RACHE 4.0 – EINE NEUE FORM DER CYBERKRIMINALITÄT

Edith Huber / Bettina Pospisil

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

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

Abstract: *Rache an Ex-Partnern, ehemaligen Firmenchefs, Unternehmen oder Staaten – Rachedelikte haben viele Gesichter und begegnen uns häufiger als man am ersten Blick erkennen würde. Mit der Ausbreitung internetfähiger Geräte, ist es leicht geworden die persönliche Rache über dem anonymen Cyberspace auszuüben. Der Beitrag beleuchtet die theoretischen Konzepte der Rache und erklärt, wie diese mit Hilfe des Cyberspace und vor allem der Ausbreitung des IoT Verbreitung findet. Darüber hinaus werden Ergebnisse aus zwei Forschungsprojekten zusammengeführt, um die Bedrohungslage näher zu beschreiben.*

Das Forschungsvorhaben wurde im Rahmen der österreichischen Sicherheitsforschung KIRAS, Programmlinie 2-3 gefördert. Projektname «CERT-Komm II» sowie dem Projekt ARES «Angriffsresiliente IoT-basierte Sensoren in der Heimautomation» der Niederösterreichischen Forschungs- und Bildungsgesellschaft gefördert.

1. Einleitung

«*Perpetrators engage in persistent destructive behavior, whether it occurs online, offline, or both. The cyber label adds something important, however. It captures the different ways the Internet exacerbates the injuries suffered*.» (Citron 2014: S. 4)

Rache im Netz ist längst nicht mehr ein Delikt, das ausschließlich Privatpersonen betrifft. Immer häufiger werden Sicherheitslücken von Unternehmen und Staaten ausgenutzt, um diesen – aus einem privaten Motiv (oftmals Rache) heraus – Schaden zuzufügen. Damit hat sich eine weitere Facette der Cyber-Kriminalität entwickelt. Mit der stetigen Ausweitung von IoT-Geräten steigen jedoch auch die Angriffsmöglichkeiten im privaten Bereich.

> *Fallbeispiel: Hans und Eva trennen sich und Hans muss aus dem gemeinsamen Haus ausziehen. Doch nur er hat Zugang zu den IoT-Geräten des Haushaltes, wie die über das Internet steuerbaren Jalousien, den Rasenmäher und die Heizung. Aus Zorn über die Trennung schaltet er zur Rache willkürlich im Winter die Heizung an und wieder aus. Eva bleibt nur noch der Weg zum Gericht, um dieses Verhalten zu unterbinden.*

So analysierte beispielsweise Kasperky auf der Basis einer Telemetrie-Analyse von 40.000 – zufällig ausgewählter – Kunden, dass immer mehr IoT Geräte mit Cyber-Angriffen konfrontiert sind.[1] Aber auch im Arbeitsumfeld werden Rachedelikte immer häufiger. Fakenews oder Hasspostings sind ein Mittel, wie sich

[1] Roesner, M.: Cyberattacken auf Smart Buildings: 37,8 Prozent im ersten Halbjahr betroffen, https://www.kaspersky.de/blog/cyber-attacken-auf-smart-buildings/20289/, 16.10.2019.

ehemalige MitarbeiterInnen an ihrem Arbeitgeber rächen wollen. Aber auch der bewusste Datendiebstahl in Unternehmen ist eine Facette dieser Kriminalitätsart. In diesem Beitrag soll auf das Phänomen Revenge-Crime mit dem speziellen Fokus auf Rache-Delikte im Bereich der Cyber-Kriminalität eingegangen werden. Dazu wird im ersten Abschnitt das Phänomen Rache generell und ihre Verbindung zur Kriminalität skizziert. In einem weiteren Schritt wird auf den rechtlichen Rahmen von Rachedelikten im Cyberspace in Österreich eingegangen und daraufhin eine Studie zur Typisierung verschiedener Rachedelikte im Cyberspace präsentiert. Abschließend werden aus der Verschränkung von Theorie und Praxis Schlussfolgerungen formuliert.

