WITHOUT A TRACE – DIE UNGEKLÄRTEN CYBERCRIME-FÄLLE DES STRAFLANDESGERICHTS WIEN

Edith Huber / Bettina Pospisil / Walter Hötzendorfer / Leopold Löschl / Gerald Quirchmayr / Christof Tschohl

Senior Researcher, Donau Universität Krems
Dr.-Karl-Dorrek-Str. 30, 3500 Krems an der Donau, AT
edith.huber@donau-uni.ac.at; http://www.donau-uni.ac.at

Junior Researcher, Donau Universität Krems, Zentrum für Infrastrukturelle Sicherheit
Dr.-Karl-Dorrek-Str. 30, 3500 Krems an der Donau, AT
bettina.pospisil@donau-uni.ac.at; http://www.donau-uni.ac.at

Senior Researcher, Research Institute AG & Co KG
Annagasse 8/1/8, 1010 Wien, AT
walter.hoetzendorfer@researchinstitute.at; http://www.researchinstitute.at

Leitung C4, Bundesministerium für Inneres
Josef-Holaubek-Platz 1, 1090 Wien, AT
Leopold.loeschl@bmi.gv.at; http://www.bmi.gv.at

Universitätsprofessor, Universität Wien, Fakultät für Informatik
Währinger Straße 29, 1090 Wien, AT
Gerald.Quirchmayr@univie.ac.at

Wissenschaftlicher Leiter, Research Institute AG & Co KG
Annagasse 8/1/8, 1010 Wien, AT
christof.tschohl@researchinstitute.at; http://www.researchinstitute.at

Schlagworte: ***Cybercrime, Computerkriminalität, Hellfeldanalyse, Modus Operandi, Tathergangsmuster***

Abstract: *Seit 2006 werden in Österreich die Fälle von Computerkriminalität in der amtlichen Kriminalstatistik unter dem Sammelbegriff «Cybercrime» erfasst. Nachdem in einem ersten Schritt die aufgeklärten Cybercrime-Fälle der letzten zehn Jahre (2006–2016) näher betrachtet wurden, widmet sich dieser Artikel den ungeklärten Fällen, welche sich in diesem Zeitraum ereigneten. Analysiert werden also jene Fälle, des Sprengels des Straflandesgerichts Wien, in welchen es nicht zu einem Urteil kam.*

1. Einleitung

Kaum eine andere Kriminalitätsart erlebte in den vergangenen Jahren so einen Boom wie die Cyber-Kriminalität. Während die Zahl der angezeigten Fälle rasant ansteigt, ist die Zahl der aufgeklärten Fälle nur mäßig steigend. Welche sind jedoch die typischen Cybercrime-Fälle, die nicht gelöst werden? Lassen sich Tathergangsmuster sowie Tatmotive klassifizieren? Ziel des hier durchgeführten Projektes war es, jene Fälle im Sprengel des Straflandesgerichts Wien zu untersuchen, bei denen die TäterInnen bzw. die Tatverdächtigen unbekannt blieben. Im Rahmen dieses Beitrags sollen Ergebnisse aus dem KIRAS Projekt «CERT-Kommunikation II»[1] dargestellt und interpretiert werden. Seit 2006 werden Cybercrime-Delikte in der Kriminalstatistik unter diesem Begriff erfasst. Generell unterscheidet man (a) Cybercrime im engeren Sinn (Core Cybercrime bzw. Cyberdependent Crime): Unter diese Definition fallen alle Delikte, die es in keiner Variante offline gibt; diese

[1] Das Forschungsvorhaben, «CERT-Kommunikation II», wurde gefördert im Rahmen des Österreichischen Sicherheitsforschungs-Förderprogramms KIRAS – einer Initiative des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT).

Kategorie umfasst die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken sowie von Geräten, Daten und Services in diesen Netzwerken. Dazu zählt «Hacking», Cyber-Vandalismus, die Verbreitung von Viren etc.; (b) Cybercrime im erweiterten Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime): Delikte, die unter diese Kategorie fallen, können auch offline existieren. Dazu zählen Delikte, wie z.B. Kreditkartenmissbrauch, Informationsdiebstahl, Geldwäsche, Vergehen gegen das Urheberrecht, Cyberstalking, Cybermobbing sowie die Nutzung, Verbreitung und Zurverfügungstellung kinderpornographischer Inhalte usw.;[2] (c) Verschleierung der Identität: Dies betrifft Täter[3], die sich einen Online-Avatar zulegen und die Anonymität dazu verwenden, kriminell zu handeln[4], bzw. Täter, die sich gestohlener Identitäten oder Fake-Identities bedienen.

