Polizei mit mehr Befugnissen für Ermittlungen im Internet und "Verbrechen des 21. Jahrhunderts" ausgestattet wird. In den Niederlanden wird nun ein Gesetz diskutiert, dass den Beamten ebensolche Befugnisse geben soll.[23]

21 vgl. Leurs, Rainer: Pädophilen-Jagd im Netz. "Die Männer sind von sich aus auf Sweetie zugegangen", URL: http://www.spiegel.de/panorama/justiz/webcam-sextourismus-terre-des-hommes-erschafft-virtuelle-zehnjaehrige-a-931939.html, veröffentlicht: 06.11.13, letzter Aufruf: 18.07.18.

22 vgl. Blei, Bianca: Webcam-Sex mit "Sweetie" hat in vielen Ländern kein Nachspiel, URL: https://derstandard.at/2000008554687/Webcam-Sex-mit-Sweetie-hat-in-vielen-Laendernkein-Nachspiel, veröffentlicht: 27.11.14, letzter Aufruf: 18.07.18.

23 vgl. ebd.

Literatur- und Quellenverzeichnis:

Blei, Bianca: Webcam-Sex mit "Sweetie" hat in vielen Ländern kein Nachspiel, URL: https://derstandard.at/2000008554687/Webcam-Sex-mit-Sweetie-hat-in-vielen-Laendernkein-Nachspiel, veröffentlicht: 27.11.14, letzter Aufruf: 18.07.18.

BR Redaktion: Mit Fake-Kinderpornos gegen Sexualverbrecher, URL: https://www.br.de/nachrichten/justizminister-will-sexualverbrecher-mit-fake-kinderpornos-koedern-100.html, veröffentlicht: 13.03.18, letzter Aufruf: 18.07.18.

Bundesamt für Sicherheit in der Informationstechnik: Phishing, URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html, veröffentlicht: k.A., letzter Aufruf: 18.07.18.

Bundeskriminalamt: Internetkriminalität/Cybercrime, URL: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html, veröffentlicht: k.A., letzter Aufruf: 08.07.18.

Bundeskriminalamt: Polizeiliche Kriminalstatistik (PKS) 2017, URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html, veröffentlicht: 08.05.18, letzter Aufruf: 18.07.18.

Bundeskriminalamt: Zahlen und Fakten zur Bekämpfung der Kinderpornografie - Klarstellung durch das Bundeskriminalamt, URL: https://www.presseportal.de/blaulicht/pm/7/3963573, veröffentlicht: 06.06.18, letzter Aufruf: 18.07.18.

Computerbild Redaktion: Viren, Würmer, Trojaner und Co. genau erklärt, URL: http://www.computerbild.de/artikel/cbs-Ratgeber-PC-Viren-Wuermer-Trojaner-und-Co.-genau-erklaert-1552156.html, veröffentlicht: 22.08.07, letzter Aufruf: 01.07.18.

Eckermann, Ines Maria: Was ist eigentlich das Darknet?, URL: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet, veröffentlicht: 11.06.17, letzter Aufruf: 18.07.18.

Eckermann, Ines Maria: Was ist eigentlich Ransomware?, URL: https://www.gdata.de/ratgeber/was-ist-eigentlich-ransomware, veröffentlicht: 15.01.17, letzter Aufruf: 01.07.18.

Förster, Moritz: Ganz ohne Social Engineering. Angriff aufs Unternehmensnetz, URL: https://www.heise.de/ix/meldung/Ganz-ohne-Social-Engineering-Angriff-aufs-Unternehmensnetz-4059973.html, veröffentlicht: 29.05.18, letzter Aufruf: 17.08.18.

Hülsbömer, Simon: Wie Sie Social Engineering erkennen, URL: https://www.computerwoche.de/a/wie-sie-social-engineering-erkennen,3094016, veröffentlicht: 22.02.16, letzter Aufruf: 18.07.18.

Landeskriminalamt Berlin: Bekämpfung der Kinderpornografie, URL: https://www.berlin.de/polizei/dienststellen/landeskriminalamt/lka-1/artikel.148846.php, veröffentlicht: k.A., letzter Aufruf: 18.07.18.

Leurs, Rainer: Pädophilen-Jagd im Netz. "Die Männer sind von sich aus auf Sweetie zugegangen", URL: http://www.spiegel.de/panorama/justiz/webcam-sextourismus-terre-des-hommes-erschafft-virtuelle-zehnjaehrige-a-931939.html, veröffentlicht: 06.11.13, letzter Aufruf: 18.07.18.

Mayrhans, Thomas/ Grimm Markus: HummingBad: Gegen den Android-Virus hilft nur dieses Mittel, URL: https://www.chip.de/news/Vorsicht-Android-Nutzer-85-Millionen-Nutzer-von-Malware-HummingBad-betroffen_96355370.html, veröffentlicht: 06.07.16, letzter Aufruf: 02.07.18.

Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg: Cybercrime, URL: https://im.baden-wuerttemberg.de/de/sicherheit/polizei/kriminalitaetsbekaempfung/cybercrime/, veröffentlicht: k.A., letzter Aufruf: 10.07.18, 13:39.

Neller, Marc: So funktioniert der illegale Waffenhandel im Netz, URL: https://www.welt.de/wirtschaft/article156844225/So-funktioniert-der-illegale-Waffenhandel-im-Netz.html, veröffentlicht: 06.07.16, letzter Aufruf: 17.07.18.

Rouse, Margaret: Spyware, URL: https://www.searchsecurity.de/definition/Spyware, veröffentlicht: 01.05.15, letzter Aufruf: 02.07.18.

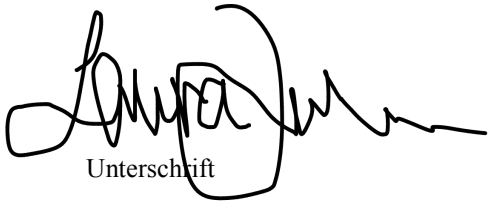
Siller, Helmut: Art. Cybercrime, in: Gabler Wirtschaftslexikon, URL: https://wirtschaftslexikon.gabler.de/definition/cybercrime-53423, veröffentlicht: 19.02.2018, letzter Aufruf: 08.07.18.

Eigenständigkeitserklärung:

Hiermit versichere ich, dass die vorliegende Arbeit selbständig verfasst wurde, dass keine anderen Quellen und Hilfsmittel als die angegebenen benutzt wurden und dass die Stellen der Arbeit, die aus fremden literarischen Werken oder Darstellungen wissenschaftlicher oder technischer Art übernommen wurden, einschließlich der in den elektronischen Medien veröffentlichten Quellen, unter Hinweis auf die Quelle gekennzeichnet wurden. Mir ist bekannt, dass Verstöße gegen das Urheberrecht, Unterlassungs- und Schadensersatzansprüche des Urhebers sowie eine strafrechtliche Ahndung durch die Strafverfolgungsbehörden begründen kann.

Magdeburg, den 17. Juli 2018

Ort und Datum



Unterschrift