2. Eine Dreiecksbeziehung: Rache, Cyber-Kriminalität und Recht

«Der Gedanke an Rache ist was Tröstliches»

(Reinhard Haller*, 10.12.2019 in der ORF-Sendung «Willkommen Österreich»)*

2.1. Das Phänomen der Rache

Das Konzept der Rache ist seit jeher ein interessantes für die Fachbereiche der Psychologie und Soziologie, wo sich die unterschiedlichsten Definitionen dazu finden. Grundsätzlich liegt hinter der Rache der Wunsch, dass einem Gegenüber Ähnliches, wie der selbst erlittene Schaden zugefügt werden soll, um einen gewissen Ausgleich herzustellen.[2, 3] Manche Autoren definieren die Racheaktion dabei als Handlung, die einen Lerneffekt ausüben soll,[4] oder als proaktive Strategie zur Bewältigung von Unrecht.[5] Die Psychologie kennt dabei unterschiedliche Interpretationen. Wenn von Rache gesprochen wird, gibt es stets zwei Opfer(gruppen), den Erstgeschädigten – wobei dieser Akt der ersten Schädigung korrespondierend mit anderen Faktoren das Rachegefühl auslöst – und den Zweitgeschädigten, welcher unter der Rachehandlung des Erstgeschädigten leidet. Somit kommt es zu einer TäterInnen/Opfer-Umkehr. Das Opfer wird aufgrund unterschiedlichster Faktoren selbst zum/r TäterIn und macht dabei den/die TäterIn der ursprünglichen Handlung zum Opfer. Dieser Prozess kann sich mehrfach wiederholen, Maes spricht dahingehend von einem «Rachezirkel».[6] Der Wunsch nach Rache entspringt zumeist aus dem – der verwerflichen Ersthandlung zugrundeliegenden – Angriff gegen das eigene Wertekonstrukt: *«Entscheidend ist also nicht nur und per se der Angriff auf den persönlichen oder sozialen Status einer Person, sondern jedweder Angriff, der sich auf Werte richtet, die für die Konstruktion der Identität der geschädigten Person konstitutiv sind.»*[7]

Unterschiedliche wissenschaftliche Studien zeigen, dass der Wunsch nach Rache als grundlegende Motivation hinter den unterschiedlichsten Kriminalitätsformen steht.[8, 9, 10] Diesen Aspekt findet man auch in der Cyber-Kriminalität wieder.

---

2 Frijda, N. H. (1994). The Lex Talionis: On vengeance. In S. H. M. van Goozen, N. E. van der Poll, & J. A. Sergeant (Hrsg.) Emotions: Essays on emotion theory, 263–289. Hillsdale, NJ: Erlbaum.

3 Tripp, M., & Bies, R. J. (1997). What's good about revenge? The avenger's perspective. In R. J. Lewicki, R. J. Bies, & B. H. Sheppard (Hrsg.), Research on negotiation in organizations 6: 145–160. Greenwich, CT: JAI.

4 Heider, F. (1977). Psychologie der interpersonalen Beziehungen. Stuttgart: Klett.

5 Gollwitzer, M. (2004). Eine Analyse von Racheaktionen und rachebezogenen Reaktionen unter gerechtigkeitspsychologischen Aspekten. Dissertation an der Universität Trier, Fachbereich Psychologie.

6 Maes, J. (1994). Psychologische Überlegungen zu Rache. Berichte aus der Arbeitsgruppe «Verantwortung, Gerechtigkeit, Moral». Nr. 76. Universität Trier, Fachbereich I – Psychologie. S. 5f.

7 Gollwitzer, M. (2004). S. 10.

8 Kivivuori, J., Savolainen, J., & Aaltonen, M. (2016). The revenge motive in delinquency: Prevalence and predictors. Acta Sociologica 59(1), S. 69–84.