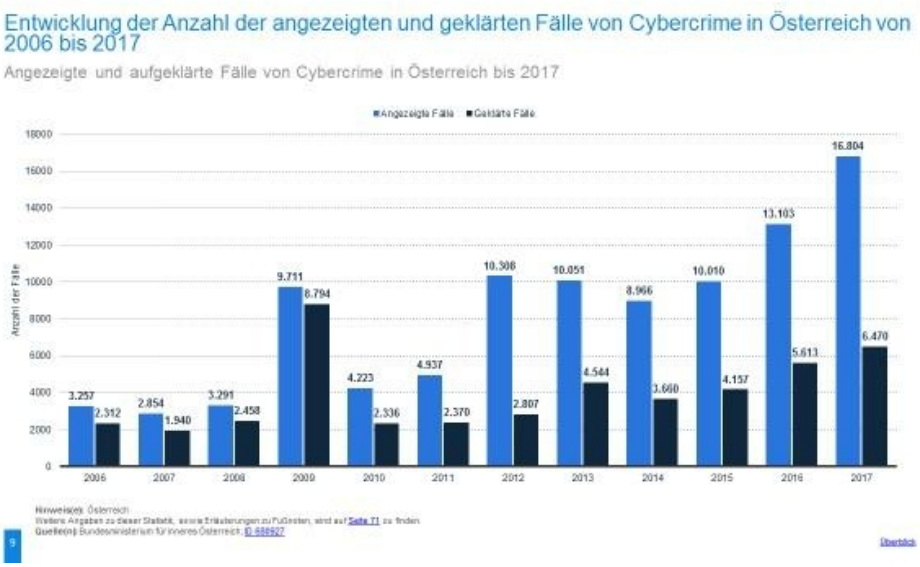

Abbildung 1: Entwicklung der Anzahl der angezeigten (helle Balken) und geklärten (dunkle Balken) Fälle von Cybercrime in Österreich von 2006 bis 2017[5]

Im Rahmen des hier angeführten Projektes wurde folgender Forschungsfrage nachgegangen: «Was sind die typischen Tathergangsmuster der ungelösten Fälle?»

2. Methodische Vorgehensweise

Zur Beantwortung dieser Hauptforschungsfrage wurde eine Aktenanalyse der Cybercrime-Delikte der Jahre 2006 bis 2016 am Wiener Straflandesgericht durchgeführt. Dazu wurden Cybercrime-Delikte im engeren Sinn sowie Cybercrime-Delikte im weiteren Sinn analysiert.[6] Delikte der Pornographischen Darstellung Minderjähriger sowie der Anbahnung von Sexualkontakten zu Unmündigen fanden in dieser Auswertung keine

2 McGuire, M. / Dowling, S., Cyber crime: A review of the evidence, 2013; Kirwan, G. / Power, A., Cybercrime, Cambridge University Press 2013.

3 An dieser Stelle sei festgehalten, dass für die allgemeine Bezeichnung von Personengruppen, zwecks besserer Lesbarkeit, die männliche Form verwendet wird, z. B. also Täter (gemeint Täter und Täterinnen, Hacker und Hackerinnen).

4 Kirwan, G. / Power, A., Cybercrime, Cambridge University Press 2013.

5 *Bundesministerium für Inneres*, Statista, 2018.