9 Levin J., & Madfis E. (2009). Mass murder at school and cumulative strain: A sequential model. American Behavioral Scientist 52(9): 1227–1245.

10 Mann R. E., & Hollin C. R. (2007). Sexual offenders' explanations for their offending. Journal of Sexual Aggression 13(1): 3–9.

2.2. Rache als Form der Cyber-Kriminalität

Auf diese Verbindung zwischen Rache und Kriminalität treffen die Möglichkeiten eines vermeintlich anonymen Cyberspace als Tatort. Damit wird es einzelnen Personen leichter gemacht Rache-Delikte über das Internet zu verrichten. Bei der Beschäftigung mit Cyber-Kriminalität können grundsätzlich zwei Arten dieser unterschieden werden.[11, 12, 13, 14] a) Cybercrime im engeren und b) Cybercrime im weiteren Sinne. Beim a) Cybercrime im engeren Sinne (auch Cyber-dependent crime u.a.) ist von jener Kriminalität die Rede, die nur im Rahmen des Cyberspace möglich ist, die es also in keiner Form offline gibt. Beispiele sind technologiebezogene Attacken wie die Verbreitung von Malware oder der Angriff auf Internetverbindungen bzw. -auftritte. Mit b) Cybercrime im weiteren Sinne (auch Cyber-enabled crime u.a.) sind solche Vergehen gemeint, welche es auch offline gibt und in den letzten Jahren eine Ergänzung um, oder eine Verschiebung in den Cyberspace erlebten. In diese Kategorie zählen Kriminalitätsformen, wie Betrug, Datendiebstahl, das Stehlen von Geschäftsgeheimnissen und Stalking genauso wie Kinderpornografie. Das Motive der Rache findet sich dabei in beiden Varianten der Cyber-Kriminalität.

3. Der rechtliche Rahmen für Rachedelikte im Cyberspace

«*Entsteht ein dauernder Schaden, so sollst du geben Leben um Leben, Auge um Auge, Zahn um Zahn, Hand um Hand, Fuß um Fuß, Brandmal um Brandmal, Beule um Beule, Wunde um Wunde*.»
(Exodus 21,23–25 LUT, Altes Testament.)

Da sich die Bezeichnung Rachedelikte auf die Motivation hinter der Tat bezieht, kommen im Grunde die verschiedensten Arten von Delikten als solche in Frage. So kann eine Person aus Rache jemanden bedrohen oder verfolgen, aber auch ein Mord kann aus Rache begangen werden. Rachedelikte haben somit viele Gesichter. Cybercrime-Delikte im engeren Sinne sind dahingehend leichter einzugrenzen. Die rechtliche Situation in Österreich spiegelt sich im StGB wie folgt: Widerrechtlicher Zugriff auf ein Computersystem (§ 118a), Verletzung des Telekommunikationsgeheimnisses (§ 119), Missbräuchliches Abfangen von Daten (§ 119a), Datenbeschädigung (§ 126a), Störung der Funktionsfähigkeit eines Computersystems (§ 126b), Missbrauch von Computerprogrammen (§ 126c), Betrügerischer Datenverarbeitungsmissbrauch (§ 148a), Datenfälschung (§ 225a), Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c). Beim Cybercrime im weiteren Sinne werden auch hier die Angaben abstrakter. Folgende Delikte werden diesbezüglich genannt: Pornographische Darstellungen Minderjähriger (§ 207a), Internetbetrug und Sonstige Straftaten im Internet. Darüber hinaus kommt es immer häufiger zu Anzeigen im Sinne des § 297 Verleumdung, § 111 Üble Nachrede und § 115 Beleidigung. Dieser rechtliche Rahmen bietet die Grundlage, für eine Betrachtung von Revenge-Crime als Form von Cyber-Kriminalität.

[11] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Zugegriffen: 22. August 2019.

[12] Furnell, S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. At Second Australian Information Warfare and Security Conference 2001.

[13] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology 2: 13–20.

[14] United Nations (2000). Crimes related to computer networks. Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf. Zugegriffen: 22. August 2019.

4. Präsentation der Studienergebnisse

Auf Basis einer Aktenanalyse am Wiener Straflandesgericht[15] wurden jene Fälle von Cyber-Kriminalität näher analysiert, die aus dem Motiv der Rache heraus durchgeführt wurden.[16] Dabei konnten vier TäterInnentypen unterschieden und der typische Modus Operandi ausgewertet werden. Die Daten wurden qualitativ und quantitativ analysiert und werden an dieser Stelle zusammengefasst dargestellt:

4.1. Typ 1: Der private Insider

Fallbeispiel: Der Täter wurde von seiner Freundin verlassen und sinnt nach Rache. Er kennt die Zugangsdaten der Ex-Freundin zum GMail-Konto, steigt mit diesen ein, ändert das Passwort und führt den Account unter falschem Namen weiter bzw. sieht private Daten ein. Durch das gestohlen GMail-Konto kann nun die Ex-Freundin auf keine Dienste von GMail zugreifen.

In solchen Fällen ist das Opfer typischerweise eine Privatperson. Der/Die TäterIn steht in einem Vertrauensverhältnis zum Opfer und kennt schutzwürdige Daten, wie zum Beispiel Passwörter zu unterschiedlichen Portalen (Social Media, E-Mailprogramm etc.). Typischer Tathergang: In diesen Accounts werden Daten gelesen, kopiert, weitergegeben, gelöscht, neu hinzugefügt, verändert. Es werden zielgerichtet Falschinformationen über das Opfer verbreitet. Meist, wird der eigentliche Account des Opfers gesperrt, sodass es nicht mehr auf die betreffende Plattform zugreifen kann. Der Racheakt besteht darin, dass mit dem Besitz des Accounts nun bestimmte Handlungen durchgeführt werden können, um das Opfer zu schädigen. So ist es mit der Ausweitung der IoT-fähigen Endgeräte möglich, dass Heizungen, Rasenmäher oder Licht ein- und ausgeschalten werden.

4.2. Typ 2: Der berufliche Insider

Fallbeispiel: Der Täter fühlt sich durch seinen Arbeitgeber ungerecht behandelt und stiehlt aus Rache Ordner und Festplatten der Firma, auf welchen sich Betriebsgeheimnisse befinden. Diese Daten werden einem Wirtschaftsprüfer zugespielt.

TäterIn und Opfer stehen hier meist in einem beruflichen Verhältnis, in Konkurrenz bzw. in einem Bekanntschaftsverhältnis. Der/Die TäterIn kennt die typischen Schwachstellen des IT-Systems, der Prozesses oder die mangelnden Sicherheitsvorkehrungen anderer Mitarbeiter und nutzt dieses Wissen aus.[17] In den meisten Fällen wird dieser Racheakt durch ein berufliches Frustrationserlebnis ausgelöst, wie die Kündigung durch den Arbeitgeber oder eine langandauernde Frustration aufgrund persönlich empfundenen Schadens (z.B. schlechte Bezahlung, Bevorzugung anderer Kollegen, falsche Versprechen oder, dass man einfach das Gefühl hat, nicht gehört zu werden.). Primäres Ziel ist zumeist die mutwillige Schädigung des Chefs des Unternehmens, um so dem Unternehmen einen Schaden hinzuzufügen. Der Modus Operandi kennzeichnet sich dadurch, dass bewusst Fehlinformationen verbreitet, Betriebsgeheimnisse weitergegeben und Berechtigungen zu Systemen nicht ordnungsgemäß verwendet werden. Der/Die TäterIn nimmt unerlaubt Einsicht in Daten, ändert oder löscht sie bzw. gibt sie an Dritte weiter. Vielerorts passieren solche Delikte auch aufgrund der mangelnden Absicherung des IT-Systems. In manchen Fällen ist es den Tätern möglich auch nach dem Ausscheiden aus dem Unternehmen noch auf die Ressourcen der Firmen zuzugreifen.