6 Im Rahmen des vorliegenden Forschungsvorhabens wurden folgende Cybercrime-Delikte des StGB im engeren Sinn untersucht: §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem), 119 (Verletzung des Telekommunikationsgeheimnisses), 119a (Miss-

Berücksichtigung. Ausgehend von dieser Grundbetrachtung lagen im Wiener Straflandesgericht im Untersuchungszeitraum rund 5.400 Akten der Staatsanwaltschaft und des Gerichts vor.[7] Zur genauen Beantwortung der Forschungsfrage und nach Sichtung der Datenlage wurden in einem ersten Schritt jene Fälle betrachtet, bei welchen es zu einer Hauptverhandlung kam. Diese Studie wurde im letzten Jahr veröffentlicht und zeigte, welche Cybercrime-Fälle gelöst werden können bzw. welche Ermittlungsformen dies unterstützten. Darüber hinaus ermöglichte diese Studie Aussagen sowohl zu Täter- als auch Opferprofilen. Nun wurden in einem zweiten Schritt jene Fälle betrachtet, bei denen der Täter unbekannt war und jene, bei denen die Akten ausschließlich bei der Staatsanwaltschaft behandelt wurden (N=2720). Aus den Akten wurde eine Zufallsstichprobe mittels Listenauswahl gezogen. Da es sich hier um eine Art der Wahrscheinlichkeitsauswahl handelt, kann von der Stichprobe auf die Grundgesamtheit geschlossen werden. Aus den Fallakten wurde somit eine repräsentative Stichprobe (n=20%) gezogen, was sich nach Ausschluss ungültiger Fälle auf eine Stichprobe von (n=)104 Tatverdächtigen belief. Als Forschungsmethode zur Analyse der Akten wurde eine quantitative Aktenanalyse nach Dölling[8] herangezogen.

3. Ergebnisse der Hellfeldanalyse

3.1. Was wir über die Opfer wissen

Cybercrime-Opfer kommen als Untersuchungsgegenstand in der Wissenschaft relativ selten vor, da landläufig die Meinung herrscht, dass jeder Opfer werden kann. Bei genauerer Betrachtung der einzelnen Delikte können jedoch Unterschiede festgestellt werden und auch Schwerpunktsetzungen und Zusammenhänge lassen sich ausmachen. Generell unterscheidet man die Opfer in Privatpersonen, Firmen, Staaten und kritische Infrastrukturen. Sie können als Einzelpersonen oder in Gruppen auftreten.[9] Die im Untersuchungszeitraum gemessenen Fälle zeigten folgendes Bild: Firmen (32,1%), Privatpersonen (46,5%), Gruppe von Privatpersonen (8,9%), Behörden (9,8%) sowie Personen öffentlichen Interesses (2,7%). Dies lässt den Schluss zu, dass nahezu die Hälfte der Cybercrime-Opfer, deren Fälle ungelöst bleiben, Privatpersonen sind. Grundsätzlich wurden dabei folgende Arten der Opferwahl unterschieden: Zielgerichtete bzw. mutwillige Angriffe, das Ausnutzen einer Schwachstelle, die willkürliche Opferwahl. In mehr als der Hälfte aller Fälle (55,8%) lässt sich eine zielgerichtete Opferwahl erkennen, in Rund einem Drittel aller Fälle wurde eine Schwachstelle ausgenutzt. Wurde eine Firma oder eine Behörde Opfer des Cyberangriffes, handelte es sich in 36,4% dieser Fälle um einen Angriff auf eine kritische Infrastruktur. Am häufigsten passieren diese Angriffe in den Bereichen Staat und Verwaltung sowie IT und Telekommunikation.

Zusammenfassend kann man daher festhalten, dass im Falle der hier betrachteten ungelösten Cybercrime-Fälle, fast die Hälfte der Opfer Privatpersonen sind, die Tatverdächtigen wählen ihre Opfer mutwillig und zielgerichtet. Bei rund einem Drittel der ungelösten Fälle sind die Opfer Firmen. Dieses Ergebnis muss vor dem Hintergrund interpretiert werden, dass nur jene Cybercrime-Fälle analysiert werden können, welche auch zur Anzeige gebracht werden. Das Dunkelfeld könnte – so die Vermutung – ein anderes Bild nahelegen.

bräuchliches Abfangen von Daten), 126a (Datenbeschädigung), 126b (Störung der Funktionsfähigkeit eines Computersystems), 126c (Missbrauch von Computerprogrammen oder Zugangsdaten), 148a (Betrügerischer Datenverarbeitungsmissbrauch sowie 225a (Datenfälschung).