[15] N=5.405, Untersuchungszeitraum 2006–2016. Akten der Staatsanwaltschaft und Akten des Gerichts.

[16] Details dazu unter: Huber, E.; Pospisil B. (Hrsg.), Die Cyberkriminellen von Wien – eine Analyse von 2006 – 2016, Krems an der Donau, 2018.

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

4.3. Typ 3: Der Cyberstalker

Fallbeispiel: Der Täter wollte eine Liebesbeziehung mit dem Opfer führen, wurde von diesem jedoch zurückgewiesen. Als Reaktion darauf sendet er ihr über Facebook, Mail und SMS unzählige Nachrichten, bestellt Sexspielzeug unter ihrem Namen und erstellt eine Homepage, auf der er herabwürdigende Fotos und private Informationen zu ihrer Person postet.

Der Begriff Cyberstalking ist eine Verbindung der Worte «Cyber» und «Stalking». Stalking kann laut Meloy (1998) in zweierlei Hinsicht interpretiert werden, nämlich

«*(1) to gather private information on the target to further a pursuit; and (2) to communicate (in real time or not) with the target to implicitly or explicitly threaten or to in-duce fear.*»[18]

Es geht also im Wesentlichen um die obsessive, langanhaltende und fortdauernde Belästigung eines Menschen, die seine Lebensführung beeinträchtigt (§107a StGB). Diese Definition ist sehr wichtig, da sich mittlerweile im umgangssprachlichen Wortgebrauch falsche Definitionen des Wortes Stalking verbreitet haben. So bezeichnen manche Personen schon den Umstand als Stalking, wenn eine dritte Person Informationen über sie recherchiert. Wissenschaftlich gesehen spricht man von Stalking, wenn es sich um eine obsessive Belästigung, über einen längeren Zeitraum hindurch handelt.[19] Stalking ist an und für sich kein neues Phänomen, bekommt jedoch mit der Ausbreitung der Telekommunikation eine neue Bedeutung. So besaßen im Jahr 2019 rund 77 Prozent der Österreicher ab 15 Jahren ein Smartphone.[20] Darüber hinaus nutzen rund 6,59 Mio. Personen das Internet.[21] Die ständige Verfügbarkeit der Telekommunikation ermöglichen ein anonymes und sofortiges Agieren des Täters. Dabei werden zwei Arten von Cyberstalking unterschieden, nämlich Cyberstalking im engeren Sinn und Cyberstalking im weiteren Sinn: Im engeren Sinn: «*Jene Verhaltensweisen, die die persönliche Freiheit, konkret die Willensbildungsfreiheit oder die Freiheit der Willensbetätigung, unter Zuhilfenahme elektronischer Kommunikationsmittel beeinträchtigen. Damit erfasst der Terminus Cyberstalking ieS [Anm: im engeren Sinn] neben Drohungen und Nötigungen auch Handlungen, die aufgrund ihrer Kontinuität und Dauer zu einer unzumutbaren Beeinträchtigung der Lebensführung führen.*»[22] «*Hingegen enthält der Begriff Cyberstalking im weiteren Sinn neben Angriffen auf Computersysteme und ehrenrührige Veröffentlichungen auf Webseiten, in Online-Foren oder in Social Network-Profilen auch unliebsames Veröffentlichen von Fotos*»[23]