7 Huber, E. / Pospisil, B. / Hötzendorfer, W. / Löschl, L. / Quirchmayr, G. / Tschohl, C., Cybercrime – Hellfeldanalyse der Akten des Wiener Straflandesgerichts von 2006–2016, in: Erich Schweighofer, Franz Kummer, Ahti Saarenpää, Burkhard Schafer, Datenschutz/LegalTech. Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, 519–528, Editions Weblaw.

8 Dölling, D., Probleme der Aktenanalyse in der Kriminologie, in: Die Täter-Individualprognose (S. 129–141). Heidelberg 1995.

9 Huber, E. / Pospisil B. (Hrsg.), Die Cyberkriminellen von Wien – eine Analyse von 2006–2016, Krems an der Donau 2018.

3.2. Modus Operandi der ungelösten Fälle

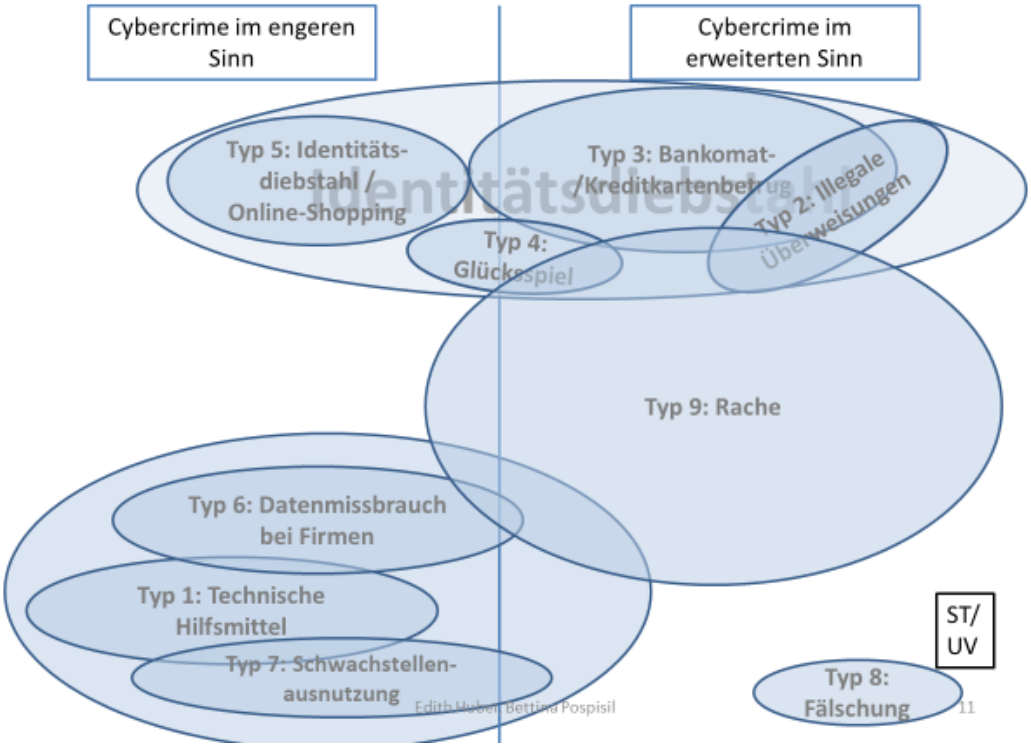

Abbildung 2: Modus Operandi der ungelösten Fälle

Der Modus Operandi der ungelösten Cybercrime-Fälle unterscheidet sich nicht wesentlich von jenem der gelösten Fälle.[10] Unterschiedlich ist die Häufigkeit der einzelnen Tathergänge. Eine detaillierte Beschreibung zu den Modi Operandi findet sich in unserer Analyse der aufgeklärten Fälle.[11] An dieser Stelle erfolgt eine kurze Zusammenfassung. Im Wesentlichen lassen sich drei Arten von Modi Operandi erkennen: Identitätsdiebstahl, Tathergänge unter der Zuhilfenahme technischer Hilfsmittel, Tathergänge aus Motiven der Rache.