In zahlreichen Fällen waren TäterIn und Opfer einmal in einer Liebesbeziehung oder der/die TäterIn stellt sich eine Liebesbeziehung mit dem Opfer vor. Aufgrund dieser Ausgangssituation, weist der Tätertyp 3 einige Parallelen zum Tätertyp 1 auf. Entscheidender Unterschied ist jedoch das Vorgehen: Während beim ersten Tätertyp eine bestehende Vertrauensbeziehung ausgenutzt wird, geht es dem Cyberstalker darum, sich zusätzliche private Informationen anzueignen. Der Tätertyp nutzt illegale Methoden, um digitale oder auch offline Informationen über das Opfer zu sammeln. Darüber hinaus kommt es im Zuge des Cyberstalking zur obsessiven Belästigung. Dabei kann das Opfer offline und online einen Schaden erleiden. Es kommt zu häufigen Kontaktaufnahmen über die unterschiedlichsten Kanäle (E-Mail, Social Media, Chat-Programme etc.). In dieser Konstellation gibt es in Vergleich zu anderen Delikten einen höheren Anteil an TäterInnen.

---

18 Pathé, M., & Mullen, P. (1997). The impact of stalkers on their victims. British Journal of Psychiatry, 170(1), 12–17. doi:10.1192/bjp.170.1.12, S.12.

19 Huber, E. (2019). Cybercrime. Eine Einführung. Wiesbaden. Springer.

20 Handelsverband Österreich (2019). https://www.handelsverband.at/fileadmin/content/images_events/eCommerce_Day_2019/Praesentationen_EDC/Gittenberger_KMU_Forschung.pdf, 16.12.2019.

21 INTEGRAL (2019) AIM – Austrian Internet Monitor, rep. Österr. ab 14 Jahren, April bis Juni 2019+Q1 2019, n=1.000 telefonische Interviews. https://www.integral.co.at/downloads/Internet/2019/08/AIM-C_-_Q2_2019.pdf. 16.12.2019.

22 Huber, E. (2012). Cyberstalking und Cybercrime – Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher. Wiesbaden. Springer. S. 12.

23 Forgo, N. et al. (2010). «Juristische Untersuchung.» In Forschungsbericht – Cyberstalking – Österreichweite Studie Zum Cyberstalking-Verhalten, S. 155. Wien: Huber, E. (2012).

4.4. Typ 4: Der Konkurrent

Fallbeispiel: Das Opfer deckt Linkfarms verschiedener Anbieter auf und wird daraufhin von unbekannten Tätern mittels falscher IP-Adressen und Spam-Emails angegriffen. Diese überlasten die Homepage des Opfers mit einer Denial-of-Service (DoS)-Attacke bis es zu einer Funktionsstörung kommt.

In diesem Fall werden berufliche und private Motive vermischt. TäterIn und Opfer stehen in Konkurrenz, dabei kann man zwei verschiedene Arten des Konkurrenzverhältnisses unterscheiden: a) Die Konkurrenz um Kunden (z.B. zwei Vertreter desselben Gewerbes), b) Konkurrierende Ideale (z.B. White Hat Hacker vs. Black Hat Hacker). Während im ersten Fall häufig Falschinformationen verbreitet werden, um die Reputation des Konkurrenten zu schädigen, kommt es im zweiten Fall häufig zu einem virtuellen Kräftemessen.

5. Schlussfolgerungen

5.1. Kränkung führt zum Wunsch nach Rache

Das Motiv der Rache ist bei Cybercrime-Delikten keine Seltenheit. Je nach Art des Delikts steht nicht nur der Wunsch nach finanzieller Bereicherung, sondern auch nach persönlicher Rache im Vordergrund. In den meisten Fällen löst die Verletzung des Selbstwertes oder eine Kränkung, beim/bei der Erstgeschädigten den Wunsch nach Rache aus. Ob es sich nun um eine/n MitarbeiterIn handelt, der/die sich nicht ausreichend gewürdigt, einen Partner, der sich hintergangen, einen/r Cyberstalker/in der sich zurückgewiesen oder eine/n Konkurrenten/in der/die sich herausgefordert fühlt. Der/Die Erstgeschädigte erfährt eine subjektive Kränkung und möchte mit Hilfe der Rache vor allem seinen Selbstwert wiederherstellen. Das kann über unterschiedliche Mechanismen erreicht werden, die selbst erhöhend wirken. Dazu zählen (1) das Verlangen nach Macht und Kontrolle, (2) die Belehrung und Bestrafung sowie (3) die Bekräftigung der eigenen Werte und Normen.

5.2. Wie auf die neue Kriminalitätsform reagieren?

Mit Blick auf die vier Typen von Revenge-Crime, die in der aktuellen Studie ausfindig gemacht werden konnten, zeigt sich ein zentraler Ansatzpunkt: die Weiterentwicklung von Bewusstsein und Kompetenz.

Diese Weiterentwicklung bezieht sich auf unterschiedlichste Zielgruppen und sollte ebenso an diese angepasst werden. In Bezug auf die Gesamtgesellschaft ist es notwendig das Bewusstsein für Cyber-Kriminalität zu erhöhen. Viele der in dieser Studie gesichteten Delikte wären durch einen skeptischeren Umgang mit sensiblen und sicherheitsrelevanten Informationen vermeidbar oder zumindest eindämmbar gewesen. So sollten auch in einer Liebes- oder Geschäftsbeziehung nur jene Zugänge und sicherheitsrelevanten Informationen geteilt werden, die unbedingt notwendig sind. Passwörter sollten nicht öfter verwendet und nach der Beendigung einer Beziehung bzw. eines Dienstverhältnisses, in welcher bzw. welchem diese offengelegt wurden, geändert werden.

In Bezug auf juristisches und polizeiliches Personal, konnte die Studie aufzeigen, dass vielen MitarbeiterInnen das Wissen über oder die Routine im Umgang mit Cybercrime-Delikten fehlt. Aus diesem Grund werden bestehende Ermittlungsmethoden, die häufig zur Aufklärung von Fällen beitragen könnten, nicht ausgeschöpft. Nur mit einer umfassenden Basis-Ausbildung kann der steigenden Verschiebung von Kriminalitätsdelikten vom offline in den online Bereich begegnet werden. Darüber hinaus wird es vor dem Hintergrund einer beschränkten Verfügbarkeit hochqualifizierter ExpertInnen nötig sein, diese für technisch und kriminalistisch anspruchsvolle Fälle einzusetzen. Das hat zur Folge, dass im Bereich der kriminalpolizeilichen Arbeit ein Aufbau von ExpertInnen erforderlich sein wird, welche durch die grundlegend ausgebildete Basis vom Tagesgeschäft befreit ist. 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.[24]

[24] Huber, E. (2019). Cybercrime. Eine Einführung. Wiesbaden. Springer.

5.3. Ausblick

Rachedelikte sind so alt wie die Menschheit selbst und somit bei weitem kein neues Phänomen. Trotzdem stellt die Verschiebung dieser Kriminalitätsform in dem Cyberspace dieses altbekannte Phänomen in einen hochmodernen Kontext und verändert damit dessen Wirkungsweise.

Immer häufiger werden Rachedelikte im beruflichen Umfeld. Die Ursachen dafür sind, wie bei allen anderen Situationen im Rachekontext die gleichen. Dies kann aber für betroffene Unternehmen unangenehme, wenn nicht existenzbedrohende Folgen haben. Neue Herausforderungen stellen unter anderen auch Fakenews da. Immer häufiger werden von ehemaligen MitarbeiterInnen oder KonkurrentInnen Falschnachrichten über Social-Media verbreitet. So berichtet beispielsweise der European Communication Monitor, dass bereits 2018 jedes vierte Unternehmen in Europa von Fakenews betroffen war.[25]

In Bezug auf den privaten Lebensbereich sind insbesondere mit der Ausweitung von IoT Geräten Revenge-Crime-Fälle keine Kavaliersdelikte mehr. Durch den nicht geregelten Umgang mit Passworten ist es potentiellen TäterInnen möglich, Opfer zu terrorisieren und deren mobile Endgeräte zu manipulieren. Juristisch wird man diesen Vergehen nur langsam Herr. Benötigt es doch zumeist eine Vielzahl von juristischen Schritten, um solche Verhaltensweisen zu beenden. Dies stellt für die Opfer eine unzumutbare Belastung dar.