Der größte Teil aller Cybercrime-Delikte in Wien fällt unter den Sammelbegriff des Identitätsdiebstahls. Dabei werden Identitäten von Kredit- und Bankkarten, Bezahldaten von Online-Shopping-Portalen, Bezahldaten von Online-Glücksspielportalen sowie Kontodaten für Überweisungen gestohlen. Die Täter haben dabei keine speziellen Informatikkenntnisse. Die Identitäten werden zumeist offline gestohlen und dann missbräuchlich online eingesetzt. Man kann hier von einer sehr niederschwelligen Art der Kriminalität sprechen. Täter und Opfer sind einander zumeist unbekannt. Die meisten dieser Delikte werden unter dem § 148a StGB zur Anzeige gebracht.

[10] Huber, E. / Pospisil, B. / Hötzendorfer, W. / Löschl, L. / Quirchmayr, G. / Tschohl, C., Cybercrime – Hellfeldanalyse der Akten des Wiener Straflandesgerichts von 2006–2016, in: Erich Schweighofer, Franz Kummer, Ahti Saarenpää, Burkhard Schafer, Datenschutz/LegalTech. Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, 519–528, Editions Weblaw.

[11] Ebenda.

Tathergänge unter Zuhilfenahme von technischen Hilfsmitteln subsumieren vor allem jene Delikte, die unter Cybercrime im engeren Sinne fallen. Durch technische Mittel, wie zum Beispiel Malware, Spyware, durch das Ausnutzen einer Schwachstelle oder durch Datenmissbrauch bei Firmen verschafft sich der Täter Zugang zu den Daten von Opfern. Die Täter selbst sind höher qualifiziert und können oft eine Informatikausbildung vorweisen. Die Taten sind strategisch geplant und aufwändig. Diese Delikte werden zumeist unter den §§ 118a, 119, 119a, 126a, 126b, 126c sowie 225a StGB zur Anzeige gebracht. Opfer sind zumeist Firmen und vereinzelt Personen des öffentlichen Lebens.

Tathergänge aus Motiven der Rache stellen eine Besonderheit dar, da sie sich zum Teil aus den anderen schon beschrieben Modi Operandi zusammensetzen. Wesentliches Unterscheidungsmerkmal ist jedoch die bewusste Planung der Tat als Racheakt. Opfer sind immer Privatpersonen, die mittels Identitätsdiebstahl, Kreditkarten-/Bankdatenbetrug oder anderen Formen geschädigt werden sollen. Die Täter planen dabei oftmals strategisch aus den Motiven der Rache die systematische Vernichtung des Opfers. Dazu sind ihnen mehrere Mittel recht. Täter können in diesen Fällen sowohl Frauen als auch Männer sein. Man kann dies auch als eine Ausweitung des Cyberstalkings betrachten. Besonders interessant sind dahingehend die neuesten Entwicklungen angesichts des § 107c StGB, der vermutlich künftig in solchen Fällen häufiger zur Anwendung kommen wird.[12, 13]

Interessantes Detail bei den ungelösten Fällen ist, dass es einen sehr hohen Anteil an Fällen gibt, bei denen Rache das Hauptmotiv ist. Typisches Fallbeispiel dafür wäre: Ein Liebespaar trennt sich nach längerer Beziehung. Er verkraftet die Trennung nicht und möchte sich nun an der Ex-Partnerin rächen. Da beide gemeinsam den Computer benutzt haben, kennt er ihre Zugangsdaten und Passwörter. Kurzerhand setzt er ihr Google-, Facebook- und Instagram-Passwort zurück und postet in ihrem Namen obszöne Bilder. Dies führt einerseits zu psychischen Problemen bzw. einem Reputationsverlust und andererseits zu Problemen des Alltags, denn viele Online-Dienste sind beispielsweise abhängig vom Google-Passwort (z.B. Android-Handy). Das Opfer hat einen erheblichen Aufwand, Daten und Dienste wiederherzustellen.

3.3. Tathergangsmuster der ungelösten Fälle

Im folgenden Kapitel sollen die typischen Tathergangsmuster bzw. -motive der ungelösten Cybercrime-Fälle des Wiener Straflandesgerichts von 2006–2016 erläutert werden. Diese geben Aufschluss über das Motiv des Täters, über die Attacke an sich sowie über die Beziehung zwischen Täter und Opfer.

3.3.1. Revenge-Crime

Rund 43% aller Fälle sind dem Tathergangsmuster bzw. -motiv Revenge-Crime zu subsumieren. Diese fallen unter den Modus Operandi – Typ 9 Rache. Cybercrime wird bewusst eingesetzt, um sich an einer Person zu rächen. Typisches Muster in diesen Fällen ist, dass die Tatverdächtigen fast ausschließlich Einzelpersonen sind. In rund einem Fünftel aller Fälle bestand eine Liebesbeziehung zwischen Tatverdächtigem und Opfer, die aus unterschiedlichen Gründen scheiterte. Das technische Vorgehen entspricht einer sehr einfachen technischen Herangehensweise, der Tatverdächtige verfügt üblicherweise nicht über Informatik- oder spezielle IT-Kenntnisse. Daher setzten die Tatverdächtigen auch keine Verschleierungsmaßnahmen. Es ist davon auszugehen, dass aufgrund der zunehmenden Digitalisierung der unterschiedlichen Lebensbereiche die Überschneidung des Typs Revenge-Crime mit Stalking-Delikten nach §§ 107a bis c StGB groß ist. Dennoch wurden sie unter den §§ 118a, 126a und 126c StGB zur Anzeige gebracht. Bei diesen Fällen zum Typ Revenge-Crime ist der Tatverdächtige aufgrund seiner Nähe zum Opfer sowie der fehlenden technischen Versiertheit im Groß-

[12] § 107c StGB «Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems» gibt es seit Ende 2015. Im Jahr 2016 wurden 302 Fälle zur Anzeige gebracht (Bundesministerium für Inneres Kriminalstatistik 2016; Wien, 2017).

[13] Huber, E. / Pospisil, B. / Hötzendorfer, W. / Löschl, L. / Quirchmayr, G. / Tschohl, C., Cybercrime – Hellfeldanalyse der Akten des Wiener Straflandesgerichts von 2006–2016, in: Erich Schweighofer, Franz Kummer, Ahti Saarenpää, Burkhard Schafer, Datenschutz/LegalTech. Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, 519–528, Editions Weblaw.

teil der Fälle bekannt (87%). Zumeist einigen sich Täter und Opfer außergerichtlich bzw. das Opfer lässt die Anklage fallen.

3.3.2. Financial-Crime

Rund ein Drittel aller Fälle (29%) ist der Kategorie Financial-Crime zuzuordnen. Das Motiv der Tatverdächtigen, die zumeist in kleinen kriminellen Organisationen agieren, ist die finanzielle Bereicherung. Typischerweise besteht keine Beziehung zwischen dem Tatverdächtigen und dem Opfer. Bei diesen handelt es sich auch hier in den meisten Fällen um Privatpersonen, aber auch Firmen sind betroffen. Das Vorgehen ist bereits etwas komplexer als im Revenge-Crime, jedoch immer noch eher simpel und erfordert keine spezielle Ausbildung oder spezifische IT-Kenntnisse. Dies spiegeln auch die Verschleierungsmaßnahmen wieder, die zwar vereinzelt eingesetzt werden, jedoch keine hohe Komplexität aufweisen. Innerhalb des Typs Financial Crime passiert die Opferwahl zumeist nach der offenen Schwachstelle. Dies hängt mit dem Motiv zusammen, dass der Täter mit möglichst wenig Aufwand einen möglichst hohen finanziellen Ertrag erzielen möchte. Die Angriffe passieren häufig über Social Engineering, die Schwachstelle ist somit die Leichtgläubigkeit bzw. Unwissenheit des Opfers. In diesen Fällen ist weniger als die Hälfte (43%) der Tatverdächtigen bekannt. Angezeigt werden sie zumeist unter §§ 118a und 126c.