6. Literatur

Citron, D. K. (2014). Hate Crimes in Cyberspace. Cambridge, Massachusetts, London: Harvard University Press.

Grupe, M. (2018) Europas Unternehmen Vernachlässigen den Kampf Gegen Fake News, European Communication Monitor, https://www.ffpr.de/2018/06/13/europas-unternehmen-vernachlaessigen-den-kampf-gegen-fake-news/.

Frijda, N. H. (1994). The Lex Talionis: On vengeance. In S. H. M. van Goozen, N. E. van der Poll, & J. A. Sergeant (Hrsg.) Emotions: Essays on emotion theory, 263–289. Hillsdale, NJ: Erlbaum.

Furnell, S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. At Second Australian Information Warfare and Security Conference 2001.

Gollwitzer, M. (2004). Eine Analyse von Racheaktionen und rachebezogenen Reaktionen unter gerechtigkeitspsychologischen Aspekten. Dissertation an der Universität Trier, Fachbereich Psychologie.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology 2: 13–20.

Handelsverband Österreich (2019). https://www.handelsverband.at/fileadmin/content/images_events/eCommerce_Day_2019/Praesentationen_EDC/Gittenberger_KMU_Forschung.pdf.

Heider, F. (1977). Psychologie der interpersonalen Beziehungen. Stuttgart: Klett.

Huber, E. (2012). Cyberstalking und Cybercrime – Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher. Wiesbaden. Springer.

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

Huber, E. (2019). Cybercrime. Eine Einführung. Wiesbaden. Springer.

INTEGRAL (2019) AIM – Austrian Internet Monitor, rep. Österr. ab 14 Jahren, April bis Juni 2019+Q1 2019, n=1.000 telefonische Interviews. https://www.integral.co.at/downloads/Internet/2019/08/AIM-C_-_Q2_2019.pdf.

Kivivuori, J., Savolainen, J., & Aaltonen, M. (2016). The revenge motive in delinquency: Prevalence and predictors. Acta Sociologica 59(1), S. 69–84.

Levin J., & Madfis E. (2009). Mass murder at school and cumulative strain: A sequential model. American Behavioral Scientist 52(9): 1227–1245.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Zugegriffen: 22. August 2019.

[25] Grupe, M. (2018) Europas Unternehmen Vernachlässigen Den Kampf Gegen Fake News, European Communication Monitor, https://www.ffpr.de/2018/06/13/europas-unternehmen-vernachlaessigen-den-kampf-gegen-fake-news/, 16.12.2019.

Maes, J. (1994). Psychologische Überlegungen zu Rache. Berichte aus der Arbeitsgruppe «Verantwortung, Gerechtigkeit, Moral». Nr. 76. Universität Trier, Fachbereich I – Psychologie.

Mann R. E., & Hollin C. R. (2007). Sexual offenders' explanations for their offending. Journal of Sexual Aggression 13(1): 3–9.

Pathé, M., & Mullen, P. (1997). The impact of stalkers on their victims. British Journal of Psychiatry, 170(1), 12–17. doi:10.1192/bjp.170.1.12.

Roesner, M.: Cyberattacken auf Smart Buildings: 37,8 Prozent im ersten Halbjahr betroffen, https://www.kaspersky.de/blog/cyberattacken-auf-smart-buildings/20289/, 16.10.2019.

Tripp, M., & Bies, R. J. (1997). What's good about revenge? The avenger's perspective. In R. J. Lewicki, R. J. Bies, & B. H. Sheppard (Hrsg.), Research on negotiation in organizations 6: 145–160. Greenwich, CT: JAI.

United Nations (2000). Crimes related to computer networks. Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf. Zugegriffen: 22. August 2019.