3.3.3. Show-Off-Crime

Der Typ Show-Off Crime umfasst 13% der analysierten Fälle. Auch hier ist der Tatverdächtige zumeist in Gruppen organisiert, die sich über das gemeinsame Interesse an der Informations- und Kommunikationstechnologie gruppierten. Aus diesen Gruppen heraus entsteht das Motiv, zu brillieren und der Welt die eigenen Fähigkeiten und damit einhergehenden Möglichkeiten zu demonstrieren. Diese Gruppen an Tätern haben meist keine Beziehung zu ihrem Opfer und greifen in erster Linie Behörden oder Firmen an. Ihr Ziel ist dabei immer, möglichst große Aufmerksamkeit zu erzielen um die eigenen Kenntnisse unter Beweis zu stellen. Die Tatverdächtigen verfügen im Normalfall über Wissen im Umgang mit IT-Technologien, welches sie entweder durch eine Ausbildung erhielten oder sich selbst aneigneten. Sie legen ein eher komplexeres Vorgehen an den Tag und nutzen dazugehörige Verschleierungsmaßnahmen um ihren Wunsch nach Aufmerksamkeit zu erfüllen. Auch aus diesem Grund handelt es sich bei den Angriffen meist um Attacken offener Schwachstellen, wobei es sich dabei zumeist um öffentlich bekannte Sicherheitslücken im Zielsystem handelt. Von Tool-basierten Angriffsformen bis hin zur Distributed-Denial-of-Service (DDoS-)Attacke werden unterschiedliche Verfahren angewendet. Mit 54% sind mehr als die Hälfte der Tatverdächtigen bekannt. Fälle des Show-Off Crime werden jedoch meist nicht aufgeklärt, da sich die Tatverdächtigen darauf verstehen, digitale Tatmittel und Beweise zu vernichten. Die Delikte werden meist unter den §§ 126a und 126c StGB angeklagt.

3.3.4. Conviction Crime

5% der Fälle können unter den Typ des Conviction Crime subsumiert werden. Tatverdächtige dieses Typs haben das Motiv, ihren Glauben bzw. ihre Ideologie zu verbreiten. Da sie hierfür vor allem auf der Suche nach geeigneten Plattformen sind, attackieren sie in erster Linie Websites, um deren Inhalte abzuändern. Tatverdächtige dieses Typs agieren meist in Gruppierungen mit der gleichen Ideologie und wählen ihre Opfer nach einer offenen Schwachstelle aus. Dabei können sowohl Privatpersonen als auch Firmen Opfer werden, eben jeder, der einen Web-Auftritt hat. In vielen Fällen kommt es zu einem Reputationsschaden des Opfers, durch die von der Gruppierung hochgeladenen, verhetzenden Inhalte.

3.3.5. Follower Crime

Häufig in Verbindung mit Show-Off Crime, tritt der Typ des Follower Crime auf. Rund 4% der Fälle können unter diesen Typ zusammengefasst werden. Da Tatverdächtige des Typs Show-Off Crime ihre Tat gerne in sozialen Netzwerken teilen bzw. die widerrechtlich erlangten Zugangsdaten und Informationen zur Straftat weitergeben, nutzen auch andere diese sich hier bietenden Möglichkeiten. Der Tatverdächtige des Follower

Crime begeht somit aus Neugierde oder aus einem fehlenden Bewusstsein heraus eine Straftat. Diese ist demnach weder zielgerichtet noch komplex.

4. Vergleich der Aktenanalysen

Wie bereits erwähnt finden sich in Bezug auf den Modus Operandi einige Gemeinsamkeiten zwischen den Akten der Hauptverhandlung und jenen der Staatsanwaltschaft. Auch bei den Täter- und Opferprofilen ist von Gemeinsamkeiten auszugehen, wobei diese bei der aktuellen Studie, aufgrund der fehlenden Informationen in den Akten, nicht überprüft werden konnten.

Neben einigen Gemeinsamkeiten fanden sich jedoch auch Themen in welchen sich große Unterschiede zwischen den Akten fanden. Im Gegensatz zu den Fällen der ersten Analyse, finden sich in dieser zweiten Analyse der Akten der Staatsanwaltschaft sehr viel mehr Fälle, in welchen der Täter unbekannt blieb (37,5%). Dies liegt zum Teil auch daran, dass die Täter in diesen Fällen technisch versierter agieren bzw. auch vermehrt Verschleierungsmaßnahmen einsetzten. Auch die Attacken sind, betrachtet man die ungeklärten Fälle, heterogener und komplexer. So finden sich im Gegensatz zu den geklärten Fällen hier auch Crime as a Service, D(D)oS-Attacken und kriminelle Finanzgeschäfte. Zusammenfassend kann also geschlossen werden, dass technisch weniger komplexe Delikte eher aufgeklärt werden als andere. Die Opfer waren bei dieser Analyse vermehrt Privatpersonen (HV: 21%, ST: 47%), was auch den verhältnismäßig hohen Anteil an Fällen erklärt, bei welchen die Schwachstelle die Leichtgläubigkeit und Unwissenheit des Opfers (38%) war.

Gründe für die Nichtaufklärung der Fälle sind vor allem die fehlenden Gründe zur weiteren Verfolgung, fehlende Anhaltspunkte und Beweise, der mangelnde Tatbestand, die fehlende Motivation der Anklage sowie die Nichtzuständigkeit der Staatsanwaltschaft.

5. Schlussfolgerungen

Basierend auf den Ergebnissen des Forschungsprojektes können zwei wesentliche Schlussfolgerungen gezogen werden: (1) Es benötigt einen Ausbau des Wissens speziell des juristischen und polizeilichen Personals zum Umgang mit Cybercrime und Cybersicherheit. (2) Darüber hinaus benötigt es einen effizienteren Einsatz der bestehenden Ressourcen von Polizei und Justiz hinsichtlich Zuständigkeiten und Auslastung.

Zu (1) zeigt sich, dass die Ermittlungen zum Thema Cybercrime in einer Spirale feststecken, welche nur durch einen Ausbau von Wissen durchbrochen werden kann. Das fehlende (a) Wissen des juristischen Personals, aber auch der Exekutive, zum Thema Cybercrime führt zu einer (b) unzureichenden Behandlung in Hinblick auf mögliche Ermittlungsverfahren (z.B. digitale Tatmittel, digitale Beute, Auslesen von Logfiles, …). Dies wiederum führt dazu, dass (c) notwendige Informationen nicht gewonnen werden können, wodurch es zu einer (d) unzureichenden Aufarbeitung des Falls kommt. Dies gipfelt nun darin, dass auch (e) die Prävention nicht verbessert werden kann und somit (f) keine Rückführung neuen Wissens aus der Praxis möglich ist. Dieser Wissensausbau könnte durch spezifische Weiterbildungen erreicht werden.

Vor dem Hintergrund einer beschränkten Verfügbarkeit hochqualifizierter Experten wird es (2) nötig sein diese Kapazitäten für technisch und kriminalistisch anspruchsvolle Fälle einzusetzen. Dies hat zur Folge, dass im Bereich der kriminalpolizeilichen Arbeit einerseits ein weiterer Aufbau von Experten erforderlich sein wird, andererseits ein breiter gestreutes Wissen verfügbar gemacht werden muss, um die vorhandenen Expertenkapazitäten von «Alltagsfällen» zu entlasten. Dazu ist eine entsprechende Basisausbildung der Polizei auf breiter Basis notwendig. In Zukunft sollte es daher eine klare Trennung zwischen technologisch anspruchsvollen Fällen und jenen Fällen geben, in denen IKT nur als Tatmittel zur Begehung traditioneller Vergehen (Betrug, Diebstahl) verwendet wird. Die bereits jetzt vorhandenen ausgezeichneten Experten müssen im Sinne von «silver-bullets» auf anspruchsvolle Fahndungen konzentriert werden.

6. Literaturverzeichnis

Bundesministerium für Inneres, Kriminalstatistik 2016, Wien 2017.

Bundesministerium für Inneres, Kriminalstatistik 2017, Wien 2018, abgerufen über statista, 5. Januar 2019.

Dölling, D., Probleme der Aktenanalyse in der Kriminologie, in: Die Täter-Individualprognose (S. 129–141). Heidelberg 1995.

Huber, E. / Pospisil B. (Hrsg.), Die Cyberkriminellen von Wien – eine Analyse von 2006–2016, Krems an der Donau 2018.

Huber, E. / Pospisil, B. / Hötzendorfer, W. / Löschl, L. / Quirchmayr, G. / Tschohl, C., Cybercrime – Hellfeldanalyse der Akten des Wiener Straflandesgerichts von 2006–2016, in: Erich Schweighofer, Franz Kummer, Ahti Saarenpää, Burkhard Schafer, Datenschutz/LegalTech. Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, 519–528, Editions Weblaw.

Kirwan, G. / Power, A., Cybercrime, Cambridge University Press 2013.

McGuire, M. / Dowling, S., Cyber crime: A review of the evidence, 2013.